DRBG Validation List

Last Update: 04/14/2017
PDF Version | HTML Version | XLSX Version

Overview

The page provides technical information about implementations that have been validated as conforming to the Deterministic Random Bit Generator (DRBG) Algorithm, as specified in Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators

Bookmarks: Each numbered item is bookmarked. To jump to the bookmark, append a "#[Number]" to the URL and press your Enter key. For example, to jump to the first IBM entry No. 787, append "#787 as in "Oct23-2015.html#787"

The list below describes implementations which have been validated as correctly implementing the DRBG algorithm, using the tests found in The DRBG Validation Suite (DRBGVS) This testing is performed by NVLAP accredited Cryptographic And Security Testing (CST) Laboratories.

The implementations below consist of software, firmware, hardware, and any combination thereof. The National Institute of Standards and Technology (NIST) has made every attempt to provide complete and accurate information about the implementations described in this document. However, due to the possibility of changes made within individual companies, NIST cannot guarantee that this document reflects the current status of each product. It is the responsibility of the vendor to notify NIST of any necessary changes to its entry in the following list.

This NIST document is cited in Zetter, K. (Sep. 24, 2013). How a Crypto 'Backdoor' Pitted the Tech World Against the NSA. *WIRED*.

It was retrieved on October 29, 2015 from the NIST website URL:
http://csrc nist.gov/groups/STM/cavp/documents/drbg/drbgval html

Retrived on April 14, 2017 (this data has not yet been added to the list below.)
http://csrc nist.gov/groups/STM/cavp/documents/drbg/drbgnewval html

The source NIST file is *horribly* coded. Suspiciously so. One could not print out the contents because the "Description/Notes" column was cut off. One could not make a PDF of the file for the same reason. Any attempt to import the file caused the researcher's computer to hang. If one tries to just read it online, the table runs off the side of the browser forcing the reader to have to scroll back and forth, which no one is going to do (except us!). The underlying HTML contained tens of thousands of anomolies that could have only been intentionally programmed into the file. The HTML used was not canonical. For example, actual quotation marks are still being placed in the HTML instead of the canonical """ characters. It uses noncanonical code for *italics* <i> instead of . It uses noncanonical code for **bold** <b> instead of ; and so on. It also used some very strange notation code that could be used to trigger some sort of tracking mechanism.

In the midst of its legacy HTML, it included modern CSS (Cascading Style Sheet) code that referenced external CSS libraries. In short, this important NIST disclosure file is a total and utter mess. One must ask why the nation's security is delegated to such intentionally obfuscating individuals. As has often been encourtered in bureaucratic documents that an agency does not want the public to actually review, the file is so large and so full of errors that it discourages the average citizen from reviewing the data. In fact, this "cleaned up" version took about 8 man-hours just to get it into this more readable state. Note, we noted that some information on Symantec's disclosures were deleted because the information ends mid-sentence, just before products are identified.

This list is ordered in reverse numerical order, by validation number. Thus, the more recent validations are located closer to the top of the list. The column after the Validation (Val.) Date column contains information indicating what modes and features for these modes has been successfully tested.

Val. No.	Vendor	Implementation	Operational Environment	Val. Date	Description/Notes
919	IBM Internet Security Systems 6303 Barfield Road Atlanta, GA 30328 USA -Ferrell Moultrie TEL: 678-234-4069 -Sheena Leake TEL: 404-238-5565	**IBM MESA / Modular Extensible Security Architecture OpenSSL** Version 5.3.1	Intel Xeon E5530 (2x) w/ RHEL 6.3 Linux on VMware ESXi 5.5	10/30/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHSVal#2941)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMACVal#2279)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3579)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3579)] "IBM MESA (Modular Extensible Security Architecture) is an appliance framework hosting applications in a secure environment and providing all cryptographic or other security-

					relevant functions to the application. For example: IBM XGS-virtual is a specific application instance hosted in this fashion."
918	IBM Internet Security Systems 6303 Barfield Road Atlanta, GA 30328 USA -Ferrell Moultrie TEL: 678-234-4069 -Sheena Leake TEL: 404-238-5565	**IBM MESA / Modular Extensible Security Architecture GSKit** Version 5.3.1	Intel Xeon E5530 (2x) w/ RHEL 6.3 Linux on VMware ESXi 5.5	10/30/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHSVal#2940)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMACVal#2278)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3578)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3578)] "IBM MESA (Modular Extensible Security Architecture) is an appliance framework hosting applications in a secure environment and providing all cryptographic or other security-relevant functions to the application. For example: IBM XGS-virtual is a specific application instance hosted in this fashion."
917	Red Hat, Inc. 100 East Davie Street Raleigh, NC 27601 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (shassse3)** Version 4.0	Intel x86 w/ Red Hat Enterprise Linux 7.1	10/30/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2939)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2277)] "Linux kernel crypto API implementation providing cryptographic services to software components executing as part of the Linux kernel."
916	Red Hat, Inc. 100 East Davie Street Raleigh, NC 27601 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (shagen) s390x** Version 4.0	s390x w/ Red Hat Enterprise Linux 7.1	10/30/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2938)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2276)] "Linux kernel crypto API implementation providing cryptographic services to software components executing as part of the Linux kernel."
915	Red Hat, Inc. 100 East Davie Street Raleigh, NC 27601 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (shagen) ppc64le** Version 4.0	ppc64le w/ Red Hat Enterprise Linux 7.1	10/30/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2937)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2275)] "Linux kernel crypto API implementation providing cryptographic services to software components executing as part of the Linux kernel."
914	Red Hat, Inc. 100 East Davie Street Raleigh, NC 27601 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (shaavx)** Version 4.0	Intel x86 w/ Red Hat Enterprise Linux 7.1	10/30/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2936)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2274)] "Linux kernel crypto API implementation providing cryptographic services to software components executing as part of the Linux kernel."
913	Red Hat, Inc. 100 East Davie Street Raleigh, NC 27601 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (shagen)** Version 4.0	Intel x86 w/ Red Hat Enterprise Linux 7.1	10/30/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2935)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2273)] "Linux kernel crypto API implementation providing cryptographic services to software components executing as part of the Linux kernel."
912	Red Hat, Inc. 100 East Davie Street Raleigh, NC 27601 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (aesni)** Version 4.0	Intel x86 w/ Red Hat Enterprise Linux 7.1	10/30/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3577)] "Linux kernel crypto API implementation providing cryptographic services to software

					components executing as part of the Linux kernel."
911	Red Hat, Inc. 100 East Davie Street Raleigh, NC 27601 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (aesasm)** Version 4.0	Intel x86 w/ Red Hat Enterprise Linux 7.1	10/30/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3571)] "Linux kernel crypto API implementation providing cryptographic services to software components executing as part of the Linux kernel."
910	**AlienVault, Inc.** 1875 S. Grant St. Suite 200 San Mateo, CA 94402 United States -Jim Hansen TEL: 650.713.3340	**AlienVault OpenSSL** Version 2.0.9	Intel Xeon E5 w/ Debian "Wheezy" 7.8	10/30/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-256) (AES Val#3566)] BlockCipher_No_df: (AES-128 , AES-256) (AES Val#3566)] "AlienVault USM for Government is a security appliance that provides complete security visibility and compliance management with five essential security capabilities - asset discovery, vulnerability assessment, intrusion detection, netflow, log analysis, and event correlation - into a single console and reporting dashboard."
909	Huawei (Dongguan) Co., Ltd. B2-5 of Nanfang Factory No.2 of Xincheng Rd Songshan Lake Science & Technology Industrial Zone Dongguan, Guangdong 523808 China -Tailiang Hong TEL: 86-755-36376922 -Blue Lee TEL: 86-755-28976679	**Huawei OpenSSL** **Version OpenSSL 1.0.1h**	HiSilicon K3V3+ w/ Android 5.0	10/23/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3565)] BlockCipher_No_df: (, AES-256) (AES Val#3565)] "General purpose cryptographic module available for Android used by Huawei devices. A variety of cryptographic services are provided, including AES, RSA, SHA, HMAC, CMAC, ECDSA, CTR_DRBG, etc."
908	Draeger Medical Systems, Inc. 6 Tech Drive Andover, MA 01810 USA -Michael Robinson TEL: 1 978 379 8000 FAX: 1 978 379 8538	**DRAEGER WCM9113 802.11ABGN VG2** **Version VG2.1 (Firmware)** **Part # MS32018**	N/A	10/23/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2661)] "DRBG routines in the DRAEGER WCM9113 802.11ABGN VG2 are based on hash based implementation as defined by SP 800-90A. These routines use SHA256 for hashing."
907	Redpine Signals, Inc. 2107 North First Street Suite #680 San Jose, CA 95131-2019 USA -Mallik Reddy TEL: 1 408 219 7868 FAX: 1 408 705 2019	**RSICryptoLib** **Version RSICryptoLib_1_1 (Firmware)** **Part # Redpine ThreadArch**	N/A	10/23/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2628)] "DRBG routines in RSICryptoLib are based on hash based implementation as defined by SP800-90A. These routines use SHA256 for hashing."
906	iboss Cybersecurity 9950 Summers Ridge Rd. Suite 160 San Diego, CA 92131 USA -Peter Martini TEL: 858-568-7051 FAX: 858-225-6158 -Christopher Park TEL: 858-568-7051 FAX: 858-225-6158	**Firesphere OpenSSL** **Version 7.1.0.0 (Firmware)**	Intel Xeon E5-1650v2 with AES-NI; Intel Xeon 2x E5-2650 with AES-NI	10/23/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-256) (AES Val#3563)] BlockCipher_No_df: (AES-128 , AES-256) (AES Val#3563)] "FireSphere OpenSSL is a suite of FIPS approved algorithms. The following algorithms are supported: AES 128 and 256, SP800-90A CTR DRBG 128 and 256, RSA SIGVer 1024, 2048, and 3072, RSA SigGen 2048 and 3072, RSA KeyGen 2048 and 3072, SHA and HMAC-SHA 1, 224, 256, 384, and 512, and RSA key wrapping."
905	VMware, Inc. 3401 Hillview Ave Palo Alto, CA 94303 USA -Gary Sturdivant TEL: 1-659-427-4429 -Eric Betts TEL: 1-650-427-1902	**VMware Horizon JCE (Java Cryptographic Extension) Module** **Version 1.0**	Intel Xeon E5-2630 w/ Horizon 6, version 6.2 with Sun JRE 1.8 on Windows Server 2012R2 running on VMware vSphere Hypervisor (ESXi) 6.0; Intel Xeon E5-2630 w/ Horizon 6, version 6.2 with Sun JRE 1.8 on Windows 7 SP1 Enterprise (32-bit) running on VMware vSphere Hypervisor (ESXi) 6.0	10/23/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-512) (SHS Val#2929)] "The VMware Horizon JCE (Java Cryptographic Extension) Module is a versatile software library that implements FIPS 140-2 approved cryptographic services for VMware products and platforms."
904	iDirect Government 13921 Park Center Road, Suite 600 Herndon, VA 20171 USA -Chris Gormont TEL: 703-880-6257	**Satellite Communication** **Version 15.0.2.2 (Firmware)**	Intel EWIXP465BAET 667 MHz	10/23/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3548)] BlockCipher_No_df: (, AES-256) (AES Val#3548)] "VT iDirect, Inc's firmware cryptographic module, Secure Satelite Broadband Solution, provides all

	FAX: 703-648-8088 -Tony Tran TEL: 703-880-6243 FAX: 703-648-8088				cryptographic operations for the management of iDirect's Transmission Security (TRANSEC) feature. The cryptographic module supports key management algorithms that allow for each member of the network to receive and decrypt data."
903	Motorola Solutions Systems Polska Sp. z o.o. Czerwone Maki 82 Krakow, n/a 30-392 Poland -Tomasz Chmiel TEL: +48 12 29 79 000 FAX: +48 12 29 79 001 -Tomasz Rypina TEL: +48 12 29 79 000 FAX: +48 12 29 79 001	**OpenSSL** **Version 1.0.1c (Firmware)**	Freescale MPC-7457; Freescale MPC-8568E	10/23/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2926)] "OpenSSL is used to provide the encryption function for S6000 and GGM8000 network devices."
902	GOTrust Technology Inc. 10F-1, No.306, Sec. 1, Wenxin Rd., Nantun Dist. Taichung City, 408 Taiwan -Jerry Lin TEL: +886-4-23202525 FAX: +886-4-23202580	**GO-Trust Cipher Library** **Version 1.0 (Firmware)**	ARM SecurCore SC300	10/16/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1672)] "The GO-Trust Cipher Library is designed to provide FIPS140-2 algorithm support for the GO-Trust SDencrypter Cryptographic Module. This module supports GO-Trust applications (for example: KingCall and KingText) by providing validated Cryptographic Services. The incorporation of these algorithms makes these products ideal for enterprise and governmen"
901	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 4083330480 FAX: 4083338101	**Brocade FIPS Crypto Library** **Version 6.0.2 (Firmware)**	E500mc	10/16/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3544)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. The Brocade stackable switch delivers the performance, flexibility, and scalability required for enterprise Gigabit Ethernet (GbE) access deployment. It offers market-leading stacking density with up to 12 switches per stack and combines chassis."
900	Gemalto 6, rue de la Verrerie CS 20001 Meudon Cedex, n/a 92197 France -Gilles ROMME TEL: +33 155015712 FAX: +33 155015170 -Guennole Tripotin TEL: +33 442365522 FAX: +33 442365236	**Cryptographic library for MultiApp V31** **Version FM Version 2.1 (Firmware)** **Part # NXP P60**	NXP SmartMX2 P60 chip family	10/16/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-128) (AES Val#3543)] "MultiApp V3.1 is a highly secured smartcard platform compliant with the Javacard 2.2.2, GP 2.1.1 & GP 2.2 Amdt D standards, designed to operate with the NXP P60xx chip. It supports: TDES, AES, AES-CMAC, SHA1-224-256-384-512, RSA, RSA CRT, ECDSA, ECC CDH & DRBG SP800-90A algorithms."
899	Nuvoton Technology Corporation No. 4, Creation Rd. III Hsinchu Science Park, n/a 300 Taiwan, R.O.C. -Yossi Talmi TEL: +972-9-9702364 FAX: +972-9-9702001 -Oren Tanami TEL: +972-9-9702390 FAX: +972-9-9702001	**Nuvoton NPCT6xx TPM 2.0 Cryptographic Engine** **Part # FB5C85E**	N/A	10/9/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2920)] "Nuvoton TPM (Trusted Platform Module), a TCG 2.0 compliant security processor with embedded firmware."
898	Nuvoton Technology Corporation No. 4, Creation Rd. III Hsinchu Science Park, n/a 300 Taiwan, R.O.C. -Yossi Talmi TEL: +972-9-9702364 FAX: +972-9-9702001 -Oren Tanami TEL: +972-9-9702390 FAX: +972-9-9702001	**Nuvoton NPCT6xx TPM 2.0 Cryptographic Engine** **Part # FB5C85D**	N/A	10/9/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2919)] "Nuvoton TPM (Trusted Platform Module), a TCG 2.0 compliant security processor with embedded firmware."
897	Kaspersky Lab UK Ltd. 1st Floor, 2 Kingdom Street Paddington	**Kaspersky Cryptographic Library 64-bit (User Mode)** **Version 2.0**	Intel(R) Core(TM)2 Duo P9600 @ 2.53GHz w/ Kaspersky Preboot OS with UEFI	10/9/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-256) (AES Val#2980)]

	London, W2 6BD United Kingdom -Oleg Andrianov TEL: +7 495 797 8700				BlockCipher_No_df: (AES-128 , AES-256) (AES Val#2980)] "Kaspersky Cryptographic Library is a software library that provides cryptographic services for various Kaspersky Lab applications."
896	Kaspersky Lab UK Ltd. 1st Floor, 2 Kingdom Street Paddington London, W2 6BD United Kingdom -Oleg Andrianov TEL: +7 495 797 8700	**Kaspersky Cryptographic Library 32-bit (User Mode)** **Version 2.0**	Intel(R) Core(TM)2 Duo P9600 @ 2.53GHz w/ Windows 7 Professional 32-bit; Intel(R) Core(TM)2 Duo P9600 @ 2.53GHz w/ Kaspersky Preboot OS with BIOS	10/9/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-256) (AES Val#2849)] BlockCipher_No_df: (AES-128 , AES-256) (AES Val#2849)] "Kaspersky Cryptographic Library is a software library that provides cryptographic services for various Kaspersky Lab applications."
895	Toshiba Corporation 1-1, Shibaura 1-chome Minato-ku, Tokyo 105-8001 Japan -Tohru Iwamoto TEL: +81-45-776-4488 FAX: +81-45-776-4106	**Toshiba Cryptographic for Enterprise HDD Hash_DRBG** **Version 1.00 (Firmware)**	Cortex-R5	10/9/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2916)] "A library of unique software cipher solutions which are standard encryption algorithm-based to provide Toshiba enterprise HDD products and the systems using them a robust and secure data storage environment."
894	Hewlett Packard Enterprise 153 Taylor Street Littleton, MA 01460 USA -Bob Pittman TEL: 1-978-264-5211 FAX: 1-978-264-5522	**HPE Comware** **Version Comware V5.2-R3303 (Firmware)**	Freescale P2020, 1.0GHz, PowerPC; Freescale P4080, 1.5GHz, PowerPC	9/30/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3540)] "Comware cryptographic library is a software library that provides cryptographic functions within HP devices."
893	Advanced Card Systems Ltd. Units 2010-2013, 20/F Chevalier Commercial Centre 8 Wang Hoi Road Kowloon Bay Hong Kong, -Andrew Chan TEL: +852-27967873 FAX: +852-27961286	**ACOS5-64** **Version 3.00 (Firmware)**	ST23YL80 Version PU7	9/30/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256) (SHS Val#2917)] "ACOS5-64 is an advanced cryptographic module specifically designed for the Public Key Infrastructure (PKI)-based applications. With its powerful cryptographic capabilities, it enhances the security and performance of RSA public key cryptographic operations that are essential to the stringent requirements of high-level security applications."
892	Kaspersky Lab UK Ltd. 1st Floor, 2 Kingdom Street Paddington London, W2 6BD United Kingdom -Oleg Andrianov TEL: +7 495 797 8700	**Kaspersky Cryptographic Library 64-bit NI (Kernel Mode)** **Version 2.0**	Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz w/ Windows 7 Enterprise 64-bit; Intel(R) Core(TM) i7-3770S CPU @ 3.10GHz w/ Windows 8.1 Enterprise 64-bit	9/30/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-256) (AES Val#2957)] BlockCipher_No_df: (AES-128 , AES-256) (AES Val#2957)] "Kaspersky Cryptographic Library is a software library that provides cryptographic services for various Kaspersky Lab applications."
891	Kaspersky Lab UK Ltd. 1st Floor, 2 Kingdom Street Paddington London, W2 6BD United Kingdom -Oleg Andrianov TEL: +7 495 797 8700	**Kaspersky Cryptographic Library 64-bit NI (User Mode)** **Version 2.0**	Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz w/ Windows 7 Enterprise 64-bit; Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz w/ Windows 8.1 Enterprise 64-bit; Intel(R) Core(TM) i7-3770S CPU @ 3.10GHz w/ Kaspersky Preboot OS with UEFI	9/30/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-256) (AES Val#2959)] BlockCipher_No_df: (AES-128 , AES-256) (AES Val#2959)] "Kaspersky Cryptographic Library is a software library that provides cryptographic services for various Kaspersky Lab applications."
890	Kaspersky Lab UK Ltd. 1st Floor, 2 Kingdom Street Paddington London, W2 6BD United Kingdom -Oleg Andrianov TEL: +7 495 797 8700	**Kaspersky Cryptographic Library 32-bit NI (User Mode)** **Version 2.0**	Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz w/ Windows 7 Enterprise 64-bit; Intel(R) Core(TM) i7-3770S CPU @ 3.10GHz w/ Windows 8.1 Enterprise 64-bit; Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz w/ Kaspersky Preboot OS with BIOS	9/30/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-256) (AES Val#2960)] BlockCipher_No_df: (AES-128 , AES-256) (AES Val#2960)] "Kaspersky Cryptographic Library is a software library that provides cryptographic services for various Kaspersky Lab applications."
889	Hewlett-Packard Longdown Avenue Stoke Gifford, Bristol BS34 8QZ United Kingdom -Laura Loredo TEL: +44 117 316 2462 -John Drew TEL: +44 560 109 0356	**OpenSSL** **Version 1.0.1p (FIPS 2.0) (Firmware)**	ARM966E	9/25/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3534)] "AES ECB and CBC: 128/256 bits, encryption/decryption. CTR DRBG with Derivation Function. GCM: 128/256 bits, encryption/decryption. HMAC-SHA-1/224/256/384/512. SP 800-135 KDF - TLS 1.0, 1.1 and 1.2, with SHA-256 and SHA-384. RSA: FIPS 186-2 RSA; GenKey9.31; SigGenPKCS1.5; SigVerPKCS1.5; SigVerPSS. SHA-1/224/256/384/512."

888	Vocera Communications Inc. 525 Race Street San Jose, CA 95126 USA -Ammath Keunemany TEL: 4088824615 FAX: 4088825101 -Crispin Jacob TEL: 918042654719	**Vocera Cryptographic Module** **Version 3.0**	Texas Instruments OMAP-L138 w/ Vocera Embedded Linux v3.0	9/25/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2912)] "Vocera B3000n Badge is a wearable hands-free voice-controlled device that provides easy to use and instantaneous communication on a wireless LAN network. The Vocera Cryptographic Module, embedded in the B3000n Badge ensures protected communications using industry-standard secure wireless communication protocols."
887	Harris Corporation 1680 University Avenue Rochester, NY 14610 USA -Steven Ruggieri TEL: 585-239-7806 FAX: 585-241-8159 -Suzanne Kwak TEL: 585-242-4686 FAX: 585-241-8159	**Harris Broadband Ethernet Radio GPP Cryptographic Library** **Version 4.10 (Firmware)**	Broadcom XLS108	9/25/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-256) (SHS Val#2911)] "This is a firmware library which executes on a general purpose processor to provide cryptographic functions for Harris' industry leading reliable, secure, and high performance Broadband Ethernet Radio (BER) products: RF-7800-OU50x/-OU47x/-OU49x."
886	Ionic Security Inc. 1170 Peachtree Street NE Suite 400 Atlanta, Georgia 30309 USA -Allen Vance TEL: 404-736-6000 -Kent Rollins TEL: 404-736-6000	**FIPS Crypto Module** **Version 1.0**	Intel Core i7 w/ Windows 7; Intel Xeon E5-2650 w/ CentOS 7.1.1503	9/25/2015	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (HMAC Val#2255)] "Ionic Security's Fusion Platform implements the FIPS Crypto Module for all cryptographic functions such as key pair generation, digital signature generation/ and verification, encryption and decryption, hashing functions, and message authentication."
885	Qualcomm Technologies Inc. 5775 Morehouse Dr San Diego, CA 92121 USA -Yin Ling Liong TEL: 858-651-7034 FAX: 858-845-1523	**QTI Pseudo Random Number Generator** **Part # Snapdragon 820**	N/A	9/25/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2908)] "Snapdragon 820 Pseudo Random Number Generator is a hardware random number generator that provides cryptographic functions through on-chip entropy sources and hash based DRBG." *10/22/15: Updated implementation information;*
884	KONA I Co. Ltd 8F EXCON Venture-Tower, 3, Eunhaeng-Ro, Yeongdeungpo-Gu Seoul, n/a 150-872 Republic of Korea -Irene Namkung TEL: +82-2-2168-7586 FAX: +82-2-3440-4405 -Sungmin Ahn TEL: +82-2-3440-9135 FAX: +82-2-3440-4405	**KONA HW Crypto Library** **Version 2.01 (Firmware)** **Part # Infineon SLE97CNFX1M00PE A22**	Infineon SLE97CNFX1M00PE A22	9/18/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3525)] "**CTR_DRBG**: AES 128/192/256 bit. AES: ECB/CBC, 128/192/256 bit. AES CMAC: 128/192/256 bit. Triple-DES: 2-key/3-key, ECB/CBC. RSA: 2048 bit encrypt/decrypt, sign/verify, key gen (legacy use 1024 bit verify with SHA-1). RSA CRT: 2048 bit key gen, sign. ECDSA: P-224/256/384/521 key gen/sign/verify (legacy use P-192 verify)."
883	Infineon Technologies AG Alter Postweg 101 Augsburg, BY 86159 Germany -Roland Ebrecht TEL: +49-821-25851-68 FAX: +49-821-25851-40 -Thomas Hoffmann TEL: +49-821-25851-24 FAX: +49-821-25851-40	**Trusted Platform Module 1.2 SLB 9670** **Version 6.80.0113.02 (Firmware)** **Part # SLB 9670**	Infineon SLB 9670 security controller IC	9/18/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3524)] "Infineon Trusted Platform Module 1.2 SLB 9670 is an implementation according to the TPM Main Specification Version 1.2 Revision 116 by Trusted Computing Group."
882	Infineon Technologies AG Alter Postweg 101 Augsburg, BY 86159 Germany -Roland Ebrecht TEL: +49-821-25851-68 FAX: +49-821-25851-40 -Thomas Hoffmann TEL: +49-821-25851-24 FAX: +49-821-25851-40	**Trusted Platform Module 1.2 SLB 9660, SLB 9665** **Version 4.80.0411.02 (Firmware)** **Part # SLB 9660/9665**	Infineon SLB 9660 or SLB 9665 security controller IC	9/18/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3523)] "Infineon Trusted Platform Module 1.2 SLB 9660/SLB 9665 is an implementation according to the TPM Main Specification Version 1.2 Revision 116 by Trusted Computing Group."
881	Ciena Corporation 7035 Ridge Road Hanover, MD 21076 USA	**SAOS** **Version 6.13.2 (Firmware)**	ARMv7; Cavium 31XX	9/18/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2904)]

	-Kevin Meagher				"Carrier Ethernet Switching Operating System and Control Application"
880	Acronis International GmbH Rheinweg 9 8200 Schaffhausen, n/a n/a Switzerland -Oleg Mikhalsky TEL: +7 (495) 648-14-27 FAX: +7 (495) 708-44-89 -Anton Enakiev TEL: +7 (495) 648-14-27 FAX: +7 (495) 708-44-89	**Acronis AnyData Cryptographic Library** **Version 1.0**	Intel Core i3-3217U without AES-NI w/ Red Hat Enterprise Linux 6.6; Intel Core i3-3217U without AES-NI w/ Red Hat Enterprise Linux 7.1; Intel Core i5-5300U with AES-NI w/ Acronis Virtual Appliance Linux 11.5 on vSphere 5.5; Intel Core i3-3217U without AES-NI w/ Windows 7 Ultimate 32bit; Intel Core i5-5300U with AES-NI w/ Windows 7 Ultimate 64bit; Intel Core i5-5300U with AES-NI w/ Intel Core i5-5300U with AES-NI; Intel Core i5-5300U with AES-NI w/ Windows 8.1 Pro 64bit ; Intel Core i3-3217U without AES-NI w/ Windows 2008 R2 64bit ; Intel Core i3-3217U without AES-NI w/ Windows 2012 R2 64bit	9/18/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2903)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2249)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3521)] "Acronis AnyData Cryptographic Library (AACL) is a cryptographic software module used in various products Acronis."
879	Acronis International GmbH Rheinweg 9 8200 Schaffhausen, n/a n/a Switzerland -Oleg Mikhalsky TEL: +7 (495) 648-14-27 FAX: +7 (495) 708-44-89 -Anton Enakiev TEL: +7 (495) 648-14-27 FAX: +7 (495) 708-44-89	**Acronis AnyData Cryptographic Library** **Version 1.0**	Intel Core i5-5300U with AES-NI w/ Red Hat Enterprise Linux 6.6; Intel Core i5-5300U with AES-NI w/ Red Hat Enterprise Linux 7.1; Intel Core i5-5300U with AES-NI w/ Windows 2008 R2 64bit; Intel Core i5-5300U with AES-NI w/ Windows 2012 R2 64bit	9/18/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3520)] "Acronis AnyData Cryptographic Library (AACL) is a cryptographic software module used in various products Acronis."
878	Intel Corporation 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Andy Nissen TEL: 651-628-5385	**McAfee Next Generation Firewall** **Version 2.0.9**	Intel i3 w/ Linux x86_64	9/11/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3517)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3517)] "A cryptographic library compiled for Linux on Intel x86_64 compatible processors."
877	B+B Smartworx 707 Dayton Road PO Box 1040 Ottawa, IL 61350 USA -Paul Conway TEL: 1-800-346-3119 FAX: 815-433-5109	**B+B Smartworx NSS Cryptographic Module** **Version 1.0**	ARM Cortex w/ Conel Linux 5	9/11/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2897)] "Network Security Services (NSS) is a set of open source C libraries designed to support cross-platform development of security-enabled applications. NSS implements major crypto algorithms and Internet security standards."
876	IBM Corporation 80 Bishop Dr., Unit B Fredericton, New Brunswick E3C 1B2 Canada -Sandra Hernandez TEL: (512) 286-5624 -Marie Fraser TEL: +353 (21) 730-6043	**IBM QCrypto Module** **Version 1.0 (Firmware)**	Intel XEON Ivy Bridge	9/11/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3512)] "The algorithms are implemented by OpenSSL version 1.0.1e provided by RedHat. Additional native bridges are implemented by IBM and allow all QRadar components to make cryptographic request to OpenSSL directly."
875	wolfSSL Inc. 10016 Edmonds Way Suite C-300 Edmonds, WA 98020 USA -Todd Ouska TEL: 503-679-1859 -Larry Stefonic TEL: 206-369-4800	**wolfCrypt** **Version 3.6.6**	Intel Core i5 w/ Windows 7 64-bit	9/4/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2893)] "WolfCrypt module is a comprehensive suite of FIPS Approved algorithms. All key sizes and modes have been implemented to allow flexibility and efficiency." *09/11/15: Updated implementation information;*
874	General Dynamics C4 Systems 77 A Street Needham, MA 02494 USA -David Aylesworth TEL: 781-400-6527	**Fortress Cryptographic Implementation - SSL** **Version 2.1 (Firmware)**	RMI Alchemy MIPS Processor; Broadcom XLS Processor	8/18/2015	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2238)] "The Fortress Cryptographic Implementation suite works in unison to provide security to your wireless and wired networks."
873	Fortinet, Inc. 1090 Kifer Road Sunnyvale, CA 94086-5301 USA -Alan Kaye TEL: 613-225-9381 x7416 FAX: 613-225-9951	**Fortinet FortiMail RNG Cryptographic Library** **Version 5.2 (Firmware)**	Intel Xeon	8/18/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3500)] "This focuses on the firmware implementation of the Fortinet FortiMail RNG Cryptographic Library v5.2 running on Intel x86 compatible processors."

872	Hewlett Packard® Enterprise 10810 Farnam Drive NBN02 Omaha, NE 68154 USA -Nagesh Kuriyavar TEL: 402-758-7262 FAX: 402-758-7332 -Matt Johnson	**OpenCall HLR Cryptographic Module** **Version I-HSS 1.08.00**	Intel Itanium 9300 w/ Non Stop OS J06.18	8/18/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3503)] "The HP OpenCall HLR Cryptographic Module provides cryptographic services that allows the HP I-HLR to protect sensitive application and subscriber data at rest and during transit." *09/10/15: Updated implementation information;*
871	Palo Alto Networks 4401 Great America Parkway Santa Clara, California 95054 USA -Richard Bishop TEL: 408-753-4000 -Jake Bajic TEL: 408-753-3901	**Palo Alto Networks Crypto Module (PA VM-series)** **Version 7.0 (PAN-OS)**	Intel Multi Core Xeon w/ VMware ESXi 5.5; Intel Multi Core Xeon w/ CentOS 6.5 - KVM; Intel Multi Core Xeon w/ Citrix XenServer 6.1.0	8/18/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3501)] BlockCipher_No_df: (, AES-256) (AES Val#3501)] "The Palo Alto Networks Crypto Module provides the cryptographic functionality for a variety of Palo Alto Networks VM-series platforms. The firewalls provide network security by enabling enterprises to see/control applications, users, and content."
870	Palo Alto Networks 4401 Great America Parkway Santa Clara, California 95054 USA -Richard Bishop TEL: 408-753-4000 -Jake Bajic TEL: 408-753-3901	**Palo Alto Networks Crypto Module (PA-200, PA-500, PA-2000, PA-3000, PA-4000, PA-5000 and PA-7000 firewalls, WF-500 and Panorama M-100/M-500)** **Version 7.0 (PAN-OS, Wildfire)/7.1 (Panorama) (Firmware)**	Cavium Octeon MIPS64; Intel Multi Core Xeon; Intel Celeron P4505; Intel i7	8/15/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3475)] BlockCipher_No_df: (, AES-256) (AES Val#3475)] "The Palo Alto Networks Crypto Module provides the cryptographic functionality for a variety of platforms i.e. the PA-200, PA-500, PA-2000, PA-3000, PA-4000, PA-5000 and PA-7000 firewalls, WF-500 and Panorama M-100/M-500."
869	Vormetric Inc. 2545 North 1st Street San Jose, CA 95131 USA -Oliver Galvez TEL: (408) 433-6000 FAX: (408) 844-8637 -Peter Tsai TEL: (408) 433-6000 FAX: (408) 844-8637	**Vormetric Data Security Server Module** **Version 5.3.0 (Firmware)**	Intel Xeon	8/15/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3499)] "Vormetric Data Security Manager that creates, stores and manages security objects such as keys, certificates and access control policies for distributed encryption agents."
868	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA -Tim Myers TEL: 800-Microsoft	**Microsoft Windows 10, Microsoft Surface Pro 3 with Windows 10, Microsoft Surface 3 with Windows 10, Microsoft Surface Pro 2 with Windows 10, Microsoft Surface Pro with Windows 10 SymCrypt Cryptographic Implementations** **Version 10.0.10240**	Intel Core i7 with AES-NI and PCLMULQDQ and SSSE 3 w/ Windows 10 (x64); AMD A4 with AES-NI and PCLMULQDQ and SSSE 3 w/ Windows 10 (x64); Intel Core i3 without AES-NI or PCLMULQDQ or SSSE 3 w/ Windows 10 (x86); AMD A4 with AES-NI and PCLMULQDQ and SSSE 3 w/ Windows 10 Enterprise (x64); Intel x64 Processor with AES-NI w/ Microsoft Surface Pro w/ Windows 10 Enterprise (x64); Intel Core i5 with AES-NI w/ Microsoft Surface Pro 2 w/ Windows 10 Enterprise (x64); Intel Core i7 with AES-NI w/ Microsoft Surface Pro 3 w/ Windows 10 Enterprise (x64); Intel Core i3 without AES-NI or PCLMULQDQ or SSSE 3 w/ Windows 10 Enterprise (x86); AMD A4 with AES-NI and PCLMULQDQ and SSSE 3 w/ Windows 10 Pro (x64); Intel x64 Processor with AES-NI w/ Microsoft Surface Pro w/ Windows 10 Pro (x64); Intel Core i5 with AES-NI w/ Microsoft Surface Pro 2 w/ Windows 10 Pro (x64); Intel Core i7 with AES-NI w/ Microsoft Surface Pro 3 w/ Windows 10 Pro (x64); Intel Core i3 without AES-NI or PCLMULQDQ or SSSE 3 w/ Windows 10 Pro (x86); Intel Atom x7 with AES-NI and PCLMULQDQ and SSSE 3 w/ Microsoft Surface 3 w/ Windows 10 Enterprise (x64) ; Intel Core i7 with AES-NI and PCLMULQDQ and SSSE 3 w/ Windows 10 Enterprise LTSB (x64); AMD A4 with AES-NI and PCLMULQDQ and SSSE 3 w/ Windows 10 Enterprise LTSB (x64); Intel Core i3 without AES-NI or PCLMULQDQ or SSSE 3 w/ Windows 10 Enterprise LTSB (x86)	8/15/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3497)] "The Microsoft Windows Next Generation Cryptographic algorithm implementation provides enhanced support for AES, AES DRBG, HMAC, SHS (SHA), and Triple-DES. All implementations are packaged into a library used by Microsoft and other third-party applications." *09/17/15: Updated implementation information; 10/09/15: Added new tested information;*
867	Toshiba Corporation 1-1, Shibaura 1-chome Minato-ku, Tokyo 105-8001 Japan	**Toshiba Cryptographic for Enterprise SSD SEC CPU FW Hash_DRBG** **Version 1.00 (Firmware)**	88SS1032B0-BTJ2C000-P167	8/15/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2879)] "A library of unique software cipher solutions which are standard encryption algorithm-based to

	-Akihiro Kimura TEL: +81-45-890-2856 FAX: +81-45-890-2593				provide Toshiba enterprise SSD products and the systems using them a robust and secure data storage environment."
866	Blue Coat Systems Inc. 420 North Mary Avenue Sunnyvale, California 94085-4121 USA -Diana Robinson TEL: 845-454-6397 -Nick Goble TEL: 978-318-7544	**Blue Coat SSL Visibility Appliance Crypto Library** **Version 1.0.3**	Intel X3450 Quad Core w/ Linux x86_64; Intel E5620 Quad Core w/ Linux x86_64; Intel E5645 Hex Core w/ Linux x86_64	8/15/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3496)] "The Blue Coat SSL Visibility Appliance decrypts multiple streams of SSL content to provide IDS/IPS, logging, forensics, and data loss prevention. This preserves complete network traffic histories necessary for compliance/threat analysis and enables SSL inspection capabilities that close the security loophole created by SSL."
865	Huawei Technologies Co. Ltd Huawei Industrial Base, Bantian Longgang Shenzhen, Guangdong 518129 China -Li Wen TEL: 0086-0755-28976679 FAX: 0086-0755-28976679	**Huawei Radio Link Encryption (RLE)** **Version 1.0 (Firmware)**	n/a	8/15/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256) (SHS Val#2884)] "The module provides the functionality of cipher (AES-CCM) transceiver of radio data as security function."
864	Huawei Technologies Co., Ltd Huawei Industrial Base, Bantian Longgang Shenzhen, Guangdong 518129 China -Li Wen TEL: 0086-0755-28976679 FAX: 0086-0755-28976679	**Huawei AR Crypto Module (AR160 Series)** **Version 1.0 (Firmware)**	n/a	8/15/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2883)] "The Huawei AR Crypto Module (AR160 Series) provides comprehensive security, performance and reliability for network environments."
863	wolfSSL Inc. 10016 Edmonds Way Suite C-300 Edmonds, WA 98020 USA -Todd Ouska TEL: 503-679-1859 -Larry Stefonic TEL: 206-369-4800	**wolfCrypt** **Version 3.6.1**	ST Micro STM32F w/ FreeRTOS 7.6	8/15/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2882)] "WolfCrypt module is a comprehensive suite of FIPS Approved algorithms. All key sizes and modes have been implemented to allow flexibility and efficiency."
862	Pure Storage, Inc. 650 Castro Street Suite #400 Mountain View, CA 94041 USA -Marco Sanvido TEL: 510-501-8968 -Ethan Miller TEL: 831-345-4864	**Flash Array Crypto Library** **Version 1.1.0**	Intel Xeon x64 CPU with AES-NI (E3/E5/E7 Family) w/ Purity 4	7/31/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3488)] "Flash Array Crypto Library is a comprehensive suite of FIPS Approved algorithms. All key sizes and modes have been implemented to allow flexibility and efficiency."
861	Alcatel-Lucent 600 March Road Ottawa, Ontario K2K 2E6 Canada -Carl Rajsic TEL: +1 613 784 6218 -Alfred Nothaft TEL: +1 972 477 5087	**Alcatel Lucent 7x50 SR OS Cryptographic Library** **Version 1.0 (Firmware)**	Cavium CN5845; Cavium CN6635; Cavium CN6645	7/31/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3484)] "The Alcatel-Lucent 7x50 SR OS Cryptographic Library is used on the Alcatel-Lucent 7x50 Service Router products."
860	Sonus Networks Inc. 4 Technology Park Drive Westford, MA 01886 USA -Adam Elshama TEL: 1-855-GO-SONUS FAX: 978-614-8101 -Nui Chan TEL: 1-855-GO-SONUS FAX: 978-614-8101	**Sonus Cryptographic Library** **Version 2 (Firmware)**	Intel Ivy Bridge	7/31/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3483)] BlockCipher_No_df: (AES-128) (AES Val#3483)] "Sonus Session Border Controller FIPS-validated cryptographic software module."
859	Sonus Networks, Inc. 4 Technology Park Drive Westford, MA 01886 USA -Adam Elshama TEL: 1-855-GO-SONUS FAX: 978-614-8101	**Sonus Cryptographic Library** **Version 2 (Firmware)**	Intel Nehalem	7/31/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3481)] BlockCipher_No_df: (AES-128) (AES Val#3481)] "Sonus Session Border Controller FIPS-validated cryptographic software module"

	-Nui Chan TEL: 1-855-GO-SONUS FAX: 978-614-8101				
858	Huawei Technologies Co. Ltd Huawei Industrial Base, Bantian Longgang Shenzhen, Guangdong 518129 China -Li Wen TEL: 0086-0755-28976679 FAX: 0086-0755-28976679	**Huawei Radio Link Encryption (RLE)** **Version 1.0 (Firmware)**	n/a	7/31/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256) (SHS Val#2873)] "The module provides the functionality of encryption transceiver of radio data as security function."
857	Huawei Technologies Co. Ltd Huawei Industrial Base, Bantian Longgang Shenzhen, Guangdong 518129 China -Li Wen TEL: 0086-0755-28976679 FAX: 0086-0755-28976679	**Huawei FIPS Cryptographic Library (HFCL)** **Version V300R003C22SPC804**	DELL PowerEdge T100 II Systems Intel Pentium w/ RHEL 5.3 evaluated at EAL4	7/31/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2872)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2221)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3477)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3477)] "Huawei FIPS Cryptographic Library (HFCL) provides FIPS approved Cryptographic functions to consuming applications via an Application Programming Interface (API)"
856	CoCo Communications 800 5th Ave Seattle, WA 98104 USA -David Weidenkopf TEL: 206-812-5783	**CoCo OpenSSL Windows 7** **Version 2.2**	Intel i5 w/ Windows 7 64 bit	7/24/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2869)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2219)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3474)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3474)] "The CoCo OpenSSL Crypto Module is an OpenSSL cryptographic library that provides cryptographic services to its calling applications."
855	Blue Coat Systems Inc. 420 North Mary Avenue Sunnyvale, California 94085-4121 USA -Diana Robinson TEL: 845-454-6397 -Nick Goble TEL: 978-318-7544	**Blue Coat SSL Visibility Appliance Crypto Library** **Version 1.0.2**	Intel X3450 Quad Core w/ Linux x86_64; Intel E5620 Quad Core w/ Linux x86_64; Intel E5645 Hex Core w/ Linux x86_64	7/24/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3473)] "The Blue Coat SSL Visibility Appliance decrypts multiple streams of SSL content to provide IDS/IPS, logging, forensics, and data loss prevention. This preserves complete network traffic histories necessary for compliance/threat analysis and enables SSL inspection capabilities that close the security loophole created by SSL."
854	Redline Communications Inc. 302 Town Centre Blvd., 4th Floor Markham, Ontario L3R OE8 Canada -Andrew Spurgeon TEL: 905-479-8344 x2471 -Weixiong Lin TEL: 905-479-8344 x2372	**RDL-3000 Management Cryptographic Suite** **Version 3.1 (Firmware)**	Cavium ECONA CNS3411 SoC	7/17/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-256) (SHS Val#2866)] "Provides several cryptographically-secure management interfaces for use in the administration and operation of the RDL-3000 platform."
853	N/A	**N/A**	N/A	7/17/2015	N/A
852	Certicom Corp. 4701 Tahoe Blvd, Building A Mississauga, Ontario L4W 0B5 Canada -Certicom Support TEL: 1-905-507-4220 FAX: 1-905-507-4230 -Certicom Sales TEL: 1-905-507-4220 FAX: 1-905-507-4230	**Security Builder GSE-J Crypto core** **Version 2.8.8**	Intel Xeon w/ CentoOS Linux 7.0 64 bit with Oracle JRE 1.8.0	7/10/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2860)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2210)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3465)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#702) (SHS Val#2860)

					"Security Builder GSE-J is a standards-based cryptographic toolkit written in Java. It supports optimized Elliptic Curve Cryptography and provides application developers with sophisticated tools to flexibly integrate encryption, digital signatures and other security mechanisms into Java-based applications."
851	Thales e-Security Meadow View House Crendon Industrial Estate Long Crendon Aylesbury, Buckinghamshire HP18 9EQ U.K. -Phil Jones TEL: +44 (0) 1844 203596 FAX: +44 (0)1844 208550 -Ian Clover TEL: +44 (0) 1293 589085 FAX: +44 (0) 1293 589001	**Datacryptor Hash_DRBG** **Version v1.7 (Firmware)**	Motorola Coldfire processor - single core	7/10/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-384) (SHS Val#1717)] "Thales e-Security implements this algorithm for applications running on its Secure Generic Sub System (SGSS) providing secure cryptographic resources to the Datacryptor® 2000 and the Datacryptor® Advanced Performance network encryption products for IP, Frame Relay and Link networks."
850	Certicom Corp. 4701 Tahoe Blvd, Building A Mississauga, Ontario L4W 0B5 Canada -Certicom Support TEL: 1-905-507-4220 FAX: 1-905-507-4230 -Certicom Sales TEL: 1-905-507-4220 FAX: 1-905-507-4230	**Security Builder Linux Kernel Crypto Core** **Version 1.0**	ARMv8 Qualcomm MSM8992 w/ Android 5.1; Intel Xeon E5620 with AES-NI w/ CentOS 7 Linux 64-bit;	7/10/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256 , SHA-384 , SHA-512) (SHS Val#2859)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256 , SHA-384 , SHA-512) (HMAC Val#2209)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3464)] "Security Builder Linux Kernel Crypto Core provides general-purpose cryptographic services to other Linux kernel modules."
849	Samsung Electronics Co. Ltd R4 416, Maetan 3-dong, Yeongtong-gu Suwon-si, Gyeonggi-do 443-742 Korea -Bumhan Kim TEL: +82-10-9397-1589	**Samsung Kernel Cryptographic Module** **Version SKC1.6**	ARMv7 w/ Android Lollipop 5.1	7/10/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2857)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2207)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3461)] "General purpose Cryptographic services available for Linux kernel used by Samsung devices to provide secured services."
848	Samsung 129 Samsung-ro Yeongtong-gu Suwon-si, Gyeonggi-do 443-742 South Korea -Changsup Ahn TEL: +82-10-3173-9021 FAX: +82-31-279-1219 -Jisoon Park TEL: +82-10-4556-5007 FAX: +82-31-279-1219	**CryptoCore_Linux** **Version 0.2.9** **Part # NA**	Intel Core i7 w/ Ubuntu 14.04	7/2/2015	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2206)] "A multipurpose cryptographic library which provides symmetric/asymmetric cipher, message digest, key agreement, PRNG and so on."
847	Samsung 129 Samsung-ro Yeongtong-gu Suwon-si, Gyeonggi-do 443-742 South Korea -Changsup Ahn TEL: +82-10-3173-9021 FAX: +82-31-279-1219 -Jisoon Park TEL: +82-10-4556-5007 FAX: +82-31-279-1219	**CryptoCore_Tizen** **Version 0.2.9** **Part # NA**	Samsung Hawk-MU w/ Tizen 2.3	7/2/2015	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2205)] "A multipurpose cryptographic library which provides symmetric/asymmetric cipher, message digest, key agreement, PRNG and so on."
846	SUSE LLC 10 Canal Park, Suite 200 Cambridge, MA 02141 USA -Thomas Biege TEL: +49 911 74053 500 -Michael Hager TEL: +49 911 74053 80	**SUSE NSS Module** **Version 1.0**	Intel x86-64 w/ SUSE Linux Enterprise Server 12	7/2/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2848)] "SUSE Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled client and server applications."

845	OpenSSL Software Foundation Inc. 1829 Mount Ephraim Road Adamstown, MD 27101 USA -Steve Marquess TEL: 877-673-6775	**OpenSSL FIPS Object Module** **Version 2.0.11**	Intel Core 2 Duo (x86) w/ VxWorks 6.7; IBM POWER 7 (PPC) w/ AIX 7.1 64-bit; IBM POWER 7 (PPC) w/ AIX 6.1 32-bit; IBM POWER 7 (PPC) w/ AIX 6.1 64-bit; IBM POWER 7 (PPC) w/ AIX 7.1 32-bit; Intel Xeon E5-2420 (x86) without AES-NI w/ DataGravity Discovery Series OS V2.0; Intel Xeon E5-2420 (x86) with AES-NI w/ DataGravity Discovery Series OS V2.0 ; IBM POWER 7 (PPC) with optimizations w/ AIX 6.1 32-bit; IBM POWER 7 (PPC) with optimizations w/ AIX 6.1 64-bit; Intel Xeon E5-2430L (x86) with AES-NI optimizations w/ Ubuntu 12.04; Intel Xeon E5-2430L (x86) without optimiztions w/ Ubuntu 12.04	7/2/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2847)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2197)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3451)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3451)] "The OpenSSL FIPS Object Module is a full featured general purpose cryptographic library that is distributed in source code form under an open source license. It can be downloaded from www.openssl.org/source/." *08/04/15: Added new tested information;* *09/04/15: Added new tested information;* *10/22/15: Added new tested information;*
844	ViaSat Inc. 6155 El Camino Real Carlsbad, CA 92009 USA -David Suksumrit TEL: 760-476-2306 FAX: 760-929-3941 -Savitha Naik TEL: 760-476-7416 FAX: 760-929-3941	**EbemCrypto** **Version 11 (Firmware)**	IBM PowerPC	7/2/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3448)] "Implements key establishment, random number generation, certificate and private key management, and wrap/unwrap of key material, and controls the FPGA implementation of traffic encryption in ViaSat's Enhanced Bandwidth Efficient Modem (EBEM-500)."
843	FireEye Inc. 1440 McCarthy Boulevard Milipitas, CA 90655 USA -Peter Kim TEL: 1-408-321-6300	**FireEye Algorithms Implementation** **Version 1.0 (Firmware)**	Intel Xeon; AMD Opteron	7/2/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3447)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3447)] "The FireEye Algorithms Implementation provides cryptographic services for CMS and LMS appliances." *07/24/15: Updated vendor information;*
842	Rajant Corporation 400 East King Street Malvern, PA 19355 USA -Martin Lamb TEL: (484) 595-0233 x409	**Firmware v11.4.0-FIPS** **Version 11.4.0-FIPS (Firmware)** **Part # ME4-2409**	Cavium CNS3420	6/26/2015	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (HMAC Val#2194)] "The BreadCrumb by Rajant Corporation is an 802.11 (Wi-Fi) and Ethernet compatible wireless mesh networking device that allows for rapid deployment of mobile wireless networks in a wide variety of environments. It is lightweight, capable of communicating via up to four different radio frequencies, and is designed to be completely mobile."
841	Rajant Corporation 400 East King Street Malvern, PA 19355 USA -Martin Lamb TEL: (484) 595-0233 x409	**Firmware v11.4.0-FIPS** **Version 11.4.0-FIPS (Firmware)** **Part # LX4-2495; LX4-2954**	Intel XScale IXP435	6/26/2015	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (HMAC Val#2193)] "The BreadCrumb by Rajant Corporation is an 802.11 (Wi-Fi) and Ethernet compatible wireless mesh networking device that allows for rapid deployment of mobile wireless networks in a wide variety of environments. It is lightweight, capable of communicating via up to four different radio frequencies, and is designed to be completely mobile."
840	Canon One Canon Park Melville, NY 11747 USA -Jiuyuan Ge TEL: 631-330-5774	**Canon imageRunner Crypto Module for MEAP** **Version 2.1.1**	Intel Atom Processor D410 w/ MontaVista Linux	6/25/2015	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-256) (HMAC Val#2191)] "Canon imageRUNNER Crypto Module for MEAP is a cryptographic module which protects stored and transmitted data using FIPS approved cryptographic algorithms."
839	Dell Inc 5450 Great America Parkway Santa Clara, CA 95054 US -Srihari Mandava	**Dell OpenSSL Cryptographic Library** **Version 2.3**	Intel Atom S1000 w/ Dell Networking Operating System 9.8(0.0); FreeScale PowerPC e500 w/ Dell Networking Operating System 9.8(0.0); Intel Atom C2000 w/ Dell Networking Operating System 9.8(0.0); Broadcom XLP w/ Dell Networking Operating System 9.8(0.0)	6/25/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3440)] BlockCipher_No_df: (, AES-256) (AES Val#3440)] "Dell OpenSSL Cryptographic Library v2.3 provides a variety of cryptographic services used

					by Dell's Data Center hardened Dell Networking OS management and routing features."
838	Cisco Systems Inc. 170 West Tasman Dr. San Jose, CA 95134 USA -Global Certification Team	**Adaptive Security Appliance (ASA) OS** **Version 9.4 (Firmware)**	Intel Atom; Intel Pentium; Intel Core i3; Intel Xeon	6/25/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#2839)] "The Cisco ASA Security Appliance Series delivers robust user and application policy enforcement, multi-vector attack protection, and secure connectivity services in cost-effective, easy-to-deploy solutions. The ASA 5500 Series Adaptive Security Appliances provide comprehensive security, performance, and reliability for network environment."
837	EFJohnson Technologies 1440 Corporate Drive Irving, TX 75038-2401 USA -Marshall Schiring TEL: (402) 479-8375 FAX: (402) 479-8472 -Josh Johnson TEL: (402) 479-8394 FAX: (402) 479-8472	**EFJ JEM2 DRBG** **Version 4.0 (Firmware)**	Texas Instruments TMS320C6400	6/25/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#2838)] "Random determinitic generator used for generating random keys and general encryption."
836	Athena Smartcard Inc. 16615 Lark Ave. Suite 202 Los Gatos, CA 95032 USA -Stéphanie Motré TEL: (408) 884-8316 FAX: (408) 884-8320	**Athena OS755 DRBG Component For SLE78** **Version I1.0 (Firmware)** **Part # SLE78**	Infineon SLE78	6/25/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2835)] "Athena OS755 is a GlobalPlatform Java Card smart card operating system implementing SP 800-90A."
835	Infoblox 3111 Coronado Drive Santa Clara, CA 95054 USA -Bill Lane TEL: 408-986-4000	**NIOS Cryptographic Library** **Version 1.0 (Firmware)**	Intel® Pentium®; Intel® Xeon®	6/25/2015	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1) (HMAC Val#1287)] "Infoblox® NIOS software, coupled with Infoblox appliances, enables customers to deploy large, robust, manageable and cost-effective Infoblox Grids™ to enable distributed delivery of core network services – including DNS, DHCP, IPAM, NTP, TFTP, and FTP."
834	SUSE LLC 10 Canal Park, Suite 200 Cambridge, MA 02141 USA -Thomas Biege TEL: +49 911 74053 500 -Michael Hager TEL: +49 911 74053 80	**Libgcrypt (AVX2 for SHA)** **Version 1.0**	Intel x86-64 w/ SUSE Linux Enterprise Server 12	6/11/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-384 , SHA-512) (SHS Val#2834)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-384 , SHA-512) (HMAC Val#2186)] "SUSE Libgcrypt is a general purpose cryptographic library based on the code from GnuPG."
833	SUSE, LLC 10 Canal Park, Suite 200 Cambridge, MA 02141 USA -Thomas Biege TEL: +49 911 74053 500 -Michael Hager TEL: +49 911 74053 80	**Libgcrypt (AVX for SHA)** **Version 1.0**	Intel x86-64 w/ SUSE Linux Enterprise Server 12	6/11/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-384 , SHA-512) (SHS Val#2833)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-384 , SHA-512) (HMAC Val#2185)] "SUSE Libgcrypt is a general purpose cryptographic library based on the code from GnuPG."
832	SUSE LLC 10 Canal Park, Suite 200 Cambridge, MA 02141 USA -Thomas Biege TEL: +49 911 74053 500 -Michael Hager TEL: +49 911 74053 80	**Libgcrypt (Assembler for AES and SSSE3 for SHA)** **Version 1.0**	Intel x86-64 w/ SUSE Linux Enterprise Server 12	6/11/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2832)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2184)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3434)] "SUSE Libgcrypt is a general purpose cryptographic library based on the code from GnuPG."
831	SUSE LLC 10 Canal Park, Suite 200 Cambridge, MA 02141 USA -Thomas Biege TEL: +49 911 74053 500	**Libgcrypt (AES-NI and C implementation for SHA)** **Version 1.0**	Intel x86-64 w/ SUSE Linux Enterprise Server 12	6/11/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2831)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2183)] **CTR_DRBG**: [Prediction Resistance Tested:

	-Michael Hager TEL: +49 911 74053 80				Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3433)] "SUSE Libgcrypt is a general purpose cryptographic library based on the code from GnuPG."
830	RSA, The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Sandy Carielli TEL: 781-515-7510	**RSA BSAFE Crypto-C Micro Edition (ME)** **Version 3.0.0.25**	ARM11 MPCore (ARMv6k) w/ VxWorks 6.8.2	6/11/2015	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2181)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#688) (SHS Val#2829) "RSA BSAFE® Crypto-C ME software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. The software supports a wide range of industry standard encryption algorithms offering developers the flexibility to choose the appropriate option to meet their requirements."
829	Hewlett-Packard Company 1160 Enterprise Way Sunnyvale, CA 94089 USA -Harjit Dhillon TEL: 916-501-1426	**HP ESKM DRBG** **Version 6.0.1 DRBG 1.1 (Firmware)**	Intel Xeon E5-2600 Family	6/11/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3428)] "HP Enterprise Secure Key Manager (ESKM) provides key generation, retrieval, and management for encryption devices and solutions. ESKM is a hardened security appliance with secure access control, administration, and logging. ESKM supports high availability with automatic multi-site clustering, replication, and failover."
828	Hewlett-Packard Company 1160 Enterprise Way Sunnyvale, CA 94089 USA -Harjit Dhillon TEL: 916-501-1426	**HP ESKM OpenSSL** **Version 6.0.1 OpenSSL 1.1 (Firmware)**	Intel Xeon E5-2600 Family	6/11/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3428)] "HP Enterprise Secure Key Manager (ESKM) provides key generation, retrieval, and management for encryption devices and solutions. ESKM is a hardened security appliance with secure access control, administration, and logging. ESKM supports high availability with automatic multi-site clustering, replication, and failover."
827	Hewlett-Packard Company 1160 Enterprise Way Sunnyvale, CA 94089 USA -Harjit Dhillon TEL: 916-501-1426	**HP ESKM DRBG** **Version 6.0.0 DRBG 1.0 (Firmware)**	Intel Xeon E5-2600 Family	6/11/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3427)] "HP Enterprise Secure Key Manager (ESKM) provides key generation, retrieval, and management for encryption devices and solutions. ESKM is a hardened security appliance with secure access control, administration, and logging. ESKM supports high availability with automatic multi-site clustering, replication, and failover."
826	Hewlett-Packard Company 1160 Enterprise Way Sunnyvale, CA 94089 USA -Harjit Dhillon TEL: 916-501-1426	**HP ESKM OpenSSL** **Version 6.0.0 OpenSSL 1.0 (Firmware)**	Intel Xeon E5-2600 Family	6/11/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3427)] "HP Enterprise Secure Key Manager (ESKM) provides key generation, retrieval, and management for encryption devices and solutions. ESKM is a hardened security appliance with secure access control, administration, and logging. ESKM supports high availability with automatic multi-site clustering, replication, and failover."
825	Thales e-Security Inc. 900 South Pine Island Road Suite 710 Plantation, FL 33324 USA -sales@thalesesec.com TEL: 888-744-4976	**nShield Algorithm Library** **Version 2.61.2 (Firmware)**	Freescale PowerPC	6/5/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3420)] "The nShield algorithm library provides cryptographic functionality for Thales nShield Hardware Security Modules." *10/22/15: Updated implementation information;*
824	Thales e-Security Inc. 900 South Pine Island Road Suite 710	**MiniHSM Algorithm Library** **Version 2.61.2 (Firmware)**	Freescale DragonBall MXL	6/5/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3419)]

	Plantation, FL 33324 USA -sales@thalesesec.com TEL: 888-744-4976				"The MiniHSM Algorithm Library provides cryptographic functionality for the MiniHSM series of Thales hardware security modules." *10/22/15: Updated implementation information;*
823	Check Point Software Technologies 5 Ha'solelim Street Tel Aviv, 67897 Israel -Malcolm Levy TEL: +972-37534561	**Check Point Cryptographic Library** **Version 1.0 (Firmware)**	Intel® Xeon®	6/5/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2824)] "Cryptographic library for Check Point Next Generation Security Appliances"
822	3e Technologies International Inc. 9715 Key West Ave Suite 500 Rockville, MD 22852 USA -Harinder Sood TEL: 301-944-1325 FAX: 301-670-6779 -Chris Guo TEL: 301-944-1294 FAX: 301-670-6779	**3eTI OpenSSL Algorithm Implementation** **Version 1.0.1-a (Firmware)**	MPC8378E	6/5/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1801)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#1253)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2060)] "Algorithms listed are used to provide encryption and authentication services within 3eTI networking products."
821	wolfSSL Inc. 10016 Edmonds Way Suite C-300 Edmonds, WA 98020 USA -Todd Ouska TEL: 503-679-1859 -Larry Stefonic TEL: 206-369-4800	**wolfCrypt** **Version 3.6.0**	Qualcomm Krait 400 as on Samsung Galaxy S5 w/ Android 4.4	6/5/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2823)] "WolfCrypt module is a comprehensive suite of FIPS Approved algorithms. All key sizes and modes have been implemented to allow flexibility and efficiency." *10/20/15: Updated implementation information;*
820	Motorola Solutions Inc. 1301 East Algonquin Road Schaumburg, IL 60196 USA -Tom Nguyen TEL: 847-576-2352	**Motorola Solutions Subscriber µMace DRBG_SP800-90A** **Version APX_ UMACE_ DRBG_ SP800-90A_ R01.00.00 (Firmware)**	Motorola µMace AT8358Z04 (Atmel Manufactured, Family of Motorola µMace AT58Z04)	6/5/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#3414)] "DRBG/SP800-90A implementation for the µMace cryptographic processor which is used in security modules embedded in Motorola Solutions security products."
819	Cavium Inc. 2315 N. First Street San Jose, CA 95131 USA -Tasha Castaneda TEL: 650-218-9914 -Steve Klinger TEL: 408-943-7375	**Octeon III Family Crypto Engine** **Part # CN7010/ CN7020/ CN7120/ CN7125/ CN7130/ CN7760/ CN7770/ CN7870/ CN7880/ CN7890; -AAP, -CP, -SCP options**	N/A	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3301)] "The Cavium OCTEON family of Multi-Core MIPS64 processors has 1 to 48 cores per chip. They integrate next-generation networking I/Os with advanced security, storage, and application hardware acceleration, offering unprecedented throughput and programmability for Layer 2 through Layer 7 processing of intelligent networks."
818	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team TEL: d	**CiscoSSL FIPS Object Module** **Version 6.0**	Cavium Octeon MIPS64 w/ Linux 2.6; Intel Xeon w/ FreeBSD 9.2	5/22/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2818)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2173)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3405)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3405)] "The Cisco FIPS Object Module is a software library that provides cryptographic services to a vast array of" *06/01/15: Added new tested information;*
817	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team TEL: d	**CiscoSSL FIPS Object Module (Assembler)** **Version 6.0**	Intel Xeon w/ Linux 2.6; Cavium Octeon MIPS64 w/ Linux 2.6; ARMv7 w/ Android 4.4; Intel Core i7 w/ Windows 8.1; Intel Core i7 with AES-NI w/ Windows 8.1	5/22/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2817)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2172)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3404)]

					BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3404)] "The Cisco FIPS Object Module is a software library that provides cryptographic services to a vast array of Cisco's networking and collaboration products." *06/01/15: Updated implementation information;*
816	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (Assembler AES, Core M)** **Version 5.0**	Core M w/ OSX 10.10	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3382)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and assembler optimized AES."
815	Dell Software Inc. 5455 Great America Parkway Santa Clara, CA 95051 USA -Usha Sanagala TEL: 408-962-6248 FAX: 408-745-9300	**SonicOS 6.2.1 for SM9800** **Version 6.2.1 (Firmware)**	Cavium Octeon II CN 6640-8core	5/22/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2816)] "The Dell(tm) SonicWALL(tm) SuperMassive(tm) Series is Dell's next-generation firewall (NGFW) platform designed for large networks to deliver scalability, reliability and deep security at multi-gigabit speeds with near zero latency."
814	Hewlett-Packard Development Company L.P. 11445 Compaq Center Dr. W Houston, TX 77070 USA -Luis Luciani TEL: 281-518-6762	**iLO SSL Firmware Crypto Library** **Version 2.11 (Firmware)**	ARM-926	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_No_df: (AES-128) (AES Val#3400)] "The HP Integrated Lights-Out 4 (HP iLO 4) built into HP ProLiant Gen8 and Gen9 servers is an autonomous secure management component embedded directly on the server motherboard. iLO SSL Firmware Crypto Library provides the cryptographic operations required for secure communication and management."
813	HyTrust Inc 1975 West El Camino Real Suite # 203 Mountain View, CA 94040 USA -Steve Pate TEL: (916)705-8610	**DRBG** **Version OpenSSL 1.0.1m and OpenSSL FIPS 2.0.9** **Part # Intel Xeon E3-1241 v3**	FreeBSD 9.2 and VMware vSphere Hypervisor (ESXi) 5.5.0u2 w/ FreeBSD 9.2	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3397)] "HyTrust KeyControl is a secure, active-active key management cluster used for creation, management and delivery of encryption keys to physical and virtual machines where files and data drives are encrypted." *07/28/15: Updated implementation information;*
812	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Generic, Core M)** **Version 5.0**	Core M w/ OSX 10.10	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3395)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
811	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Generic, Core M 32bit)** **Version 5.0**	Core M w/ OSX 10.10	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3394)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
810	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (AES-NI with optimized modes, Core M)** **Version 5.0**	Core M w/ OSX 10.10	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3393)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
809	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (AES-NI with optimized modes, CoreM 32bit)** **Version 5.0**	Core M w/ OSX 10.10	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3392)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS compiled for 32bit word size."

808	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Assembler AES, Core M)** **Version 5.0**	Core M w/ OSX 10.10	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3389)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
807	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Assembler AES, Core M 32bit)** **Version 5.0**	Core M w/ OSX 10.10	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3387)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES compiled for 32bit word size."
806	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (Generic, Core M)** **Version 5.0**	Core M w/ OSX 10.10	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3385)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
805	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (AES-NI w/ optimized modes, Core M)** **Version 5.0**	Core M w/ OSX 10.10	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3384)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
804	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A8X)** **Version 5.0**	Apple A8X w/ iOS 8	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3381)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
803	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Kernel Module (Generic, A8X)** **Version 5.0**	Apple A8X w/ iOS 8	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3380)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
802	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A8X 32bit)** **Version 5.0**	Apple A8X w/ iOS 8	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3379)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software compiled for 32bit word size."
801	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A8X)** **Version 5.0**	Apple A8X w/ iOS 8	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3377)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
800	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A8X 32bit)** **Version 5.0**	Apple A8X w/ iOS 8	5/22/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3376)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES compiled for 32bit word size."
799	HP Security Voltage 20400 Stevens Creek Blv Suite 500 Cupertino, CA 95014 USA -Luther Martin TEL: (408) 886 - 3200 FAX: (408) 886 - 3201	**Voltage Cryptographic Module v.5.0** **Version 5.0**	Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz w/ Windows Server 2012 R2 w/o AES-NI	5/22/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256 , SHA-512) (SHS Val#2794)] "The Voltage Cryptographic Module provides the validated algorithms used by the HP SecureMail, HP SecureFile and HP SecureData families of products."

798	HP Security Voltage 20400 Stevens Creek Blv Suite 500 Cupertino, CA 95014 USA -Luther Martin TEL: (408) 886 - 3200 FAX: (408) 886 - 3201	**Voltage Cryptographic Module v.5.0** **Version 5.0**	Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz w/ Windows Server 2012 R2 with AES-NI	5/22/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256 , SHA-512) (SHS Val#2793)] "The Voltage Cryptographic Module provides the validated algorithms used by the HP SecureMail, HP SecureFile and HP SecureData families of products."
797	HP Security Voltage 20400 Stevens Creek Blv Suite 500 Cupertino, CA 95014 USA -Luther Martin TEL: (408) 886 - 3200 FAX: (408) 886 - 3201	**Voltage Cryptographic Module v.5.0** **Version 5.0**	Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz w/ CentOS w/o AES-NI	5/22/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256 , SHA-512) (SHS Val#2792)] "The Voltage Cryptographic Module provides the validated algorithms used by the HP SecureMail, HP SecureFile and HP SecureData families of products."
796	HP Security Voltage 20400 Stevens Creek Blv Suite 500 Cupertino, CA 95014 USA -Luther Martin TEL: (408) 886 - 3200 FAX: (408) 886 - 3201	**Voltage Cryptographic Module v.5.0** **Version 5.0**	Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz w/ CentOS with AES-NI	5/15/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256 , SHA-512) (SHS Val#2791)] "The Voltage Cryptographic Module provides the validated algorithms used by the HP SecureMail, HP SecureFile and HP SecureData families of products."
795	Cardiocom LLC 7980 Century Blvd. Chanhassen, MN 55317 USA -Brian Golden TEL: 888-243-8881	**CC AM1** **Version CC AM1 v1.0.0**	Intel Xeon E5620 w/ Windows 2008 R2 x64	5/15/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3349)] "CC AM 1 supports the FIPS module CC FM TLS/SRTP 1.0 which facilitates secure communication for the TLS and SRTP protocols."
794	Cardiocom LLC 7980 Century Blvd. Chanhassen, MN 55317 USA -Brian Golden TEL: 888-243-8881	**CC AM1** **Version CC AM1 v1.0.0**	Texas Instruments OMAP4430 2X ARM Cortex A9 MP Core w/ Android 4.0.4	5/15/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3349)] "CC AM 1 supports the FIPS module CC FM TLS/SRTP 1.0 which facilitates secure communication for the TLS and SRTP protocols."
793	Security First Corporation 29811 Santa Margarita Parkway Suite 600 Rancho Santa Margarita, CA 92688 USA -Rick Orsini TEL: 949-858-7525 FAX: 949-858-7092	**Secure Parser Library** **Version 4.7.1.0**	Qualcomm Snapdragon 800 series (ARMv7) w/ Android 4.4; Qualcomm Snapdragon 800 series (ARMv7) w/ Android 5.0; Intel Core i5 (3rd Gen) with AES-NI disabled w/ Microsoft Windows 7 64-bit; Intel Core i5 (3rd Gen) with AES-NI w/ Microsoft Windows 7 64-bit; AMD E1 with AES-NI disabled w/ Microsoft Windows 8 64-bit; AMD E1 with AES-NI w/ Microsoft Windows 8 64-bit	5/15/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3365)] "The Secure Parser Library is a suite of general security routines using FIPS Approved algorithms for its cryptography. An AES key size of 256 bits and equivalent key sizes for all other algorithms are supported by the library."
792	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Andy Nissen TEL: 651-770-6151	**McAfee Advanced Threat Defense** **Version 3.4.6**	Intel x86_64 w/ Linux 3.10.45	5/15/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3364)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3364)] "OpenSSL FIPS Object Module 2.0.5 running on Linux 3.10.45 on Intel x86_64 HW"
791	Oracle Communications 100 Crosby Drive Bedford, MA 01730 USA -Nikhil Suares TEL: 781-538-7568 -Madhu Mathiyalagan TEL: 781-538-7514	**Acme Packet Cryptographic Library** **Version EC6.4.1M1 (Firmware)**	Intel Core Duo T2500; Intel Celeron M 440; Intel Celeron M 440	5/15/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1) (SHS Val#2788)] "The Acme Packet 3820 and 4500 are one rack unit (1U) platforms that feature Oracle's purpose-built hardware design tightly integrated with Acme Packet OS, to provide the critical controls for delivering trusted, real-time communications - voice, video, and application data sessions - across Internet Protocol (IP) network borders"
790	LogRhythm 4780 Pearl East Circle Boulder, CO 80301 USA -Emily Dobson TEL: 720-881-5348	**LogRhythm OpenSSL** **Version 6.3.4**	Intel Xeon E5-2420 w/ Microsoft Windows Server 2008 R2	5/15/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2787)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2142)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3363)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3363)]

					"This module provides support for secure communications over a network using the OpenSSL library."
789	Northop Grumman M5 Network Security Level 1 218 Northbourne Avenue Braddon, ACT 2612 Australia -Warwick Hoyle TEL: +611300656019 FAX: +611300365893 -Kristian Howard TEL: +611300656019 FAX: +611300365893	**SCS Java Cryptographic Services** **Version SCS-100 (Firmware 23)**	Intel(R) Atom(TM) CPU E660 @ 1.30GHz w/ SCS-100 (v5.3.6); Intel(R) Atom(TM) CPU Z510 @ 1.10GHz w/ SCS-100 (v5.3.6)	5/8/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2784)] "A module that provides a Java-language application program interface (API) for use by other processes that require cryptographic functionality within the SCS 100 and 200 hardware platforms"
788	Brocade Communications Systems, Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**Brocade FIPS Crypto Library** **Version 5.0.1 (Firmware)**	E500mc	5/8/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2937)] "Brocade cryptographic library is used in Brocade NOS based switches to implement the cryptographic related modules." *10/09/15: Updated implementation information;*
787	IBM 9000 S. Rita Rd. Tucson, AZ 85744 USA -Christine Knibloe TEL: (412) 977-9398	**TS1150 Cryptographic Firmware Library** **Version 38L7468 (Firmware)**	PPC 405	5/8/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#2783)] "Firmware cryptographic implementation that adds secure key channel capabilities to the IBM TS1150." *06/23/15: Updated vendor informaton;*
786	Ultra Electronics AEP Knaves Beech Business Centre Loudwater, High Wycombe, Buckinghamshire HP10 9UT United Kingdom -Paul Kettlewell TEL: +44 (0)1628 642624 -Vicky Hayes TEL: +44 (0)1628 642623	**Advanced Configurable Crypto Environment v3** **Version 011395 v2 r4 (Firmware)**	P2020 QorIQ	5/8/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256 , SHA-512) (SHS Val#2782)] "The Ultra Electronics AEP Advanced Configurable Crypto Environment v3 (ACCEv3) provides highly secure cryptographic services and key storage. It is the foundation of a range of products including the Keyper Plus."
785	Juniper Networks Inc. 1194 North Mathilda Ave. Sunnyvale, CA 94089 USA -Scott Mckinnon	**Junos FIPS Version 12.1 X46 - OpenSSL** **Version 12.1 X46 D20.6 (Firmware)**	Cavium Octeon CN5645 w/ internal accelerators (HW/FW);Cavium Octeon CN5020 w/ internal accelerators (HW/FW) w/ Junos FIPS Version 12.1 X46 D20.6; Cavium Octeon CN5230 w/ internal accelerators (HW/FW) w/ Junos FIPS Version 12.1 X46 D20.6; Cavium Octeon CN6335 w/ internal accelerators (HW/FW) w/ Junos FIPS Version 12.1 X46 D20.6; Cavium Octeon CN5645 w/ internal accelerators (HW/FW) w/ Junos FIPS Version 12.1 X46 D20.6; Intel Celeron w/ Broadcom XLR accelerator (HW/FW) w/ Junos FIPS Version 12.1 X46 D20.6; Intel Celeron w/ Broadcom XLR accelerator (HW/FW) w/ Junos FIPS Version 12.1 X46 D20.6; Intel Celeron w/ Broadcom XLP accelerator (HW/FW) w/ Junos FIPS Version 12.1 X46 D20.6	5/8/2015	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256) (HMAC Val#2136)] "Juniper Networks, Inc. JUNOS 12.1 X46 for SRX and LN Series Platforms supports the definition of and enforces information flow policies among network nodes. The routers provide for stateful inspection of every packet that traverses the network and provide central management to manage the network security policy."
784	Nimble Storage Inc. 211 River Oaks Parkway San Jose, CA 95134 USA -Kent Peacock TEL: +1-408-514-3452	**Nimble Storage OpenSSL FIPS Object Module** **Version 2.0.9**	Intel ES-2403V2 with AES-NI w/ Linux 2.6; Intel ES-2450V2 with AES-NI w/ Linux 2.6; Intel ES-2470V2 with AES-NI w/ Linux 2.6	5/8/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2778)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2134)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3351)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3351)] "The Nimble Storage OpenSSL FIPS Object Module is a general purpose cryptographic module compiled from the source code for the OpenSSL FIPS Object Module 2.0.9. It is incorporated into the family of Nimble Storage appliances."
783	Dell Inc 5450 Great America Parkway	**Dell OpenSSL Cryptographic Library**	Intel Atom C2000 w/ Dell Networking Operating System 9.8(0.0); Intel Atom	5/8/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (

	Santa Clara, CA 95054 US -Srihari Mandava	**Version 2.2**	S1000 w/ Dell Networking Operating System 9.8(0.0); Broadcom XLP w/ Dell Networking Operating System 9.8(0.0); FreeScale PowerPC e500 w/ Dell Networking Operating System 9.8(0.0)		AES-256) (AES Val#3350)] BlockCipher_No_df: (, AES-256) (AES Val#3350)] "Dell OpenSSL Cryptographic Library v2.2 provides a variety of cryptographic services used by Dell's Data Center hardened Dell Networking OS management and routing features."
782	Information Assurance Specialists Inc 900 Route 168 Suite C4 Turnersville, NJ 08012 USA -Nicholas Podolak TEL: 856-581-8033	**IAS Router FIPS** **Version IASRouter-2015-06-10_23s36eb (Firmware)**	Intel Bay Trail with AES-NI	6/11/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3430)] "IAS Router FIPS is a comprehensive suite of FIPS Approved algorithms. All key sizes and modes have been implemented to allow flexibility and efficiency."
781	Samsung Electronics Co., Ltd. 416, Maetan 3-Dong Youngton Gu Suwon, Gyeonggi 152-848 South Korea -Abraham Joseph Kang TEL: +1-408-324-3678 FAX: +1-408-324-3640 -Bumhan Kim TEL: +82-10-4800-6711	**Samsung SCrypto** **Version 1.0**	Samsung Electronics Exynos 7420 w/ MOBICORE Tbase 302A	4/17/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2773)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2129)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3339)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3339)] "Provide general purpose cryptographic services to TrustZone applications on the mobile platform for the protection of data in transit."
780	Hewlett-Packard Development Company L.P. 11445 Compaq Center Dr. W Houston, TX 77070 USA -Ramesh Narayanan TEL: +91 80 338 65384 -Rituparna Mitra TEL: +91 80 251 65735	**HP BladeSystem Onboard Administrator Firmware** **Version 4.40 (Firmware)**	PowerPC 440EPX processor	4/17/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-256) (AES Val#3333)] BlockCipher_No_df: (AES-128 , AES-256) (AES Val#3333)] "The module provides administrative control of HP BladeSystem c-Class enclosures. The cryptographic functions of the module provide security for administrative access via HTTPS and SSH, and to administrative commands for the BladeSystem enclosure."
779	Senetas Corporation Ltd. and SafeNet Inc. 312 Kings Way South Melbourne, Victoria 3025 Australia -John Weston TEL: +61 3 9868 4555 FAX: +61 3 9821 4899	**CN6000 Series Common Crypto Library** **Version 2.6.1 (Firmware)**	Intel ATOM	4/17/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2772)] "The CN6000 Series Common Crypto Library Module provides FIPS 140-2 approved cryptographic algorithms for CN6000 Series Encryptors. Based upon OpenSSL the Common Crypto Library provides an Application Programming Interface (API) to support security relevant services." *06/08/15: Updated implementation information;*
778	Senetas Corporation Ltd. and SafeNet Inc. 312 Kings Way South Melbourne, Victoria 3025 Australia -John Weston TEL: +61 3 9868 4555 FAX: +61 3 9821 4899	**CN1000 and CN3000 Series Common Crypto Library** **Version 4.6.1 (Firmware)**	Freescale MPC8280	4/17/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2771)] "The CN1000 and CN3000 Series Common Crypto Library Module provides FIPS 140-2 approved cryptographic algorithms for the CN1000 and CN3000 Series Encryptors. Based upon OpenSSL the Library provides an Application Programming Interface (API) to support security relevant services." *06/08/15: Updated implementation information;*
777	Senetas Corporation Ltd. and SafeNet Inc. 312 Kings Way South Melbourne, Victoria 3025 Australia -John Weston TEL: +61 3 9868 4555 FAX: +61 3 9821 4899	**CN4010 and CN6010 Series Common Crypto Library** **Version 2.6.1 (Firmware)**	ARM Cortex A9	4/17/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2770)] "The CN4010 and CN6010 Series Common Crypto Library Module provides FIPS 140-2 approved cryptographic algorithms for the CN4010 and CN6010 Series Encryptors. Based upon OpenSSL the Library provides an Application Programming Interface (API) to support security relevant services." *06/08/15: Updated implementation information;*
776	Hewlett-Packard Development	**HP BladeSystem c-Class Virtual Connect**	Freescale MPC8347 Processor; Freescale	4/17/2015	**CTR_DRBG**: [Prediction Resistance Tested:

	Company L.P. 11445 Compaq Center Dr. W Houston, TX 77070 USA -Julie Ritter TEL: (281) 514-4087	**Library** **Version 4.41 (Firmware)**	MPC8535 Processor		Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3334)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3334)] "The HP BladeSystem is a rack-mount enterprise-class computing infrastructure designed to maximize power while minimizing costs, saving up to 56% of the total cost of ownership compared to traditional infrastructures."
775	wolfSSL Inc. 10016 Edmonds Way Suite C-300 Edmonds, WA 98020 USA -Todd Ouska TEL: 503-679-1859 -Larry Stefonic TEL: 206-369-4800	**wolfCrypt** **Version 3.6.0**	Apple(tm) A8 as on iPhone(tm) 6 w/ iOS 8.1	4/17/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2763)] "WolfCrypt module is a comprehensive suite of FIPS Approved algorithms. All key sizes and modes have been implemented to allow flexibility and efficiency." *04/29/15: Updated implementation information; 10/20/15: Updated implementation information;*
774	Sony Mobile Communications Inc. 1-8-15 Kohnan Minato-ku, Tokyo 108-0075 Japan -Takuya Nishibayashi TEL: +81-3-5782-5285 FAX: +81-3-5782-5258	**Xperia Cryptographic Module DRBG Component** **Version 1.0.0**	Qualcomm Snapdragon 810 (ARMv8) with Cryptographic Instructions w/ Android 5.0;Qualcomm Snapdragon 810 (ARMv8) without Cryptographic Instructions w/ Android 5.0	4/17/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2762)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2120)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3329)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3329)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#658) (SHS Val#2762) "Xperia Cryptographic Module DRBG Component provides cryptographic service for Android mobile device." *05/19/15: Updated implementation information;*
773	Feitian Technologies Co., Ltd Floor 17, Tower B, Huizhi Mansion, No.9 Xueqing Road Haidian, Beijing 100085 China -PENG Jie TEL: +8610 62304466-419 FAX: +8610 62304477 -WenSheng Ju TEL: +8610 62304466-527 FAX: +8610 62304477	**DRBG** **Part # SLE 78CLUFX**	N/A	4/10/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: [3KeyTDES (TDES Val#1899))] "The Physical True Random Number Generator module and Symmetric Crypto Processor are used for DRBG processing."
772	Accellion Inc. 1804 Embarcadero Road Suite 200 Palo Alto, Ca 94303 USA -Prateek Jain TEL: 65-62445670 FAX: 65-62445678	**OpenSSL Object Module** **Version 1.0.1**	Intel Xeon QuadCore w/ Red Hat Enterprise Linux 5	4/10/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3326)] "Accellion Cryptographic Module is a key component of Accellion's secure collaboration solution that enables enterprises to securely share and transfer files. Extensive tracking and reporting tools allow compliance with SOX, HIPAA, FDA and GLB regulations while providing enterprise grade security and ease of use."
771	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (Generic, Xeon)** **Version 5.0**	Intel Xeon w/ OSX 10.10	4/10/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3325)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
770	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (Generic, i7)** **Version 5.0**	Intel i7 w/ OSX 10.10	4/10/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3324)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."

769	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (Generic, i5)** **Version 5.0**	Intel i5 w/ OSX 10.10	4/10/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3323)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
768	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Kernel Module (Generic, A8)** **Version 5.0**	Apple A8 w/ iOS 8	4/10/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3322)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
767	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Kernel Module (Generic, A7)** **Version 5.0**	Apple A7 w/ iOS 8	4/10/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3321)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
766	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Kernel Module (Generic, A6X)** **Version 5.0**	Apple A6X w/ iOS 8	4/10/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3320)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
765	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Kernel Module (Generic, A6)** **Version 5.0**	Apple A6 w/ iOS 8	4/10/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3319)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
764	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Kernel Module (Generic, A5X)** **Version 5.0**	Apple A5X w/ iOS 8	4/10/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3318)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
763	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Kernel Module (Generic, A5)** **Version 5.0**	Apple A5 w/ iOS 8	4/10/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3317)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
762	Oracle Communications 100 Crosby Drive Bedford, MA 01730 USA -Nikhil Suares TEL: (781) 538-7568 -Madhu Mathiyalagan TEL: (781) 538-7514	**Acme Packet Cryptographic Library** **Version EC6.4.1 (Firmware)**	Intel Core Duo T2500; Intel Celeron M 440; Intel Core Duo T9400	3/27/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1) (SHS Val#2748)] "The Acme Packet 3820 and 4500 are one rack unit (1U) platforms that feature Oracle's purpose-built hardware design tightly integrated with Acme Packet OS, to provide the critical controls for delivering trusted, real-time communications - voice, video, and application data sessions - across Internet Protocol (IP) network borders."
761	Samsung Electronics Co. Ltd R4 416, Maetan 3-dong, Yeongtong-gu Suwon-si, Gyeonggi-do 443-742 Korea -Brian Wood TEL: 908-809-7939 FAX: 908-809-7974	**Samsung OpenSSL - Galaxy S6** **Version OpenSSL 1.0.1j**	System LSI Exynos 7420 w/ Android 5.0.2	3/27/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2747)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2106)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3314)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3314)] "General purpose cryptographic services available for Android used by Samsung devices to provide secure cryptography."

760	Samsung Electronics Co. Ltd R4 416, Maetan 3-dong, Yeongtong-gu Suwon-si, Gyeonggi-do 443-742 Korea -Brian Wood TEL: 908-809-7939 FAX: 908-809-7974	**Samsung OpenSSL - Note 4** **Version OpenSSL 1.0.1j**	Qualcomm Snapdragon 805 w/ Android 5.0.1	3/27/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2746)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2105)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3313)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3313)] "General purpose cryptographic services available for Android used by Samsung devices to provide secure cryptography."
759	IBM Internet Security Systems 6303 Barfield Road Atlanta, GA 30328 USA -Ferrell Moultrie TEL: (678) 234-4069 -Kim Barnes TEL: (404) 238-6024	**XGS 7100** **Version 5.3**	Intel Xeon E5-2658v2 w/ RHEL 6.3 Linux	3/27/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2743)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2102)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3310)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3310)] "IBM Security Network Protection is designed to protect your business critical network infrastructure through a unique combination of threat protection, visibility and control. IBM extends the abilities of traditional intrusion prevention systems by offering a next-generation solution that provides visibility and control over their network."
758	IBM Internet Security Systems 6303 Barfield Road Atlanta, GA 30328 USA -Ferrell Moultrie TEL: (678) 234-4069 -Kim Barnes TEL: (404) 238-6024	**XGS 5100** **Version 5.3**	Intel Core i7-2600 w/ RHEL 6.3 Linux	3/27/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2742)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2101)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3309)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3309)] "IBM Security Network Protection is designed to protect your business critical network infrastructure through a unique combination of threat protection, visibility and control. IBM extends the abilities of traditional intrusion prevention systems by offering a next-generation solution that provides visibility and control over their network."
757	IBM Internet Security Systems 6303 Barfield Road Atlanta, GA 30328 USA -Ferrell Moultrie TEL: (678) 234-4069 -Kim Barnes TEL: (404) 238-6024	**XGS 4100** **Version 5.3**	Intel Core i3-2115C w/ RHEL 6.3 Linux	3/27/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2741)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2100)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3308)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3308)] "IBM Security Network Protection is designed to protect your business critical network infrastructure through a unique combination of threat protection, visibility and control. IBM extends the abilities of traditional intrusion prevention systems by offering a next-generation solution that provides visibility and control over their network."
756	IBM Internet Security Systems 6303 Barfield Road Atlanta, GA 30328 USA -Ferrell Moultrie TEL: (678) 234-4069	**XGS 3100** **Version 5.3**	Intel Pentium B915C w/ RHEL 6.3 Linux	3/27/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2740)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC

	-Kim Barnes TEL: (404) 238-6024				Val#2099)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3307)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3307)] "IBM Security Network Protection is designed to protect your business critical network infrastructure through a unique combination of threat protection, visibility and control. IBM extends the abilities of traditional intrusion prevention systems by offering a next-generation solution that provides visibility and control over their network."
755	Hagiwara Solutions Co. Ltd. 2-5-12 Nishiki Naka-ku, Nagoya, Aichi 460-0003 Japan -Yoshihiro Kito TEL: +81-53-455-6700 FAX: +81-53-455-6701 -Masaki Takikawa TEL: +81-53-455-6700 FAX: +81-53-455-6701	**Dyakon Crypto Engine - Hash_DRBG** **Version 1.0 (Firmware)**	HS310S-FI	3/27/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256) (SHS Val#2732)] "The Dyakon Crypto Engine is a cryptographic library including the hardware-based data encryption and decryption engine. This cryptographic engine provides the secure data protection and the secure key management found in Hagiwara Solutions storage products."
754	Redpine Signals Inc. 2107 North First Street Suite #680 San Jose, CA 95131-2019 USA -Mallik Reddy TEL: +1 408 219 7868 FAX: +1 408 705 2019	**RSICryptoLib** **Version RSICryptoLib_1_0 (Firmware)** **Part # Redpine ThreadArch**	N/A	3/27/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2628)] "Algorithm routines implemented in RSICryptoLib"
753	IBM Corporation 80 Bishop Dr., Unit B Fredericton, New Brunswick E3C 1B2 Canada -Peter Clark TEL: (416) 478-0224 -Chris LeMesurier TEL: (416) 478-0224	**Cryptographic Security Kernel** **Version 1.0**	Intel Xeon w/ RHEL 6	3/27/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3131)] "The IBM Cryptographic Security Kernel is a multi-algorithm library providing general-purpose cryptographic services. The module provides a single, FIPS-Approved API for cryptography allowing for centralized FIPS mode status, logging, and reporting."
752	Juniper Networks Inc. 1194 North Mathilda Ave. Sunnyvale, CA 94089 USA -Balachandra Shanabhag TEL: +91 8061214260	**OpenSSL Crypto Lib** **Version Junos 14.1R4 (Firmware)**	Intel LC5500 and LC3500 Jasper Forest family; Intel L52xx Wolfdale family	3/20/2015	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2094)] "Comprehensive, scalable and secure switching & routing solutions specifically designed to meet the needs of campus, enterprises and service providers. All of our switches & routers - core, Multiservice edge and edge Ethernet - run on one common operating system- Junos." *03/27/15: Update implementation information;*
751	Juniper Networks, Inc. 1194 North Mathilda Ave. Sunnyvale, CA 94089 USA -Balachandra Shanabhag TEL: +91 8061214260	**Authentec (Quicksec)** **Version Junos 14.1R4 (Firmware)**	Intel LC5500 and LC3500 Jasper Forest family; Intel L52xx Wolfdale family	3/20/2015	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1) (HMAC Val#2091)] "Comprehensive, scalable and secure switching & routing solutions specifically designed to meet the needs of campus, enterprises and service providers. All of our switches & routers - core, Multiservice edge and edge Ethernet - run on one common operating system- Junos." *03/27/15: Updated implementation information;*
750	Samsung Electronics Co. Ltd R4 416, Maetan 3-dong, Yeongtong-gu Suwon-si, Gyeonggi-do 443-742 Korea -Kyung-Hee Lee TEL: +82-10-9397-1589	**Samsung Kernel Cryptographic Module** **Version SKC1.6**	ARMv8 w/ Android Lollipop 5.0.2	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2731)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2090)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3292)] "General purpose Cryptographic services available for Linux kernel used by Samsung devices to provide secured services."
749	LG Electronics Inc.	**LG OpenSSL**	Qualcomm Snapdragon 800-series w/	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance

	20 Yoido-dong Youngdungpo-gu Seoul, n/a 152-721 Republic of Korea -Joonwoong Kim TEL: 82-10-2207-1919 FAX: 82-2-6950-2080 -Adam Wick TEL: 503-808-7216 FAX: 503-350-0833	**Version 1.0.1h**	Android 5.0.1; Qualcomm Snapdragon 800-series (64-bit) w/ Android 5.0.1		Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2730)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2089)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3291)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3291)] "General-purpose cryptographic services available for Android used by LG devices to provide secured services to applications via the OpenSSL FIPS Object Module, which is a full featured general purpose cryptographic library." *06/25/15: Added new tested information;*
748	LG Electronics Inc. 20 Yoido-dong Youngdungpo-gu Seoul, n/a 152-721 Republic of Korea -Joonwoong Kim TEL: 82-10-2207-1919 FAX: 82-2-6950-2080 -Adam Wick TEL: 503-808-7216 FAX: 503-350-0833	**LG Framework** **Version 1.0**	Qualcomm Snapdragon 800-series (32-bit) w/ Android 5.0.1; Qualcomm Snapdragon 800-series (64-bit) w/ Android 5.0.1	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2728)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2087)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3289)] "General-purpose cryptographic services available for Android used by LG devices to provide secured services to Java applications via the Bouncy Castle Java Cryptography Extension provider." *06/25/15: Added new tested information and updated implementation information;*
747	SUSE LLC 10 Canal Park, Suite 200 Cambridge, MA 02141 USA -Thomas Biege TEL: +49 911 74053 500 -Michael Hager TEL: +49 911 74053 80	**Linux kernel crypto API (C implementation)** **Version 1.0**	Intel x86-64 w/ SUSE Linux Enterprise Server 12	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2727)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2086)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3288)] "Linux kernel crypto API is an open-source software written mainly in C. The module provides various cryptographic services to software components within the Linux kernel. This test covers the generic C implementations of various ciphers."
746	SUSE LLC 10 Canal Park, Suite 200 Cambridge, MA 02141 USA -Thomas Biege TEL: +49 911 74053 500 -Michael Hager TEL: +49 911 74053 80	**Linux kernel crypto API (AVX2 for SHA-2)** **Version 1.0**	Intel x86-64 w/ SUSE Linux Enterprise Server 12	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256 , SHA-384 , SHA-512) (SHS Val#2726)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256 , SHA-384 , SHA-512) (HMAC Val#2085)] "Linux kernel crypto API is an open-source software written mainly in C. The module provides various cryptographic services to software components within the Linux kernel. This test covers AVX2 assembler implementation of SHA-2 on Intel x86 64bit HP hardware."
745	SUSE, LLC 10 Canal Park, Suite 200 Cambridge, MA 02141 USA -Thomas Biege TEL: +49 911 74053 500 -Michael Hager TEL: +49 911 74053 80	**Linux kernel crypto API (Assembler for AES and SSSE3 for SHA)** **Version 1.0**	Intel x86-64 w/ SUSE Linux Enterprise Server 12	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2725)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2084)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3287)] "Linux kernel crypto API is an open-source software written mainly in C. The module provides various cryptographic services to software components within the Linux kernel. This test covers the generic assembler implementation of AES and SSSE3 assembler implementation of SHA on Intel x86 64bit HP hardware."
744	SUSE LLC 10 Canal Park, Suite 200	**Linux kernel crypto API (AES-NI and AVX for SHA-2)**	Intel x86-64 w/ SUSE Linux Enterprise Server 12	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256 ,

	Cambridge, MA 02141 USA -Thomas Biege TEL: +49 911 74053 500 -Michael Hager TEL: +49 911 74053 80	**Version 1.0**			SHA-384 , SHA-512) (SHS Val#2724)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256 , SHA-384 , SHA-512) (HMAC Val#2083)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3286)] "Linux kernel crypto API is an open-source software written mainly in C. The module provides various cryptographic services to software components within the Linux kernel. This test covers the AES-NI implementation of AES and AVX assembler implementation of SHA-2 on Intel x86 64bit HP hardware."
743	Hewlett-Packard (TippingPoint) 14231 Tandem Boulevard Austin, TX 78728 USA -Kevin Pimm TEL: (512) 432-2969	**HP TippingPoint Crypto Core NSS** **Version 3.12.9.1**	Intel Xeon E5-2620v3 w/ CentOS 5.6; Intel Xeon E5-2690v3 w/ CentOS 5.6	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2723)] "This implementation represents a version of the FIPS certified Mozilla Network Security Services (NSS) compiled for CentOS 5.6."
742	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on XGS 7100** **Version 8.4.0.0**	Intel E5-2658 v2 2.4 GHz w/ RHEL 6.3 Linux	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2722)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2081)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3284)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3284)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
741	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on XGS 5100** **Version 8.4.0.0**	Intel Core i7-2600 3.4 GHz w/ RHEL 6.3 Linux	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2721)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2080)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3283)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3283)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
740	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on XGS 4100** **Version 8.4.0.0**	Intel i3-2115C 2.0 GHz w/ RHEL 6.3 Linux	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2720)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2079)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3282)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3282)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
739	Hewlett-Packard (TippingPoint) 14231 Tandem Boulevard Austin, TX 78728 USA -Kevin Pimm TEL: (512) 432-2969	**HP TippingPoint Crypto Core OpenSSL** **Version 2.0.8**	Intel Xeon E5-2620v3 w/ CentOS 5.6;Intel Xeon E5-2690v3 w/ CentOS 5.6	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2719)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC

					Val#2078)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3281)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3281)] "This implementation represents a version of the FIPS certified Mozilla Network Security Services (NSS) compiled for CentOS 5.6."
738	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on XGS 3100** **Version 8.4.0.0**	Intel Pentium B915C 1.5 GHz w/ RHEL 6.3 Linux	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2718)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2077)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3280)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3280)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
737	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on SP4001** **Version 8.4.0.0**	Intel Core i7-2600 3.4 GHz w/ Windows Server 2012 R2 64-bit	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2717)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2076)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3279)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3279)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
736	Hewlett-Packard Company 1160 Enterprise Way Sunnyvale, CA 94089 USA -Indra Fitzgerald TEL: 650-258-5477	**HP ESKM DRBG** **Version 6.0.0 (Firmware)**	Intel Xeon E5-2600 Family	3/20/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3277)] "HP Enterprise Secure Key Manager (ESKM) provides key generation, retrieval, and management for encryption devices and solutions. ESKM is a hardened security appliance with secure access control, administration, and logging. ESKM supports high availability with automatic multi-site clustering, replication, and failover."
735	Hewlett-Packard Company 1160 Enterprise Way Sunnyvale, CA 94089 USA -Indra Fitzgerald TEL: 650-258-5477	**HP ESKM OpenSSL** **Version 6.0.0 (Firmware)**	Intel Xeon E5-2600 Family	3/20/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3277)] "HP Enterprise Secure Key Manager (ESKM) provides key generation, retrieval, and management for encryption devices and solutions. ESKM is a hardened security appliance with secure access control, administration, and logging. ESKM supports high availability with automatic multi-site clustering, replication, and failover."
734	Zoll Medical 269 Mill Rd. Chemlsford, MA 01824 USA -Navid Shaidani TEL: 978-421-9843 -Bryan Newman TEL: 978-421-9843	**OpenSSL Fips Object Module** **Version 2.0.7 (Firmware)** **Part # ***	Texas Instruments AM3703 Cortex A8 (ARM 7)	3/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2714)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2074)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3276)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3276)]

					"OpenSSL Fips Object Module implements all necessary algorithms required for SSL communications." *10/20/15: Updated implementation information;*
733	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A8 32bit)** **Version 5.0**	Apple A8 w/ iOS 8	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3274)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software compiled for 32bit word size."
732	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A7 32bit)** **Version 5.0**	Apple A7 w/ iOS 8	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3273)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software compiled for 32bit word size."
731	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A8)** **Version 5.0**	Apple A8 w/ iOS 8	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3272)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
730	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A7)** **Version 5.0**	Apple A7 w/ iOS 8	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3271)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
729	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A6X)** **Version 5.0**	Apple A6X w/ iOS 8	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3270)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
728	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A6)** **Version 5.0**	Apple A6 w/ iOS 8	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3269)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
727	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A5X)** **Version 5.0**	Apple A5X w/ iOS 8	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3268)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
726	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A5)** **Version 5.0**	Apple A5 w/ iOS 8	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3267)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
725	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Generic, i5 32bit)** **Version 5.0**	Intel i5 w/ OSX 10.10	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3266)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software compiled for 32bit word size."
723	OpenSSL Software Foundation Inc.	**OpenSSL FIPS Object Module**	Apple A7 (ARMv8) 64-bit without NEON and Crypto Extensions w/ iOS 8.1; Apple	3/13/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-

	1829 Mount Ephraim Road Adamstown, MD 27101 USA -Steve Marquess TEL: 877-673-6775	**Version 2.0.10**	A7 (ARMv8) 64-bit with NEON and Crypto Extensions w/ iOS 8.1; Freescale P2020 (PPC) w/ VxWorks 6.9; Apple A7 (ARMv8) with NEON w/ iOS 8.1 32-bit; Apple A7 (ARMv8) without NEON w/ iOS 8.1 32-bit; Qualcomm APQ8084 (ARMv7) without NEON w/ Android 5.0 32-bit; Qualcomm APQ8084 (ARMv7) with NEON w/ Android 5.0 32-bit; SAMSUNG Exynos7420 (ARMv8) without NEON and Crypto Extensions w/ Android 5.0 64-bit; SAMSUNG Exynos7420 (ARMv8) with NEON and Crypto Extensions w/ Android 5.0 64-bit		224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2702)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2063)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3264)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3264)] "The OpenSSL FIPS Object Module is a full featured general purpose cryptographic library that is distributed in source code form under an open source license. It can be downloaded from www.openssl.org/source/." *04/17/15: Added new tested information;* *05/29/2015: Updated implementation information;* *08/11/15: Updated implementation information;*
722	RSA The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Sandy Carielli TEL: 781-515-7510	**RSA BSAFE® Crypto-J JSAFE and JCE Software Module** **Version 6.2**	Intel Core i7 w/ Windows 8.1 (64-bit); NVIDIA Tegra 3 w/ Android 4.1.2	3/13/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2701)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2062)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3263)] "RSA BSAFE Crypto-J security software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. It supports a wide range of industry standard encryption algorithms offering Java developers the flexibility to choose the option most appropriate to meet their requirements" *03/26/15: Added new tested information;*
721	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Generic, Xeon)** **Version 5.0**	Intel Xeon w/ OSX 10.10	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3262)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
720	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Generic, Xeon 32bit)** **Version 5.0**	Intel Xeon w/ OSX 10.10	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3261)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
719	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Generic, i7)** **Version 5.0**	Intel i7 w/ OSX 10.10	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3260)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
718	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Generic, i7 32bit)** **Version 5.0**	Intel i7 w/ OSX 10.10	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3259)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
717	Samsung Electronics co. Ltd. 95, samsung 2-ro Giheung-gu Yongin-si, Gyeonggi-do 446-711 Korea -Jinsu Hyun TEL: 82-31-8037-3737	**Security Sub-System(SSS) V6.7_2** **Part # 1.0**	N/A	3/13/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2665)] "SSS is the cryptographic hardware module of Samsung Exynos. This module implements block ciphers (AES and TDES), hashes (SHA-1, SHA-256, SHA-384 and SHA-512), message authentication codes (HMAC and CMAC) and a pseudo random number generator (DRBG)." *03/19/15: Updated implementation information;*

716	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Generic, i5)** **Version 5.0**	Intel i5 w/ OSX 10.10	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3257)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
715	Aruba Networks, Inc. 1344 Crossman Ave Sunnyvale, CA 94089 USA -Steve Weingart TEL: +1 830 850 1544	**ArubaOS OpenSSL Module** **Version 6.4.3-FIPS (Firmware)**	x86-64	3/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3256)] "The Aruba MOVE Architecture forms the core network infrastructure for supporting mobile and wireless computing devices. The system enables enterprise-scale 802.11 wireless LANs (Wi-Fi), secure remote VPNs, and mobility-optimized wired networks."
714	ViaSat, Inc. 6155 El Camino Real Carlsbad, CA 92009 USA -David Suksumrit TEL: 760-476-2306 FAX: 760-929-3941 -Savitha Naik TEL: 760-476-7416 FAX: 760-929-3941	**EbemCrypto** **Version EbemCrypto Version 10 (Firmware)**	IBM Power PC	3/6/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3253)] "Implements authentication, key negotiation/generation, and controls FPGA implementation of traffic encryption in ViaSat's Enhanced Bandwidth Efficient Modem (EBEM-500)."
713	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Windows x86-64 for 64 bits with AES-NI** **Version 8.4.1.0**	Intel x86_64 with AES-NI w/ Microsoft Windows Server 2008	3/6/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3252)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3252)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
712	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Windows x86-64 for 64 bits** **Version 8.4.1.0**	Intel x86_64 w/ Microsoft Windows Server 2008	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2688)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2051)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3251)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3251)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
711	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Windows x86-64 for 32 bits with AES-NI** **Version 8.4.1.0**	Intel x86_64 with AES-NI w/ Microsoft Windows Server 2008	3/6/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3250)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3250)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
710	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia	**ICC Algorithmic Core on Windows x86-64 for 32 bits** **Version 8.4.1.0**	Intel x86_64 w/ Microsoft Windows Server 2008	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2687)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC

	-Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420				Val#2050)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3249)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3249)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
709	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Ubuntu PPC64 for 64 bits with PAAs** **Version 8.4.1.0**	IBM Power8 with hardware accelerators w/ Ubuntu 14.04 LE	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2686)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2049)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3248)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3248)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
708	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Ubuntu PPC64 for 64 bits** **Version 8.4.1.0**	IBM Power8 w/ Ubuntu 14.04 LE	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2685)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2048)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3247)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3247)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
707	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Solaris Sparc for 64 bits with PAAs** **Version 8.4.1.0**	Sparc T4 with hardware accelerators w/ Solaris 11	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2684)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2047)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3246)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3246)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
706	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Solaris Sparc for 64 bits** **Version 8.4.1.0**	Sparc T4 w/ Solaris 11	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2683)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2046)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (

					AES-128 , AES-192 , AES-256) (AES Val#3245)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3245)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
705	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Solaris Sparc for 32 bits with PAAs** **Version 8.4.1.0**	Sparc T4 with hardware accelerators w/ Solaris 11	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2682)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2045)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3244)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3244)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
704	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Solaris Sparc for 32 bits** **Version 8.4.1.0**	Sparc T4 w/ Solaris 11	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2681)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2044)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3243)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3243)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
703	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on SLES zSeries for 64 bits with PAAs** **Version 8.4.1.0**	IBM zSeries s390x with CPACF hardware support w/ SUSE Linux Enterprise Server 11	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2680)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2043)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3242)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3242)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
702	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on SLES zSeries for 64 bits** **Version 8.4.1.0**	IBM zSeries s390x w/ SUSE Linux Enterprise Server 11	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2679)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2042)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3241)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3241)]

					"ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
701	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on SLES zSeries for 32 bits with PAAs** **Version 8.4.1.0**	IBM zSeries s390x with CPACF hardware support w/ SUSE Linux Enterprise Server 11	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2678)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2041)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3240)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3240)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
700	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on SLES zSeries for 32 bits** **Version 8.4.1.0**	IBM zSeries s390x w/ SUSE Linux Enterprise Server 11	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2677)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2040)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3239)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3239)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
699	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL x86-64 for 64 bits with AES-NI** **Version 8.4.1.0**	Intel x86_64 with AES-NI w/ Red Hat Linux Enterprise Server 7.0	3/6/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3238)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3238)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/15/15: Updated implementation information;*
698	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL x86-64 for 64 bits** **Version 8.4.1.0**	Intel x86_64 w/ Red Hat Linux Enterprise Server 7.0	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2676)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2039)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3237)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3237)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/08/15: Updated implementation information;*
697	IBM® Corporation	**ICC Algorithmic Core on RHEL x86-64**	Intel x86_64 with AES-NI w/ Red Hat	3/6/2015	**CTR_DRBG**: [Prediction Resistance Tested:

	Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**for 32 bits with AES-NI** **Version 8.4.1.0**	Linux Enterprise Server 7.0		Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3236)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3236)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/08/15: Updated implementation information;*
696	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL x86-64 for 32 bits** **Version 8.4.1.0**	Intel x86_64 w/ Red Hat Linux Enterprise Server 7.0	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2675)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2038)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3235)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3235)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/08/15: Updated implementation information;*
695	Hewlett-Packard Company 1160 Enterprise Way Sunnyvale, CA 94089 USA -Indra Fitzgerald TEL: 650-258-5477	**HP ACS Loader** **Version 0.67 (Firmware)**	AMCC PowerPC440EPx	3/6/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3234)] "The Atalla Cryptographic Subsystem (ACS) is a multi-chip embedded cryptographic module that provides secure cryptographic processing, key management, and storage capabilities."
694	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL PPC64 for 64 bits with PAAs** **Version 8.4.1.0**	IBM Power8 with hardware accelerators w/ Red Hat Linux Enterprise Server 7.0 BE	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2673)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2037)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3233)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3233)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/08/15: Updated implementation information;*
693	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL PPC64 for 64 bits** **Version 8.4.1.0**	IBM Power8 w/ Red Hat Linux Enterprise Server 7.0 BE	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2672)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2036)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3232)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3232)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/08/15: Updated implementation information;*
692	IBM® Corporation Seabank Centre	**ICC Algorithmic Core on RHEL PPC64 for 32 bits with PAAs**	IBM Power8 with hardware accelerators w/ Red Hat Linux Enterprise Server 7.0	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-224 ,

	12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**Version 8.4.1.0**	BE		SHA-256 , SHA-384 , SHA-512) (SHS Val#2671)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2035)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3231)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3231)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/08/15: Updated implementation information;*
691	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL PPC64 for 32 bits** **Version 8.4.1.0**	IBM Power8 w/ Red Hat Linux Enterprise Server 7.0 BE	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2670)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2034)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3230)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3230)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/08/15: Updated implementation information;*
690	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on AIX PPC64 for 64 bits with PAAs** **Version 8.4.1.0**	IBM Power8 with hardware accelerators w/ IBM AIX 7.1	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2669)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2033)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3229)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3229)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/08/15: Updated implementation information;*
689	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on AIX PPC64 for 64 bits** **Version 8.4.1.0**	IBM Power8 w/ IBM AIX 7.1	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2668)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2032)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3228)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3228)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/08/15: Updated implementation information;*
688	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia	**ICC Algorithmic Core on AIX PPC64 for 32 bits with PAAs** **Version 8.4.1.0**	IBM Power8 with hardware accelerators w/ IBM AIX 7.1	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2667)] **HMAC_Based DRBG**: [Prediction Resistance

	-Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420				Tested: Enabled and Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2031)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3227)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3227)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/08/15: Updated implementation information;*
687	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on AIX PPC64 for 32 bits** **Version 8.4.1.0**	IBM Power8 w/ IBM AIX 7.1	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2666)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2030)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3226)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3226)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *05/08/15: Updated implementation information;*
686	Samsung Electronics co. Ltd. 95, samsung 2-ro Giheung-gu Yongin-si, Gyeonggi-do 446-711 Korea -Jinsu Hyun TEL: 82-31-8037-3737	**Security Sub-System(SSS) V6.7_1** **Part # 1.0**	N/A	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2665)] "SSS is the cryptographic hardware module of Samsung Exynos. This module implements block ciphers (AES and TDES), hashes (SHA-1, SHA-256, SHA-384 and SHA-512), message authentications codes (HMAC and CMAC) and a pseudo random number generator (DRBG)." *03/16/15: Updated implementation information;*
685	Draeger Medical Systems Inc. 6 Tech Drive Andover, MA 01810 USA -Michael Robinson TEL: +1 978 379 8000 FAX: +1 978 379 8538	**DRAEGER WCM9113 802.11ABGN VG2** **Version VG2 (Firmware)** **Part # MS32018**	N/A	3/6/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2661)] "Algorithm routines implemented in the DRAEGER WCM9113 802.11ABGN VG2" *03/26/15: Updated implementation information;*
684	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**Brocade Cryptographic Library used in the interface module** **Version BRCD-LP-CRYPTO-VER-1.0 (Firmware)**	Freescale 1199 MHz Power PC processor P2010E	2/27/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#934)] "Brocade cryptographic library used in the interface, module implements crypto operations in hardware and in software. The Brocade MLXe Series provides industry leading wire-speed port capacity without compromising the performance of advanced capabilities such as IPSec, IKEv2, IPv6, MPLS and MPLS Virtual Private Networks (VPNs)."
683	Accellion Inc. 1804 Embarcadero Road Suite 200 Palo Alto, Ca 94303 USA -Prateek Jain TEL: 65-62445670 FAX: 65-62445678	**OpenSSL Object Module** **Version 1.0.1**	Intel Xeon QuadCore w/ CentOS 6.4 on VMware ESXi 5.1.0	2/20/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3212)] "Accellion Kiteworks Cryptographic Module is a key component of Accellion's Kiteworks product that enables enterprises to securely share and transfer files. Extensive tracking and reporting tools allow compliance with SOX, HIPAA, FDA and GLB regulations while providing enterprise grade security and ease of use."
682	IBM Internet Security Systems 6303 Barfield Road Atlanta, GA 30328 USA	**GSKit: ICC 8.2.2** **Version 4.6.1 (Firmware)**	Intel(R) Xeon(R) CPU E5540 @ 2.53GHz	2/20/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2657)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-

	-Scott Sinsel TEL: (404) 348-9355				224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2023)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3210)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3210)] "The Network Intrusion Prevention System (IPS) automatically blocks malicious attacks while preserving network bandwidth and availability."
681	Hewlett-Packard Company 153 Taylor Street Littleton, MA 01460 USA -Bob Pittman TEL: 1-978-264-5211 FAX: 1-978-264-5522	**HP Comware** **Version ComwareV7.1-R2416 (Firmware)**	Broadcom XLP108AQ 1GHz	2/20/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3208)] "Comware cryptographic library is a software library that provides cryptographic functions within HP devices."
680	Cavium Inc. 2315 N. First Street San Jose, CA 95131 USA -Tejinder Singh TEL: 408-943-7403 FAX: 408-577-1992 -Phanikumar Kancharla TEL: 408-943-7496	**Cavium Crypto Library** **Version 1.0.0 (Firmware)**	Cavium Octeon Family, CN61XX	2/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3205)] "This module implements listed algorithms OpenSSL and Octeon 61XX processor."
679	IBM Internet Security Systems 6303 Barfield Road Atlanta, GA 30328 USA -Scott Sinsel TEL: (404) 348-9355	**FIPS module version 2.0.1** **Version 4.6.1 (Firmware)**	Intel(R) Xeon(R) CPU E5540 @ 2.53GHz	2/13/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2651)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2018)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3204)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3204)] "The Network Intrusion Prevention System (IPS) automatically blocks malicious attacks while preserving network bandwidth and availability."
678	IBM Internet Security Systems 6303 Barfield Road Atlanta, GA 30328 USA -Scott Sinsel TEL: (404) 348-9355	**GSKit ICC 8.2.2** **Version 3.1.1**	Intel Xeon E5540 @ 2.53GHz w/ winW (64-bit)	2/13/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2650)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2017)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3202)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3202)] "SiteProtector security feature using IBM Global Security Kit (GSKit)."
677	Micron Technology 570 Alder Drive Milpitas, CA 95035 USA -Dale McNamara TEL: 408-834-1729	**Legacy Crypto Module** **Version 36856 (Firmware)**	Marvell 88SS91XX (ARMv5)	2/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3201)] "AES Component implements AES key size of 256 bits used for encrypting CSP's. SHA256 used for check character generation. RSA used for F/W package signature verification. CTR_DRBG is used for AES KEY generation."
676	SUSE, LLC 10 Canal Park, Suite 200 Cambridge, MA 02141 USA -Thomas Biege TEL: +49 911 74053 500 -Michael Hager TEL: +49 911 74053 80	**OpenSSL (SSSE3 Assembler for AES and SHA-1)** **Version 2.0**	Intel x86-64 w/ SUSE Linux Enterprise Server 12	2/13/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1) (SHS Val#2648)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1) (HMAC Val#2016)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3199)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3199)] "OpenSSL is an open-source library of various cryptographic algorithms written mainly in C. This test covers the SSSE3 assmbler implementation

					of AES and SHA-1 on Intel x86 64bit HP hardware."
675	SUSE LLC 10 Canal Park, Suite 200 Cambridge, MA 02141 USA -Thomas Biege TEL: +49 911 74053 500 -Michael Hager TEL: +49 911 74053 80	**OpenSSL (Generic Assembler for AES and SHA)** **Version 2.0**	Intel x86-64 w/ SUSE Linux Enterprise Server 12	2/13/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2646)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2015)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3198)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3198)] "OpenSSL is an open-source library of various cryptographic algorithms written mainly in C. This test covers the generic assembler implementation of AES and SHA on Intel x86 64bit HP hardware."
674	SUSE LLC 10 Canal Park, Suite 200 Cambridge, MA 02141 USA -Thomas Biege TEL: +49 911 74053 500 -Michael Hager TEL: +49 911 74053 80	**OpenSSL (AES-NI and AVX+SSSE3 for SHA-1)** **Version 2.0**	Intel x86-64 w/ SUSE Linux Enterprise Server 12	2/13/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1) (SHS Val#2648)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1) (HMAC Val#2014)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3197)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3197)] "OpenSSL is an open-source library of various cryptographic algorithms written mainly in C. This test covers the AES-NI implementation of AES and AVX+SSSE3 assembler implementation of SHA-1 on Intel x86 64bit HP hardware."
673	Watchdata Technologies Pte Ltd 7F QiMing International Building Wangjing Lize Middle Park No.101 Beijing, Chaoyang District 100102 China -Fan Nannan TEL: 18001226917 FAX: 01064365760 -Wang Xuelin TEL: 18001226735 FAX: 01064365760	**WatchKey ProX USB Token** **Part # AS518 and PCB K023314A**	N/A	2/13/2015	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2647)] "The WatchKey ProX USB token provides digital signature generation and verification for online authentication of online transactions and data encryption/decryption to online service users" *05/22/15: Updated vendor information;*
672	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -CHRIS TEL: 408-333-0480 FAX: 408-333-8101	**Brocade FIPS Crypto Library** **Version 7.4.0 (Firmware)**	E500mc	2/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2892)] "Brocade cryptographic library is used in Brocade FOS based switches to implement the cryptographic related modules."
671	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**Brocade FIPS Crypto Library** **Version 7.4.0 (Firmware)**	PPC 440GPX and PPC 8548	2/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2893)] "Brocade cryptographic library is used in Brocade FOS based switches to implement the cryptographic related modules."
670	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**Brocade FIPS Crypto Library** **Version 7.4.0 (Firmware)**	AMCC PPC 440EPX	2/13/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2876)] "Brocade cryptographic library is used in Brocade FOS based switches to implement the cryptographic related modules."
669	Blue Coat Systems Inc. 420 North Mary Avenue Sunnyvale, California 94085-4121 USA	**Blue Coat SSL Visibility Appliance Crypto Library** **Version 1.0.2**	Intel X3450 Quad Core w/ Linux x86_64; Intel E5620 Quad Core w/ Linux x86_64; Intel E5645 Hex Core w/ Linux x86_64	2/6/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3195)]

	-Diana Robinson TEL: 845-454-6397 -Nick Goble TEL: 978-318-7544				"The Blue Coat SSL Visibility Appliance decrypts multiple streams of SSL content to provide IDS/IPS, logging, forensics, and data loss prevention. This preserves complete network traffic histories necessary for compliance/threat analysis and enables SSL inspection capabilities that close the security loophole created by SSL."
668	Websense, Inc. 10240 Sorrento Valley Road San Diego, CA 92121 USA -Matt Sturm	**Java Crypto Module** **Version 2.0**	Intel Xeon E5-2400 w/ Microsoft Windows Server 2012	1/30/2015	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2011)] "The Websense Java Crypto Module provides cryptographic functions for a variety of security solutions from Websense."
667	KONA I Co. Ltd 8F EXCON Venture-Tower, 3, Eunhaeng-Ro, Yeongdeungpo-Gu Seoul, n/a 150-872 Republic of Korea -Irene Namkung TEL: +82-2-2168-7586 FAX: +82-2-3440-4405 -Sungmin Ahn TEL: +82-2-3440-9135 FAX: +82-2-3440-4405	**KONA HW Crypto Library** **Version 2.0 (Firmware)** **Part # Infineon SLE97CNFX1M00PE A22**	Infineon SLE97CNFX1M00PE A22	1/30/2015	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3189)] "**CTR_DRBG**: AES 128/192/256 bit. AES: ECB/CBC, 128/192/256 bit. AES CMAC: 128/192/256 bit. Triple-DES: 2-key/3-key, ECB/CBC. RSA: 2048 bit encrypt/decrypt, sign/verify, key gen (legacy use 1024 bit verify with SHA-1). RSA CRT: 2048 bit key gen, sign. ECDSA: P-224/256/384/521 key gen/sign/verify (legacy use P-192 verify)."
666	Hewlett-Packard Development Company L.P. 11445 Compaq Center Dr. W Houston, TX 77070 USA -Julie Ritter TEL: (281) 514-4087	**HP BladeSystem c-Class Virtual Connect Library** **Version 1.0 (Firmware)**	Freescale MPC8347 Processor; Freescale MPC8535 Processor	1/23/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3186)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3186)] "The HP BladeSystem is a rack-mount enterprise-class computing infrastructure designed to maximize power while minimizing costs, saving up to 56% of the total cost of ownership compared to traditional infrastructures."
665	Feitian Technologies Co., Ltd Floor 17, Tower B, Huizhi Mansion, No.9 Xueqing Road Haidian, Beijing 100085 China -Tibi TEL: (+86)010-62304466-821 FAX: (+86)010-62304477 -PENG Jie TEL: (+86)010-62304466-419 FAX: (+86)010-62304477	**FEITIAN-FIPS-Cryptographic Library V1.0.0** **Version 1.0.0 (Firmware)** **Part # SLE78CLUFX5000PHM**	Infineon SLE78CLUFX5000PHM	1/23/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3183)] "FEITIAN-FIPS-Cryptographic Library V1.0.0 implements AES, TDES, CMAC, TDES MAC, SH1, SHA256, SHA512, DRBG, RSA, and KDF, and operates on Infineon SLE78CLFX4000PM for FEITIAN-FIPS-JCOS V1.0.0, which is smart card complied with Java Card 2.2.2 and Global Platform 2.2.1." *02/05/15: Updated vendor information;*
664	Feitian Technologies Co. Ltd Floor 17, Tower B, Huizhi Mansion, No.9 Xueqing Road Haidian, Beijing 100085 China -Tibi TEL: (+86)010-62304466-821 FAX: (+86)010-62304477 -PENG Jie TEL: (+86)010-62304466-419 FAX: (+86)010-62304477	**FEITIAN-FIPS-Cryptographic Library V1.0.0** **Version 1.0.0 (Firmware)** **Part # SLE77CLFX2400PM**	Infineon SLE77CLFX2400PM	1/23/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3182)] "FEITIAN-FIPS-Cryptographic Library V1.0.0 implements AES, TDES, CMAC, TDES MAC, SH1, SHA256, SHA512, DRBG, RSA, and KDF, and operates on Infineon SLE78CLFX4000PM for FEITIAN-FIPS-JCOS V1.0.0, which is smart card complied with Java Card 2.2.2 and Global Platform 2.2.1." *02/17/15: Updated vendor information;*
663	Pure Storage Inc. 650 Castro Street Suite #400 Mountain View, CA 94041 USA -Marco Sanvido TEL: 510-501-8968 -Ethan Miller TEL: 831-345-4864	**Flash Array Crypto Library** **Version 1.0.0**	Intel Xeon x64 CPU with AES-NI (E3/E5/E7 Family) w/ Purity 4	1/23/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3181)] "Flash Array Crypto Library is a comprehensive suite of FIPS Approved algorithms. All key sizes and modes have been implemented to allow flexibility and efficiency."
662	Palo Alto Networks 4401 Great America Parkway Santa Clara, California 95054 USA -Richard Bishop TEL: 408-753-4000 -Jake Bajic TEL: 408-753-4000	**Palo Alto Networks Crypto Module** **Version 6.1 (Firmware)**	Intel Multi Core Xeon	1/16/2015	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128) (AES Val#3180)] "The Palo Alto Networks Crypto Module provides the cryptographic functionality for the Panorama M-100." *03/04/15: Updated implementation information;* *03/06/15: Updated implemement information;*

661	N/A	**N/A**	N/A	1/16/2015	N/A
660	Aruba Networks, Inc. 1344 Crossman Ave Sunnyvale, CA 94089 USA -Jon Green TEL: 408-227-4500 FAX: 408-227-4550 -Steve Weingart TEL: 1-830-580-1544	**ArubaOS OpenSSL Module** **Version ArubaOS 6.4.3-FIPS (Firmware)**	Broadcom BCM53014	12/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3176)] "The Aruba MOVE Architecture forms the core network infrastructure for supporting mobile and wireless computing devices. The system enables enterprise-scale 802.11 wireless LANs (Wi-Fi), secure remote VPNs, and mobility-optimized wired networks."
659	Samsung Electronics Co., Ltd. 416, Maetan 3-Dong Youngton Gu Suwon, Gyeonggi 152-848 South Korea -Abraham Joseph Kang TEL: +1-408-324-3678 FAX: +1-408-324-3640 -Bumhan Kim TEL: +82-10-4800-6711	**Samsung SCrypto** **Version 1.0**	Qualcomm MSM8974 w/ QSEE 2.0	12/24/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2627)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#2002)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3175)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3175)] "Provide general purpose cryptographic services to TrustZone applications on the mobile platform for the protection of data in transit."
658	SPYRUS, Inc. 1860 Hartog Drive San Jose, CA 95131-2203 USA -William Sandberg-Maitland TEL: 613-298-3426	**SPYCOS 3.0** **Version 3.0 (Firmware)** **Part # 742100004F**	SPYCOS 3.0	12/24/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#2529)] "SPYCOS 3.0 is a hardware cryptographic module that enables security critical capabilities such as user authentication, message privacy, integrity and secure storage in rugged, tamper-evident QFN and microSD form factors. The SPYCOS 3.0 Module communicates with a host computer via the standard USB interface."
656	Samsung Electronics Co., Ltd. 416, Maetan 3-Dong Youngton Gu Suwon, Gyeonggi 152-848 South Korea -Abraham Joseph Kang TEL: +1-408-324-3678 FAX: +1-408-324-3640 -Bumhan Kim TEL: +82-10-4800-6711	**Samsung SCrypto** **Version 1.0**	Samsung Electronics Exynos 5422 w/ MOBICORE Tbase 300	12/24/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2616)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1991)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3163)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3163)] "Provide general purpose cryptographic services to TrustZone applications on the mobile platform for the protection of data in transit."
655	Qualcomm Technologies, Inc. 5775 Morehouse Dr San Diego, CA 92121 USA -Lu Xiao TEL: 858-651-5477	**DRBG of QTI Cryptographic Module on Crypto Core V5.3.0.** **Version v5.3.0**	Snapdragon 810 w/ Android 5.0	12/24/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3164)] "The DRBG follows NIST SP 800-90A and produces deterministic random bits with the entropy collected from hardware."
654	Fortinet, Inc. 1090 Kifer Road Sunnyvale, CA 94086-5301 USA -Daniel Hayes TEL: 613-225-9381 x7643 FAX: 613-225-9951 -Alan Kaye TEL: 613-225-9381 x7416 FAX: 613-225-9951	**Fortinet FortiAnalyzer RBG Cryptographic Library** **Version 5.2.1 (Firmware)**	Intel Celeron; Intel Xeon E5	12/24/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#From current implementation submitted "Fortinet Fo)] "This document focuses on the software implementation of the Fortinet FortiAnalyzer RBG Cryptographic Library v5.0 running on Intel x86 compatible processors."
653	Fortinet, Inc. 1090 Kifer Road Sunnyvale, CA 94086-5301 USA -Daniel Hayes TEL: 613-225-9381 x7643 FAX: 613-225-9951 -Alan Kaye TEL: 613-225-9381 x7416	**Fortinet FortiManager RBG Cryptographic Library** **Version 5.2.1 (Firmware)**	Intel Xeon E3; Intel Xeon E5	12/24/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#From current implementation submitted "Fortinet Fo)] "This document focuses on the software implementation of the Fortinet FortiManager RBG Cryptographic"

	FAX: 613-225-9951				
652	Fortinet Inc. 1090 Kifer Road Sunnyvale, CA 94086-5301 USA -Daniel Hayes TEL: 613-225-9381 x7643 FAX: 613-225-9951 -Alan Kaye TEL: 613-225-9381 x7416 FAX: 613-225-9951	**Fortinet FortiOS RBG Cryptographic Library** **Version 5.0.10 (Firmware)**	ARM v5 Compatible; Intel Atom; Intel Celeron; Intel i3-540 Dual Core; Intel i5-750 Quad Core; Intel Xeon	12/19/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3169)] "This document focuses on the firmware implementation of the Fortinet FortiOS RBG Cryptographic Library v5.0 running on Intel x86 compatible processors."
651	Barracuda Networks 3175 Winchester Road Campbell, CA 95008 USA -Andrea Cannon TEL: 703-743-9068	**Barracuda Cryptographic Software Module** **Version 1.0.1.8**	Intel Xeon, Intel Xeon with AES-NI, AMD Opteron, AMD Opteron with AES-NI w/ Barracuda OS v2.3.4	12/19/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2618)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1993)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3165)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3165)] "The Barracuda Cryptographic Software Module is a cryptographic software library that provides fundamental cryptographic functions for applications in Barracuda security products that use Barracuda OS v2.3.4 and require FIPS 140-2 approved cryptographic functions."
650	wolfSSL Inc. 10016 Edmonds Way Suite C-300 Edmonds, WA 98020 USA -Todd Ouska TEL: 503-679-1859 -Larry Stefonic TEL: 206-369-4800	**wolfCrypt** **Version 3.6.0**	Intel Core i7 w/ Linux 3.13 64-bit	12/12/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2614)] "WolfCrypt module is a comprehensive suite of FIPS Approved algorithms. All key sizes and modes have been implemented to allow flexibility and efficiency." *10/20/15: Updated implementation information;*
649	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -James Reardon TEL: (651) 628-2700 FAX: (651) 628-2701	**McAfee NSP NS Crypto Lib** **Version 2.0.5 (Firmware)**	Intel Xeon E5	12/12/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3156)] "Cryptographic services for the McAfee NSP Intrusion Prevention appliances"
648	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -James Reardon TEL: (651) 628-2700 FAX: (651) 628-2701	**McAfee NSP M Crypto Lib** **Version 2.0.5 (Firmware)**	Broadcom XLR	12/12/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3155)] "Cryptographic services for the McAfee NSP Intrusion Prevention appliances"
647	Blue Coat Systems Inc. 420 North Mary Avenue Sunnyvale, California 94085-4121 USA -Diana Robinson TEL: 845-454-6397 -Nick Goble TEL: 978-318-7544	**Blue Coat SSL Visibility Appliance Crypto Library** **Version 1.0.1**	Intel X3450 Quad Core w/ Linux x86_64; Intel E5620 Quad Core w/ Linux x86_64; Intel E5645 Hex Core w/ Linux x86_64	12/12/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3154)] "The Blue Coat SSL Visibility Appliance decrypts multiple streams of SSL content to provide IDS/IPS, logging, forensics, and data loss prevention. This preserves complete network traffic histories necessary for compliance/threat analysis and enables SSL inspection capabilities that close the security loophole created by SSL."
646	Red Hat Inc. 1801 Varsity Drive Raleigh, NC 27606 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (ibm-64-gen)** **Version 2.6.32-504.23.1**	Intel x86 w/ Red Hat Enterprise Linux 6.6	12/5/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2608)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1986)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3152)] "Linux kernel crypto API implementation providing cryptographic services to software components executing as part of the Linux kernel - this tests covers the generic C implementations

					of various ciphers on Intel x86 64 bit IBM hardware." *02/17/15: Updated implementation information; 07/28/15: Updated implementation information;*
645	Red Hat, Inc. 1801 Varsity Drive Raleigh, NC 27606 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (hp-64-gen)** **Version 2.6.32-504.23.1**	Intel x86 w/ Red Hat Enterprise Linux 6.6	12/5/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2607)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1985)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3151)] "Linux kernel crypto API implementation providing cryptographic services to software components executing as part of the Linux kernel - this tests covers the generic C implementations of various ciphers on Intel x86 64 bit HP hardware." *02/13/15: Updated implementation information; 06/01/15: Updated implementation information;*
644	Red Hat, Inc. 1801 Varsity Drive Raleigh, NC 27606 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (ibm-64-aesni-blkasm)** **Version 2.6.32-504.23.1**	Intel x86 w/ Red Hat Enterprise Linux 6.6	12/5/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3150)] "Linux kernel crypto API implementation providing cryptographic services to software components executing as part of the Linux kernel - this tests covers the AES-NI implementation (aes-aesni) and the PCLMULQDQ-NI implementation (ghash) on Intel x86 64 bit IBM hardware." *02/17/15: Updated implementation information; 06/01/15: Updated implementation information;*
643	Red Hat, Inc. 1801 Varsity Drive Raleigh, NC 27606 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (ibm-64-aesni)** **Version 2.6.32-504.23.1**	Intel x86 w/ Red Hat Enterprise Linux 6.6	12/5/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3149)] "Linux kernel crypto API implementation providing cryptographic services to software components executing as part of the Linux kernel - this tests covers the AES-NI implementation (aes-aesni) and the PCLMULQDQ-NI implementation (ghash) on Intel x86 64 bit IBM hardware." *02/17/15: Updated implementation information; 06/01/15: Updated implementation information;*
642	Red Hat, Inc. 1801 Varsity Drive Raleigh, NC 27606 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (ibm-64-aesasm)** **Version 2.6.32-504.23.1**	Intel x86 w/ Red Hat Enterprise Linux 6.6	12/5/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3148)] "Linux kernel crypto API implementation providing cryptographic services to software components executing as part of the Linux kernel - this tests covers the assembler AES implementation (aes-asm) on Intel x86 64 bit IBM hardware." *02/17/15: Updated implementation information; 06/01/15: Updated implementation information;*
641	Red Hat, Inc. 1801 Varsity Drive Raleigh, NC 27606 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (hp-64-aesni-blkasm)** **Version 2.6.32-504.23.1**	Intel x86 w/ Red Hat Enterprise Linux 6.6	12/5/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3147)] "Linux kernel crypto API implementation providing cryptographic services to software components executing as part of the Linux kernel - this tests covers the AES-NI implementation (aes-aesni) and the PCLMULQDQ-NI implementation (ghash) on Intel x86 64 bit HP hardware." *02/13/15: Updated implementation information; 06/01/15: Updated implementation information;*
640	Red Hat, Inc. 1801 Varsity Drive Raleigh, NC 27606 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (hp-64-aesni)** **Version 2.6.32-504.23.1**	Intel x86 w/ Red Hat Enterprise Linux 6.6	12/5/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3146)] "Linux kernel crypto API implementation providing cryptographic services to software components executing as part of the Linux kernel - this tests covers the AES-NI implementation

					(aes-aesni) and the PCLMULQDQ-NI implementation (ghash) on Intel x86 64 bit HP hardware." *02/13/15: Updated implementation informaiton; 06/01/15: Updated implementation information;*
639	Red Hat, Inc. 1801 Varsity Drive Raleigh, NC 27606 USA -Ann-Marie Rubin TEL: 978 392 1000	**Linux Kernel crypto API (hp-64-aesasm)** **Version 2.6.32-504.23.1**	Intel x86 w/ Red Hat Enterprise Linux 6.6	12/5/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3145)] "Linux kernel crypto API implementation providing cryptographic services to software components executing as part of the Linux kernel - this tests covers the assembler AES implementation (aes-asm) on Intel x86 64 bit HP hardware." *02/13/15: Updated implementation information; 06/01/15: Updated implementation information;*
638	Canon Inc. 30-2 Shimomaruko 3-chome Ohta-ku, Tokyo 146-8501 Japan -Yoichi Toyokura TEL: +81-3-3758-2111 FAX: +81-3-3758-1160	**DRBG Library on Canon MFP Security Chip** **Version V01L01R02 (Firmware)**	FR80E	12/5/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2601)] "The DRBG Library provides cryptographic services for Canon MFP Security Chip."
637	INSIDE Secure Eerikinkatu 28 Helsinki, 00180 Finland -Serge Haumont TEL: +358 40 5808548 -Marko Nippula TEL: +358 40 7629394	**SafeZone FIPS Cryptographic Module Option A** **Version 1.1**	Intel Atom Z3740 with AES-NI w/ 64 bit library w/ Ubuntu Linux (kernel 3.13); Intel Atom Z2560 w/ 32 bit library w/ Android 4.2; Intel Atom Z3740 with AES-NI w/ 32 bit library w/ Ubuntu Linux (kernel 3.13); Intel Atom Z3740 without AES-NI w/ 64 bit library w/ Ubuntu Linux (kernel 3.13); ARMv6 w/ Raspbian Linux (kernel 3.10); ARMv7 w/ iOS 7.1; ARM64 w/ iOS 7.1; ARMv7-a w/ Android 4.4; ARMv7-a w/	12/5/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3123)] "SafeZone FIPS Cryptographic Module is a FIPS 140-2 Security Level 1 validated software cryptographic module from INSIDE Secure. The module is a toolkit which provides the most commonly needed cryptographic primitives for a large variety of applications, including but not limited to, primitives for DAR, DRM, TLS, and VPN on mobile devices."
636	Sage Microelectronics Corp 910 Campisi Way Suite-2A Campbell, CA 95008 USA -Chris Tsu TEL: 408-309-9118 -Larry Ko TEL: 408-768-1378	**RNG Library** **Version 1.0 (Firmware)** **Part # S261, Rev. A**	Sagemicro S261 (Hardware IC CHIP)	12/5/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-256) (AES Val#2835)] BlockCipher_No_df: (AES-128 , AES-256) (AES Val#2835)] "True Random number generator"
635	Brocade Communications Systems, Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0408 FAX: 408-333-8101	**Brocade FIPS Crypto Library** **Version FOS 7.4.0 (Firmware)**	CN6880	12/5/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#3130)] "Brocade cryptographic library is used in Brocade FOS based switches to implement the cryptographic related modules."
634	INSIDE Secure Eerikinkatu 28 Helsinki, 00180 Finland -Serge Haumont TEL: +358 40 5808548 -Marko Nippula TEL: +358 40 7629394	**SafeZone FIPS Cryptographic Module** **Version 1.1** **Part # n**	Intel Atom Z3740 with AES-NI w/ 64 bit library w/ Ubuntu Linux (kernel 3.13); Intel Atom Z2560 w/ 32 bit library w/ Android 4.2; Intel Atom Z3740 with AES-NI w/ 32 bit library w/ Ubuntu Linux (kernel 3.13); Intel Atom Z3740 without AES-NI w/ 64 bit library w/ Ubuntu Linux (kernel 3.13); ARMv6 w/ Raspbian Linux (kernel 3.10); ARMv7 w/ iOS 7.1; ARM64 with ARMv8 Crypto Extensions w/ iOS 7.1; iOS 7.1 w/ iOS 7.1; ARMv7-a w/	11/21/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-128) (AES Val#3123)] "SafeZone FIPS Cryptographic Module is a FIPS 140-2 Security Level 1 validated software cryptographic module from INSIDE Secure. This compact and portable module provides the most commonly needed cryptographic primitives for a large variety of applications, including but not limited to DAR, DRM, TLS, and VPN."
633	Brocade Communications Systems, Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-8000 FAX: 408-333-8101	**Brocade Vyatta Network OS OpenSSL Cryptographic module** **Version 1.0**	Intel Xeon CPU X5560 @ 2.80GHz w/ Brocade Vyatta Series 3500 Network OS 3.2.1R1	11/14/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2598)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3122)] "Built for Network Functions Virtualixation (NFV), Brocade Vyatta 5650 and 5630 vRouters are the first virtual routers capable of providing advance routing in software without sacrificing the

					reliability and performance of hardware networking solutions." *12/09/14: Updated implementation information;*
632	RSA The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Sandy Carielli TEL: 781-515-7510	**RSA BSAFE Crypto-C Micro Edition (ME)** **Version 3.0.0.23**	ARM Cortex A7 Dual Core w/ Linaro Linux (kernel 3.10.33)	11/14/2014	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1959)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#565) (SHS Val#2578) "RSA BSAFE® Crypto-C ME software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. The software supports a wide range of industry standard encryption algorithms offering developers the flexibility to choose the appropriate option to meet their requirements."
631	Red Hat Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (AES-NI and AVX+SSSE3 for SHA) 64 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/14/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2577)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1958)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3119)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3119)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 64bit word size." *03/19/15: Updated implementation information;*
630	Red Hat Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (Straight Assembler SHA) 64bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2575)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1956)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
629	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (Straight Assembler SHA) 32bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2574)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1955)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
628	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Mark Hanson TEL: +1 651 628 1633 FAX: +1 651 628 2706	**McAfee Linux OpenSSL** **Version 1.0.1**	Xeon E5540 w/ MLOS v2.2.3 running on VMware ESXi 5.0 hypervisor	11/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2573)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1954)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3117)] "McAfee Linux cryptographic modules provide cryptographic services for McAfee Linux and security appliance products built upon this platform. McAfee Linux is an operating system built with a focus on the needs of security appliances."

627	McAfee, Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Mark Hanson TEL: +1 651 628 1633 FAX: +1 651 628 2706	**McAfee Linux OpenSSL** **Version 1.0.1 (Firmware)**	Celeron; Core i3; Xeon E5540	11/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2572)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1953)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3116)] "McAfee Linux cryptographic modules provide cryptographic services for McAfee Linux and security appliance products built upon this platform. McAfee Linux is an operating system built with a focus on the needs of security appliances."
626	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (AES-NI and AVX+SSSE3 for SHA) 64 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2570)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1951)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3114)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3114)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 64bit word size." *03/19/15: Updated implementation information;*
625	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (AES-NI and AVX+SSSE3 for SHA)** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2569)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1950)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3113)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3113)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
624	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (AES SSSE3 Assembler AES) 64 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3112)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3112)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
623	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (Straight Assembler AES) 32 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3111)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3111)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
622	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (Straight Assembler AES) 64 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3110)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3110)] "User space library providing general cryptographic services which can be linked to

					from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
621	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (AES SSSE3 assembler) 32 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3109)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3109)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
620	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (Straight Assembler SHA) 64 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2568)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1949)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
619	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (Straight Assembler SHA) 32 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2567)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1948)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
618	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (SHA SSSE3 Assembler SHA) 64 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2566)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1947)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
617	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (SHA SSSE3 Assembler SHA) 32 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2565)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1946)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
616	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (AES SSSE3 assembler) 32 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3108)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3108)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*

615	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (AES SSSE3 Assembler AES) 64 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3107)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3107)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
614	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (AES-NI and AVX+SSSE3 for SHA) 32 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2565)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1946)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3106)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3106)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
613	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (Straight Assembler AES) 32 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3105)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3105)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
612	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (Straight Assembler AES) 64 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3104)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3104)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
611	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (SHA SSSE3 Assembler SHA) 32bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2564)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1945)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
610	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann Marie Rubin	**OpenSSL (SHA SSSE3 Assembler SHA) 64 bit** **Version 1.0.1e-30.el6_6.5**	Intel x86 w/ Red Hat Enterprise Linux 6.6	11/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2563)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1944)] "User space library providing general cryptographic services which can be linked to from any program. The module was tested with 32bit word size." *03/19/15: Updated implementation information;*
609	Apple Inc. 1 Infinite Loop	**Apple OSX CoreCrypto Kernel Module (Assembler AES, Xeon)**	Intel Xeon w/ OSX 10.10	11/7/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES

	Cupertino, CA 95014 USA -Shawn Geddis	**Version 5.0**			Val#3102)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and assembler optimized AES."
608	Chunghwa Telecom Co., Ltd. Telecommunication Laboratories No.99, Dianyan Rd. Yang-Mei, Taoyuan 326 Taiwan, ROC -Yeou-Fuh Kuan TEL: +886-3-424-4333 FAX: +886-3-424-4129 -Char-Shin Miou TEL: +886-3-424-4381 FAX: +886-3-424-4129	**HiKey Cryptographic Library** **Version 3.6 (Firmware)**	Renesas RS-4 series	11/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2557)] "HiKey Cryptographic Library v3.6 supports SHA-1, SHA-256, SHA-384, SHA-512, Hash-DRBG, 3DES-3Key-MAC, 3DES-3Key encrypt/decrypt, ECDSA(p-224/256/384), RSA 2048 encrypt/decrypt (including RSA-CRT), RSA signature generation /verification (including RSA-CRT) and APDU command/response encryption and/or MAC."
607	OpenSSL Software Foundation, Inc. 1829 Mount Ephraim Road Adamstown, MD 27101 USA -Steve Marquess TEL: 877-673-6775	**OpenSSL FIPS Object Module** **Version 2.0.9**	Apple A7 (ARMv8) with NEON w/ Apple iOS 7.1 64-bit; Apple A7 (ARMv8) without NEON w/ Apple iOS 7.1 64-bit ; Arm920Tid (ARMv4) w/ TS-Linux 2.4	10/31/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2553)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1937)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3090)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3090)] "The OpenSSL FIPS Object Module is a full featured general purpose cryptographic library that is distributed in source code form under an open source license. It can be downloaded from www.openssl.org/source/." *12/04/14: Added new tested information;*
606	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann-Marie Rubin	**Red Hat NSS Softoken (64 bit)** **Version 3.14.3-22**	Intel x86 w/ Red Hat Enterprise Linux 6.6	10/31/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2552)] "User space library providing general cryptographic services used by the NSS cryptographic library. The module was tested with 64bit word size on IBM hardware." *11/18/14: Updated implementation information;* *12/16/14: Updated implementation information;* *02/23/15: Update implementation information;*
605	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann-Marie Rubin	**Red Hat NSS Softoken (32 bit)** **Version 3.14.3-22**	Intel x86 w/ Red Hat Enterprise Linux 6.6	10/31/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2551)] "User space library providing general cryptographic services used by the NSS cryptographic library. The module was tested with 64bit word size on IBM hardware." *11/18/14: Updated implementation information;* *12/16/14: Updated implementaion information;* *02/23/15: Update implementation information;*
604	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann-Marie Rubin	**Red Hat NSS Softoken (64 bit)** **Version 3.14.3-22**	Intel x86 w/ Red Hat Enterprise Linux 6.6	10/31/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2550)] "User space library providing general cryptographic services used by the NSS cryptographic library. The module was tested with 64bit word size on HP hardware." *11/17/14: Updated implementation information;* *12/16/14: Updated implementation information;* *02/23/15: Update implementation information;*
603	Red Hat, Inc. 100 East David Street Raleigh, NC 27601 USA -Ann-Marie Rubin	**Red Hat NSS Softoken (32 bit)** **Version 3.14.3-22**	Intel x86 w/ Red Hat Enterprise Linux 6.6	10/31/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2549)] "User space library providing general cryptographic services used by the NSS cryptographic library. The module was tested with 64bit word size on HP hardware." *11/17/14: Update implementation information;* *12/16/14: Updated implementation information;*

					02/23/15: Updated implementation information;
602	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (AES-NI with optimized modes, Xeon)** **Version 5.0**	Intel Xeon w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3070)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
601	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (AES-NI with optimized modes, i7)** **Version 5.0**	Intel i7 w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3069)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
600	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (AES-NI with optimized modes, i5)** **Version 5.0**	Intel i5 w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3068)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
599	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (Assembler AES, i7)** **Version 5.0**	Intel i7 w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3067)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and assembler optimized AES."
598	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (Assembler AES, i5)** **Version 5.0**	Intel i5 w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3066)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and assembler optimized AES."
597	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (AES-NI with optimized modes, Xeon 32bit)** **Version 5.0**	Intel Xeon w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3060)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS compiled for 32bit word size."
596	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (AES-NI with optimized modes, Xeon)** **Version 5.0**	Intel Xeon w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3059)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
595	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (AES-NI with optimized modes, i7 32bit)** **Version 5.0**	Intel i7 w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3058)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS compiled for 32bit word size."
594	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (AES-NI with optimized modes, i7)** **Version 5.0**	Intel i7 w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3057)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."

593	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (AES-NI with optimized modes, i5 32bit)** **Version 5.0**	Intel i5 w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3056)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS compiled for 32bit word size."
592	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (AES-NI with optimized modes, i5)** **Version 5.0**	Intel i5 w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3055)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
591	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Assembler AES, Xeon 32bit)** **Version 5.0**	Intel Xeon w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3047)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES compiled for 32bit word size."
590	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Assembler AES, Xeon)** **Version 5.0**	Intel Xeon w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3046)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
589	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Assembler AES, i7)** **Version 5.0**	Intel i7 w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3045)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
588	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Assembler AES, i7 32bit)** **Version 5.0**	Intel i7 w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3044)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES compiled for 32bit word size."
587	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Assembler AES, i5 32bit)** **Version 5.0**	Intel i5 w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3043)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES compiled for 32bit word size."
586	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Assembler AES, i5)** **Version 5.0**	Intel i5 w/ OSX 10.10	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3042)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
585	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A6X)** **Version 5.0**	Apple A6X w/ iOS 8	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3038)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
584	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A5X)** **Version 5.0**	Apple A5X w/ iOS 8	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3037)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."

583	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A5)** **Version 5.0**	Apple A5 w/ iOS 8	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3036)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
582	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A8 32bit)** **Version 5.0**	Apple A8 w/ iOS 8	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3035)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES compiled for 32bit word size."
581	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A8)** **Version 5.0**	Apple A8 w/ iOS 8	10/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3034)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
580	Intel Corporation 2200 Mission College Blvd Santa Clara, CA 95054 USA -Ammon J Christiansen TEL: (503)-712-4557 -DJ Johnston TEL: (503)712-4457	**Rangeley DRNG** **Part # RTL1p0**	N/A	10/16/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-128) (AES Val#3032)] "Digital Logic Design implementation SP 800-90A AES-CTR-DRBG." *03/02/15: Updated vendor information;*
579	Certicom Corp. 4701 Tahoe Blvd, Building A Mississauga, Ontario L4W 0B5 Canada -Certicom Support TEL: 1-905-507-4220 FAX: 1-905-507-4230 -Certicom Sales TEL: 1-905-507-4220 FAX: 1-905-507-4230	**Security Builder® FIPS Core** **Version 6.0.2.1**	Intel Core i7-2720QM w/ AES-NI w/ Windows 7 Enterprise 64-bit; ARMv7 w/ Windows Phone 8.0; ARMv7 w/ Android 4.4.2; Intel Atom CPU Z2460 w/ Android 4.0.4; ARMv7 w/ iOS version 6.1.4 ; ARMv8 w/ Android 5.0.1; ARMv7S w/ iOS 6.1.4; ARMv8 w/ iOS 8.0; Intel Xeon with AES-NI w/ Windows 7; Intel Xeon E5620 with AES-NI w/ CentOS Linux Release 7.1 64-bit; Intel Core i7-3615QM w/ Mac OS X Yosemite 10.10.4	10/16/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2530)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#1914)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3029)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-256) (P-384: , SHA-384) (P-521: , SHA-512) (ECDSA Val#553) (SHS Val#2530) "Security Builder® FIPS Core provides application developers with cryptographic tools to easily integrate encryption, digital signatures and other security mechanisms into C-based apps for FIPS 140-2 and Suite B security. It can also be used with Certicom's PKI, IPSec SSL and IPSec and SSL modules." *04/13/15: Updated vendor and implementation information;* *10/09/15: Added new tested information;*
578	EROAD Inc. Level 3 260 Oteha Valley Road Albany, North Shore 0632 Auckland, * * New Zealand -Bruce Wilson TEL: +64 9 927 4700 FAX: +64 9 927 4701	**The EROAD Cryptographic Library** **Version 1.0 (Firmware)** **Part # MK70FN1M0VMJ12**	MK70FN1M0VMJ12	10/16/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2517)] "The EROAD Cryptographic Module is the heart of EROAD's advanced GNSS based transport technology. It is a secure, high performance, cryptographic processing engine and has been designed to meet FIPS-140-2 at Security Level 3. It is used within the EROAD product suite to provide trusted cryptographic security services."
577	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A7 32bit)** **Version 5.0**	Apple A7 w/ iOS 8	10/16/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3017)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES compiled for 32bit word size."
576	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A7)** **Version 5.0**	Apple A7 w/ iOS 8	10/16/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3016)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks.

					The testing applies to user space and assembler optimized AES."
575	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A6)** **Version 5.0**	Apple A6 w/ iOS 8	10/16/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#3015)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
574	Broadcom Corporation 5300 California Avenue Irvine, CA 92617 USA -Mark Litvack TEL: 408-919-4428	**Broadcom Crypto firmware** **Version 1.0 (Firmware)** **Part # XLP200 B0**	XLP200 series	10/16/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3014)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3014)] "The XLP200 series (XLP104, XLP108, XLP204, XLP208) of multi-core processors can deliver an unprecedented 160Gbps throughput and 240 million packets-per-second of application performance for next-generation 3G/4G mobile wireless infrastructure, enterprise, storage, security, metro, edge and core infrastructure network applications."
573	LG Electronics Inc. 20 Yoido-dong Youngdungpo-gu Seoul, n/a 152-721 Republic of Korea -Joonwoong Kim TEL: 82 10 2207 1919 FAX: 82 2 6950 2080	**OpenSSL Cryptographic Library** **Version 1.0.1e**	Qualcomm Snapdragon 800 w/ Android 4.4.2	9/30/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2519)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1903)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#3011)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#3011)] "General-purpose cryptographic services available for Android used by LG devices to provide secured services to applications via the OpenSSL FIPS Object Module, which is a full featured general purpose cryptographic library."
572	Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**ACT2-Lite** **Part # 15-14497-02(NDS_ACT2_V1)**	N/A	9/26/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#3002)] "ACT-2Lite is an ASSP which is based on a smart card hardware platform with custom ROM code provided by Cisco."
571	Hewlett-Packard Company 153 Taylor Street Littleton, MA 01460 USA -Bob Pittman TEL: 1-978-264-5211 FAX: 1-978-264-5522	**HP Comware** **Version ComwareV7.1-R1005 (Firmware)**	Broadcom XLP316, 1.2GHz, MIPS	9/19/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2989)] "Comware cryptographic library is a software library that provides cryptographic functions within HP devices."
570	Apriva ISS LLC 8501 North Scottsdale Road Suite 110 Scottsdale, AZ 85253 USA -Robert Smith TEL: 480-421-1227 FAX: 480-994-3190 -Randy Best TEL: 480-421-1204 FAX: 480-994-3190	**Apriva CTR_DRBG** **Version 1.0**	Intel Xeon with AES-NI w/ Red Hat Enterprise Linux 6	9/12/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2234)] "The Apriva CTR_DRBG is used to generate cryptographic keys for the Apriva VPN Server."
569	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**Brocade FastIron IP product Crypto Library** **Version BRCD-IP-CRYPTO-VER-3.0 (Firmware)**	Dual-core ARM Cortex A9 1Ghz	9/12/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2505)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2981)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2981)] "This Brocade cryptographic library is used in Brocade FastIron based switches to implement the cryptographic related modules." *08/04/15: Updated implementation information;*

568	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-8000 FAX: 408-333-8101	**Brocade Vyatta Network OS OpenSSL Cryptographic Module** **Version 1.0**	Intel Xeon Processor E5-2680 v2 (25 M Cache, 2.80 GHz) w/ Brocade Vyatta Network OS 3.2.1R1	9/12/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2503)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1888)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2979)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2979)] "Built for Network Functions Virtualixation (NFV), Brocade Vyatta 5650 and 5630 vRouters are the first virtual routers capable of providing advance routing in software without sacrificing the reliability and performance of hardware networking solutions." *12/09/14: Updated implementation information;*
567	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Mark Hanson TEL: +1 651 628 1633 FAX: +1 651 628 2706	**RSA BSAFE Crypto-J** **Version 6.1**	Intel Xeon w/ McAfee Linux 2.2.3 running on VMware ESXi 5.0	9/12/2014	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1885)] "McAfee Firewall Enterprise Control Center simplifies the management of multiple McAfee Firewall Enterprise appliances. Control Center enables centralized management and monitoring of the McAfee Firewall Enterprise solutions, allowing network administrators to centrally define firewall policy, deploy updates and inventory their firewall products."
566	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Mark Hanson TEL: +1 651 628 1633 FAX: +1 651 628 2706	**RSA BSAFE Crypto-J** **Version 6.1**	Intel Celeron w/ McAfee Linux 2.2.3; Intel Xeon w/ McAfee Linux 2.2.3	9/12/2014	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1884)] "McAfee Firewall Enterprise Control Center simplifies the management of multiple McAfee Firewall Enterprise appliances. Control Center enables centralized management and monitoring of the McAfee Firewall Enterprise solutions, allowing network administrators to centrally define firewall policy, deploy updates and inventory their firewall products."
565	Dell Inc 5450 Great America Parkway Santa Clara, CA 95054 US -Jan Provan TEL: (510) 377-1842	**Dell OpenSSL Cryptographic Library** **Version 2.1**	Intel Centerton w/ Dell Networking Operating System E9.6.0.0; FreeScale PowerPC e500 w/ Dell Networking Operating System E9.6.0.0; Intel Xeon w/ Dell Networking Operating System E9.6.0.0; Broadcom XLP w/ Dell Networking Operating System E9.6.0.0	9/12/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2971)] BlockCipher_No_df: (, AES-256) (AES Val#2971)] "Dell OpenSSL Cryptographic Library v2.1 provides a variety of cryptographic services used by Dell's Data Center hardened Dell Networking OS management and routing features." *12/16/14: Updated vendor information;*
564	N/A	**N/A**	N/A	9/12/2014	N/A
563	Samsung Electronics Co.,Ltd. Samsung 1-ro Hwaseong-si, Gyeonggi-do 275-18 Korea -Jisoo Kim TEL: 82-31-3096-2832 FAX: 82-31-8000-8000	**Secure UFS (Universal Flash Storage)** **Part # Hash_DRBG V1.0**	N/A	9/12/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2494)] "Secure UFS is a high-performance embedded storage that provides on-the-fly encryption/decryption of user data without performance loss. It implements AES256-XTS for user data encryption, ECDSA P-224 for FW authentication, and Hash_DRBG for key generation." *02/03/15: Updated implementation information;*
562	Ciena Corporation 7035 Ridge Road Hanover, MD 21076 USA -Patrick Scully TEL: 613-670-3207	**Ciena 6500 Packet-Optical Platform 4x10G Cryptography Engine** **Version 1.10 (Firmware)**	Xilinx XC7Z045	8/29/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2963)] BlockCipher_No_df: (, AES-256) (AES Val#2963)] "The Ciena 6500 Packet-Optical Platform 4x10G Encryption OTR offers an integrated transport encryption solution providing a protocol-agnostic wirespeed encryption service for use in small to large enterprises or datacenters and also offered through service providers as a differentiated managed service."
561	Kaspersky Lab UK Ltd. 1st Floor, 2 Kingdom Street Paddington	**Kaspersky Cryptographic Library 64-bit (User Mode)** **Version 2.0**	Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz w/ Windows 7 Enterprise 64-bit; Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz w/ Windows 8.1 Enterprise 64-bit; Intel(R)	8/29/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2492)]

	London, W2 6BD United Kingdom -Oleg Andrianov TEL: +7 495 797 8700		Core(TM)2 Duo P9600 @ 2.53GHz w/ Kaspersky Preboot OS with UEFI		**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#1879)] "Kaspersky Cryptographic Library is a software library that provides cryptographic services for various Kaspersky Lab applications." *09/25/15: Added new tested information;*
560	Kanguru Solutions 1360 Main Street Millis, MA 02054 USA -Nate Cote TEL: 508-376-4245 FAX: 508-376-4462	**Kanguru Defender 300/3000 USB Drive** **Version 2.10.10 (Firmware)** **Part # KDF3K-CM**	v2.10.10	8/28/2014	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256) (HMAC Val#1878)] "The Kanguru Defender 3000 and Kanguru Defender Elite300 are 256-bit AES hardware encrypted USB flash drives. They are used to securely store sensitive data on the device or run secure applications from the drive. The Kanguru Defender line of products is remotely manageable through the Kanguru Remote Management Console(KRMC)."
559	Exar Corporation 48720 Kato Road Fremont, CA 94538 USA -Larry Hu TEL: 510-668-7145 FAX: 510-668-7028 -Bin Wu TEL: 86-13777873933 FAX: 86-571-88156615	**Exar XR92xx series die** **Part # XR9240**	N/A	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-256 , SHA-512) (P-384: , SHA-256 , SHA-512) (P-521: SHA-256 , SHA-512) (SHS Val#2490) "The XR92xx provides hardware acceleration of compression, encryption and authentication algorithms including gzip/zlib/Deflate, LZS/eLZS, AES, 3DES, RC4, SHA, HMAC, GMAC and public key algorithms such as DSA, DH, RSA, ECDSA, ECDH and is designed to optimize SSL/IPsec/SRTP packet processing."
558	Kaspersky Lab UK Ltd. 1st Floor, 2 Kingdom Street Paddington London, W2 6BD United Kingdom -Oleg Andrianov TEL: +7 495 797 8700	**Kaspersky Cryptographic Library 64-bit (Kernel Mode)** **Version 2.0**	Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz w/ Windows 7 Enterprise 64-bit; Intel(R) Core(TM) i7-3770S CPU @ 3.10GHz w/ Windows 8.1 Enterprise 64-bit	8/28/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2489)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#1876)] "Kaspersky Cryptographic Library is a software library that provides cryptographic services for various Kaspersky Lab applications." *09/25/15: Added new tested information;*
557	Kaspersky Lab UK Ltd. 1st Floor, 2 Kingdom Street Paddington London, W2 6BD United Kingdom -Oleg Andrianov TEL: +7 495 797 8700	**Kaspersky Cryptographic Library 32-bit (Kernel Mode)** **Version 2.0**	Intel(R) Core(TM)2 Duo P9600 @ 2.53GHz w/ Windows 7 Professional 32-bit	8/28/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2488)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#1875)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-256) (AES Val#2956)] BlockCipher_No_df: (AES-128 , AES-256) (AES Val#2956)] "Kaspersky Cryptographic Library is a software library that provides cryptographic services for various Kaspersky Lab applications." *09/25/15: Added new tested information;*
556	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Klaus Majewski TEL: +358-40-824-7908 -Jorma Levomäki TEL: +358-9-476711	**McAfee NGFW Cryptographic Library Module (320)** **Version 2.0**	Intel Atom Processor D525 w/ GNU / Linux (Debian) 6.0 -based distribution	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2955)] "McAfee NGFW Cryptographic Library is a software module that provides cryptographic services required by the McAfee NGFW product."
555	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Klaus Majewski TEL: +358-40-824-7908	**McAfee NGFW Cryptographic Library (1035)** **Version 2.0**	Intel Celeron Processor 725c with AES-NI w/ GNU / Linux (Debian) 6.0 -based distribution	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2954)] "McAfee NGFW Cryptographic Library is a software module that provides cryptographic services required by the McAfee NGFW product."

	-Jorma Levomäki TEL: +358-9-476711				
554	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Klaus Majewski TEL: +358-40-824-7908 -Jorma Levomäki TEL: +358-9-476711	**McAfee NGFW Cryptographic Library Module (1065)** **Version 2.0**	Intel Core i3-2115c with AES-NI w/ GNU / Linux (Debian) 6.0 -based distribution	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2953)] "McAfee NGFW Cryptographic Library is a software module that provides cryptographic services required by the McAfee NGFW product."
553	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Klaus Majewski TEL: +358-40-824-7908 -Jorma Levomäki TEL: +358-9-476711	**McAfee NGFW Cryptographic Library Module (1402)** **Version 2.0**	Intel Xeon Processor E5-1650v2 with AES-NI w/ GNU / Linux (Debian) 6.0 -based distribution	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2952)] "McAfee NGFW Cryptographic Library is a software module that provides cryptographic services required by the McAfee NGFW product."
552	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Klaus Majewski TEL: +358-40-824-7908 -Jorma Levomäki TEL: +358-9-476711	**McAfee NGFW Cryptographic Library Module (3202)** **Version 2.0**	Intel Xeon Processor E5-2660 with AES-NI w/ GNU / Linux (Debian) 6.0 -based distribution	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2951)] "McAfee NGFW Cryptographic Library is a software module that provides cryptographic services required by the McAfee NGFW product."
551	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Klaus Majewski TEL: +358-40-824-7908 -Jorma Levomäki TEL: +358-9-476711	**McAfee NGFW Cryptographic Library Module (3202a)** **Version 2.0**	Intel Xeon Processor E5-2660 without AES-NI w/ GNU / Linux (Debian) 6.0 -based distribution	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2950)] "McAfee NGFW Cryptographic Library is a software module that provides cryptographic services required by the McAfee NGFW product."
550	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Klaus Majewski TEL: +358-40-824-7908 -Jorma Levomäki TEL: +358-9-476711	**McAfee NGFW Cryptographic Library Module (3206)** **Version 2.0**	Intel Xeon Processor E5-2680 with AES-NI w/ GNU / Linux (Debian) 6.0 -based distribution	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2949)] "McAfee NGFW Cryptographic Library is a software module that provides cryptographic services required by the McAfee NGFW product."
549	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Klaus Majewski TEL: +358-40-824-7908 -Jorma Levomäki TEL: +358-9-476711	**McAfee NGFW Cryptographic Library Module (3206a)** **Version 2.0**	Intel Xeon Processor E5-2680 without AES-NI w/ GNU / Linux (Debian) 6.0 -based distribution	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2948)] "McAfee NGFW Cryptographic Library is a software module that provides cryptographic services required by the McAfee NGFW product."
548	Hewlett-Packard Company 153 Taylor Street Littleton, MA 01460 USA -Bob Pittman TEL: 1-978-264-5211 FAX: 1-978-264-5522	**HP Comware** **Version Comware V7.1-R2311 (Firmware)**	RMI(Netlogic) XLS408, 1.2GHz, MIPS	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2945)] "Comware cryptographic library is a software library that provides cryptographic functions within HP devices."
547	Hewlett-Packard Company 153 Taylor Street Littleton, MA 01460 USA -Bob Pittman TEL: 1-978-264-5211 FAX: 1-978-264-5522	**HP Comware** **Version Comware V7.1-R2111 (Firmware)**	Broadcom XLP316, 1.2GHz, MIPS	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2944)] "Comware cryptographic library is a software library that provides cryptographic functions within HP devices."
546	Hewlett-Packard Company 153 Taylor Street Littleton, MA 01460 USA	**HP Comware** **Version Comware V7.1-R2406 (Firmware)**	Freescale P2020, 1.2GHz, PowerPC	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2943)] "Comware cryptographic library is a software library that provides cryptographic functions

	-Bob Pittman TEL: 1-978-264-5211 FAX: 1-978-264-5522				within HP devices."
545	Hewlett-Packard Company 153 Taylor Street Littleton, MA 01460 USA -Bob Pittman TEL: 1-978-264-5211 FAX: 1-978-264-5522	**HP Comware** **Version Comware V7.1-R7328 (Firmware)**	Freescale MPC8548, 1.0GHz, PowerPC	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2942)] "Comware cryptographic library is a software library that provides cryptographic functions within HP devices."
544	Oracle Corporation 4220 Network Circle Santa Clara, CA 95054 USA -Joshua Brickman TEL: +1 781 442 0451 FAX: +1 781 442 0451 -Tyrone Stodart	**Java Card Platform for Infineon on SLE 78 (SLJ 52GxxyyyzR)** **Version 1.0f (Firmware)** **Part # SLE78 M7892B11**	Infineon SLE78 M7892B11 smart card microcontroller	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-128) (AES Val#2941)] "The TOE is a part of Java Card Platform (JCP) composed of a Smart Card Platform (SCP) and embedded software. Validation covers straight RSA as well as RSA in CRT implementation." *04/15/15: Updated implementation information;*
543	Hewlett-Packard Company 153 Taylor Street Littleton, MA 01460 USA -Bob Pittman TEL: 1-978-264-5211 FAX: 1-978-264-5522	**HP Comware with Hardware Accelerators** **Version 5.2.109 (Firmware)**	P1020, 880MHz, PowerPC; XLP432, 1.4GHz, MIPS; XLR732, 950Mhz, MIPS; XLS208, 750Mhz, MIPS	8/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2940)] "Comware cryptographic library is a software library that provides cryptographic functions within HP devices."
542	Microsemi Corporation One Enterprise Aliso Viejo, CA 92656 USA -Richard Newell TEL: +1 (408) 643-6146	**Microsemi SoC Cryptographic Module Mark II** **Version 1.1 (Firmware)**	Mentor Graphics Questa Simulator 10.1c	8/11/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2935)] "The Microsemi SoC Cryptographic Module provides custom hardware/firmware acceleration of the standard cryptographic algorithms used in Microsemi FPGAs and SoC FPGAs like Igloo®2 and SmartFusion®2. They are used to securely configure the devices, and are also made available to the FPGA user via an internal bus interface for use in end applications."
541	Blue Coat Systems Inc. 420 North Mary Avenue Sunnyvale, California 94085-4121 USA -Diana Robinson TEL: +1 (845) 454-6397 -Tammy Green TEL: +1 (801) 999-2973	**Blue Coat SGOS Crypto Library** **Version 3.1.4 (Firmware)**	Intel Xeon E5-2418L; Intel Xeon E5-2430; Intel Xeon E5-2658	8/11/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2931)] BlockCipher_No_df: (, AES-256) (AES Val#2931)] "The Blue Coat Crypto Library v1.0 provides the necessary cryptographic services to a proprietary operating system (SGOS 6.5.2) developed specifically for use in Blue Coat's ProxySG line of appliances."
540	OpenSSL Software Foundation Inc. 1829 Mount Ephraim Road Adamstown, MD 27101 USA -Steve Marquess TEL: 877-673-6775	**OpenSSL FIPS Object Module** **Version 2.0.8**	Xeon E5-2430L (x86) without AES-NI w/ FreeBSD 10.0; Xeon E5-2430L (x86) with AES-NI w/ FreeBSD 10.0; Intel Xeon E5440 (x86) 32-bit without AES-NI w/ FreeBSD 8.4; Intel Xeon E3-1220 (x86) without AES-NI w/ VMware Horizon Workspace 2.1 under vSphere; Intel Xeon E3-1220 (x86) with AES-NI w/ VMware Horizon Workspace 2.1 under vSphere; Freescale i.MX25 (ARMv4) w/ QNX 6.5	8/11/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2465)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1856)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2929)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2929)] "The OpenSSL FIPS Object Module is a full featured general purpose cryptographic library that is distributed in source code form under an open source license. It can be downloaded from www.openssl.org/source/." *09/22/14: Added new tested information;* *10/29/14: Added new tested information;*
539	Blue Coat Systems, Inc. 420 North Mary Avenue Sunnyvale, California 94085-4121 USA -Diana Robinson TEL: +1 (845) 454-6397 -Tammy Green TEL: +1 (801) 999-2973	**SGOS 6.5 Cryptographic Library** **Version 3.1.3 (Firmware)**	AMD64 Opteron (Istanbul); AMD64 Opteron (Shanghai); Intel Clarkdale; Intel Lynnfield; VIA NANO	7/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2925)] BlockCipher_No_df: (, AES-256) (AES Val#2925)] "The SGOS 6.5 Cryptographic Library provides the necessary cryptographic services to a proprietary operating system (SGOS 6.5) developed specifically for use on a series of hardware appliances that serve as Internet proxy and Wide Area Network (WAN) optimizer devices."

538	Fortinet Inc. 899 Kifer Road Sunnyvale, CA 94086 USA -Alan Kaye TEL: 613-225-9381 FAX: 613-225-2951	**FortiClient FCCrypt Cryptolibrary v5.0** **Version 5.0**	Intel Core 2 Duo w/ Windows 7 Enterprise ; N/A	7/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2912)] "The FCCrypt library provides the following services for the FortiClient 5.0: HMAC, SHA-1, SHA-256, AES CBC, AES ECB, 3DES, RSA and NIST 800-90A RBG."
537	Oberthur Technologies 402 rue d'Estienne d'Orves Colombes, n/a 92700 France -GOYET Christophe TEL: +1 703 322 8951 -BOUKYOUD Saïd TEL: +33 1 78 14 72 58 FAX: +33 1 78 14 70 20	**DRBG on Cosmo V8** **Version 07831.4 (Firmware)** **Part # 0F**	ID-One PIV-C on Cosmo V8 ; N/A	7/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2910)] "ID-One Cosmo V8 is a dual interface (ISO 7816 & ISO 14443) smartcard hardware platform compliant with Javacard 3.0.1 and GlobalPlatform 2.2.1 chip which includes a NIST SP800-90 compliant DRBG relying on block cipher AES, thus providing security strength of 17." *08/07/14: Updated implementation information;*
536	Beijing Huada Infosec Technology Co. Ltd 4F,Tower B,Yandong Building No.2 Wanhong West Street Chaoyang District Beijing, Beijing 100015 P.R.China -Junmai Zhang TEL: 13810645150 FAX: 84505865 -Yanhua Liu TEL: 13811696396 FAX: 84505865	**ISRNG01 V1.0** **Version V1.0 (Firmware)**	IS8U256A with 8-bit ISC8051 embedded ; N/A	7/31/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2448)] "ISRNG01 V1.0 Hardware Cryptographic Library provides core cryptographic functionality for Beijing Huada Infosec's security IC providing a capability to develop complex and flexible security applications."
535	Microsemi Corporation One Enterprise Aliso Viejo, CA 92656 USA -Richard Newell TEL: +1 (408) 643-6146	**Microsemi SoC Cryptographic Module Mark I** **Version 1.0 (Firmware)**	Mentor Graphics Questa Simulator 10.1c ; N/A	7/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2908)] "The Microsemi SoC Cryptographic Module provides custom hardware/firmware acceleration of the standard cryptographic algorithms used in Microsemi FPGAs and SoC FPGAs like Igloo®2 and SmartFusion®2. They are used to securely configure the devices, and are also made available to the FPGA user via an internal bus interface for use in end applications."
534	Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification team	**IOS Common Cryptographic Module (IC2M) Algorithm Module** **Version 2.0 (Firmware)**	Atheros QCA9550; Freescale SC1018; Freescale SC1023 ; N/A	7/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2901)] "IOS Common Cryptographic Module" *07/10/15: Updated implementation information;*
533	Canon Inc. 30-2 Shimomaruko 3-chome Ohta-ku, Tokyo 146-8501 Japan -Yoichi Toyokura TEL: +81-3-3758-2111 FAX: +81-3-3758-1160	**Canon MFP Security Chip** **Version 2.10 (Firmware)**	FR80E	7/18/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2446)] "Canon MFP Security Chip provides high-performance data encryption and decryption via SATA interface."
532	Atmel Corporation 1150 E. Cheyenne Mountain Blvd Colorado Springs, CO 80906 USA -Jim Hallman TEL: (919) 846-3391	**ATECC108A** **Version 0x1003 (Firmware)**	Cadence NC Verilog hardware simulator	7/18/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-128) (AES Val#2905)] "Atmel CryptoAuthentication: Secure authentication and product validation device."
531	Hewlett-Packard Development Company, L.P. 20555 State Highway 249 Houston, TX 77070 USA -Catherine Schwartz TEL: (281) 514-9658 -Jaycee Murlidar TEL: (248) 840-5144	**HP Secure Encryption Engine v1.0** **Part # PM8064**	N/A	7/10/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-256) (AES Val#2904)] "HP Secure Encryption is a controller-based data encryption solution for HP ProLiant Gen8 or newer servers that protects data at rest on any bulk storage attached to the HP Smart Array controller. The solution comprises our 12G family of HP Smart Array controllers, the HP Physical Security Kit, and the HP Secure Encryption licensing." *06/01/15: Updated implementation information;* *06/16/15: Updated vendor information;*

530	Hewlett-Packard Development Company L.P. 20555 State Highway 249 Houston, TX 77070 USA -Catherine Schwartz TEL: (281) 514-9658 -Jaycee Murlidar TEL: (248) 840-5144	**HP Secure Encryption Engine v1.0** **Part # PM8062**	N/A	7/10/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-256) (AES Val#2903)] "HP Secure Encryption is a controller-based data encryption solution for HP ProLiant Gen8 or newer servers that protects data at rest on any bulk storage attached to the HP Smart Array controller. The solution comprises our 12G family of HP Smart Array controllers, the HP Physical Security Kit, and the HP Secure Encryption licensing." *06/01/15: Updated implementation information; 06/16/15: Updated vendor information;*
529	Hewlett-Packard Development Company, L.P. 20555 State Highway 249 Houston, TX 77070 USA -Catherine Schwartz TEL: (281) 514-9658 -Jaycee Murlidar TEL: (240)840-5144	**HP Secure Encryption Engine v1.0** **Part # PM8061**	N/A	7/10/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-256) (AES Val#2902)] "HP Secure Encryption is a controller-based data encryption solution for HP ProLiant Gen8 or newer servers that protects data at rest on any bulk storage attached to the HP Smart Array controller. The solution comprises our 12G family of HP Smart Array controllers, the HP Physical Security Kit, and the HP Secure Encryption licensing." *06/01/15: Updated implementation information; 06/16/15: Updated vendor information;*
528	Aruba Networks Inc. 1344 Crossman Ave Sunnyvale, CA 94089 USA -Jon Green TEL: 408-227-4500 FAX: 408-227-4550 -Steve Weingart TEL: 1-830-580-1544	**ArubaOS OpenSSL Module** **Version ArubaOS 6.4 (Firmware)**	Broadcom XLP Series; Freescale QorIQ P10XX Series	7/10/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2900)] "The Aruba MOVE Architecture forms the core network infrastructure for supporting mobile and wireless computing devices. The system enables enterprise-scale 802.11 wireless LANs (Wi-Fi), secure remote VPNs, and mobility-optimized wired networks. The Broadcom XLP Series includes Broadcom XLP 204, XLP 208, XLP 316, XLP 408, XLP 416 and XLP 432 processors; the Freescale QorIQ P10XX Series includes P1010 and P1020 processors." *12/04/14: Updated implementation information; 12/24/14: Updated implementation information; 08/18/15: Updated implementation information;*
527	Integral Memory PLC. Unit 6 Iron Bridge Close Iron Bridge Business Park Off Great Central Way London, Middelsex NW10 0UF United Kingdom -Patrick Warley TEL: +44 (0)20 8451 8700 FAX: +44 (0)20 8459 6301 -Samik Halai TEL: +44 (0)20 8451 8704 FAX: +44 (0)20 8459 6301	**Integral Crypto AES 256 Bit USB 3.0 Firmware Library** **Version 1.0 (Firmware)**	PS2251-15	7/10/2014	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256) (HMAC Val#1834)] "The Integral Crypto AES 256 Bit USB 3.0 Firmware Library is intended for use with The Integral Crypto AES 256 Bit USB 3.0 Cryptographic Modules. The modules are removable storage devices which encrypt the content transferred onto them, and come in 2GB, 4GB, 8GB, 16GB, 32GB, 64GB, 128GB, 256GB, 512GB and 1TB sizes."
526	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**OSSL** **Version Openssl-0.9.8g-8.0.0 (Firmware)**	Cavium 56XX	7/10/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2894)] "Cisco WLAN Controllers provide centralized control, management and scalability for small, medium and large-scale Government WLAN networks using APs joined over secure DTLS connection and support IEEE 802.11i security standard with WPA2 to enable a Secure Wireless Architecture." *10/14/2014: Added KDF 800-135 IKEv1 KDF and SNMP KDF and updated implementation description.*
525	Juniper Networks, Inc. 1194 N. Mathilda Ave. Sunnyvale, CA 94089 USA -Ajit Kumar Singh Parihar TEL: +91 8030539304	**OPENSSL** **Version Junos 13.2X51-D20 (Firmware)**	Marvell Feroceon 88FR131; Freescale PowerPC e500v2 Core; Junos 13.2X51-D20; Broadcom XLR XLS 400 Series (DCF); Intel Xeon E3-1200 Family (Sandy Bridge)	7/10/2014	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1826)] "Comprehensive, scalable and secure routing solutions specifically designed to meet the needs of both enterprises and service providers. All of our routers - core, Multiservice edge and edge ethernet - run on one common operating system - Junos."
524	Juniper Networks Inc. 1194 N. Mathilda Ave.	**OPENSSL**	Marvell Feroceon 88FR571; Freescale PowerPC e500v2 Core	7/10/2014	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-

	Sunnyvale, CA 94089 USA -Ajit Kumar Singh Parihar TEL: +91 8030539304	**Version Junos 13.2X50-D19 (Firmware)**			224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1825)] "Comprehensive, scalable and secure routing solutions specifically designed to meet the needs of both enterprises and service providers. All of our routers - core, Multiservice edge and edge ethernet - run on one common operating system - Junos."
523	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA -Tim Myers TEL: 800-Microsoft	**Windows Storage Server 2012 R2, Microsoft Windows RT 8.1, Microsoft Surface with Windows RT 8.1, Microsoft Surface Pro with Windows 8.1, Microsoft Surface 2, Microsoft Surface Pro 2, Microsoft Surface Pro 3, Microsoft Windows Phone 8.1, Microsoft Windows Embedded 8.1 Industry and Microsoft StorSimple 8100 Cryptography Next Generation Cryptographic Implementations** **Version 6.3.9600**	NVIDIA Tegra 4 Quad-Core w/ Microsoft Surface 2 w/ Windows RT 8.1 (ARMv7 Thumb-2); NVIDIA Tegra 3 Quad-Core w/ Windows RT 8.1 (ARMv7 Thumb-2); Qualcomm Snapdragon S4 w/ Windows Phone 8.1 (ARMv7 Thumb-2); Qualcomm Snapdragon 400 w/ Windows Phone 8.1 (ARMv7 Thumb-2); Windows Phone 8.1 (ARMv7 Thumb-2) w/ Windows Phone 8.1 (ARMv7 Thumb-2); Qualcomm Snapdragon S4 w/ Windows RT 8.1 (ARMv7 Thumb-2); NVIDIA Tegra 3 Quad-Core w/ Microsoft Surface w/ Windows RT 8.1 (ARMv7 Thumb-2); AMD A4 with AES-NI and PCLMULQDQ and SSSE3 w/ Microsoft Windows 8.1 Enterprise (x64); Intel Core i3 without AES-NI and with PCLMULQDQ and SSSE3 w/ Microsoft Windows 8.1 Enterprise (x64); Intel Core i7 with AES-NI and PCLMULQDQ and SSSE3 w/ Microsoft Windows 8.1 Enterprise (x64); AMD A4 without AES-NI or PCLMULQDQ or SSSE3 w/ Microsoft Windows 8.1 Enterprise (x86); AMD Athlon 64 X2 without AES-NI w/ Microsoft Windows 8.1 Enterprise (x86); Intel Core i7 without AES-NI or PCLMULQDQ or SSSE3 w/ Microsoft Windows 8.1 Enterprise (x86); Intel Pentium without AES-NI w/ Microsoft Windows 8.1 Enterprise (x86); Intel Core i3 without AES-NI and with PCLMULQDQ and SSSE3 w/ Microsoft Windows Embedded 8.1 Industry Enterprise (x64); AMD A4 without AES-NI or PCLMULQDQ or SSSE3 w/ Microsoft Windows Embedded 8.1 Industry Enterprise (x86); AMD A4 with AES-NI and PCLMULQDQ and SSSE3 w/ Microsoft Windows Embedded 8.1 Industry Enterprise (x64); Intel Core i7 with AES-NI and PCLMULQDQ and SSSE3 w/ Microsoft Windows Embedded 8.1 Industry Enterprise (x64); AMD Athlon 64 X2 without AES-NI w/ Microsoft Windows Embedded 8.1 Industry Enterprise (x86); Intel Core i7 without AES-NI or PCLMULQDQ or SSSE3 w/ Microsoft Windows Embedded 8.1 Industry Enterprise (x86); Intel Pentium without AES-NI w/ Microsoft Windows Embedded 8.1 Industry Enterprise (x86); AMD A4 without AES-NI or PCLMULQDQ or SSSE3 w/ Microsoft Windows 8.1 Enterprise (x64); AMD Athlon 64 X2 without AES-NI w/ Microsoft Windows 8.1 Enterprise (x64); Intel Pentium without AES-NI w/ Microsoft Windows 8.1 Enterprise (x64); AMD A4 with AES-NI and PCLMULQDQ and SSSE3 w/ Microsoft Windows Server 2012 R2 (x64); Intel Core i7 with AES-NI and PCLMULQDQ and SSSE3 w/ Microsoft Windows Server 2012 R2 (x64); Intel Core i3 without AES-NI and with PCLMULQDQ and SSSE3 w/ Microsoft Windows Server 2012 R2 (x64); Intel Pentium without AES-NI w/ Microsoft Windows Embedded 8.1 Industry Enterprise (x64); AMD A4 without AES-NI or PCLMULQDQ or SSSE3 w/ Microsoft Windows Embedded 8.1 Industry Enterprise (x64); AMD Athlon 64 X2 without AES-NI w/ Microsoft Windows Embedded 8.1 Industry Enterprise (x64); Intel Core i7 without AES-NI or PCLMULQDQ or SSSE3 w/ Microsoft Windows Embedded 8.1 Industry Enterprise (x64); Intel Core i3 without AES-NI and with PCLMULQDQ and SSSE3 w/ Microsoft Windows Storage Server 2012 R2 (x64); AMD A4 with AES-NI and PCLMULQDQ and SSSE3 w/ Microsoft Windows Storage Server 2012 R2 (x64); Intel Core i7 with AES-NI and PCLMULQDQ and SSSE3 w/ Microsoft Windows Storage Server 2012 R2 (x64);	7/10/2014	**Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-256) (ECDSA Val#505) (SHS Val#2373) "The Microsoft Windows Kernel Mode Cryptographic Primitives Library -- Cryptography Next Generation (CNG) -- is a general purpose, software-based, cryptographic module which provides FIPS 140-2 Level 1 cryptography." *12/11/14: Added new tested information;* *03/13/15: Added new tested information;*

			AMD A4 without AES-NI or PCLMULQDQ or SSSE3 w/ Microsoft Windows Server 2012 R2 (x64); AMD Athlon 64 X2 without AES-NI w/ Microsoft Windows Server 2012 R2 (x64); Intel Core i7 without AES-NI or PCLMULQDQ or SSSE3 w/ Microsoft Windows Server 2012 R2 (x64); Intel Pentium without AES-NI w/ Microsoft Windows Server 2012 R2 (x64); AMD A4 without AES-NI or PCLMULQDQ or SSSE3 w/ Microsoft Windows Storage Server 2012 R2 (x64); AMD Athlon 64 X2 without AES-NI w/ Microsoft Windows Storage Server 2012 R2 (x64); Intel Core i7 without AES-NI or PCLMULQDQ or SSSE3 w/ Microsoft Windows Storage Server 2012 R2 (x64); Intel Pentium without AES-NI w/ Microsoft Windows Storage Server 2012 R2 (x64); Intel Core i5 with AES-NI and PCLMULQDQ and SSSE3 w/ Microsoft Surface Pro 2 w/ Microsoft Windows 8.1 Enterprise (x64); Intel Core i5 with AES-NI and PCLMULQDQ and SSSE3 w/ Microsoft Surface Pro w/ Windows 8.1 Pro (x64); Intel Core i5 with AES-NI and PCLMULQDQ and SSSE3 w/ Microsoft Surface Pro 2 w/ Windows 8.1 Pro (x64) ; Intel Xeon E5-2648L without AES-NI w/ Microsoft StorSimple 8100 w/ Microsoft Windows Server 2012 R2; Intel Xeon E5-2648L with AES-NI w/ Microsoft StorSimple 8100 w/ Microsoft Windows Server 2012 R2; Intel Core i7 with AES-NI and PCLMULQDQ and SSSE 3 w/ Microsoft Surface Pro 3 w/ Windows 8.1 Pro (x64)		
522	Cisco Systems Inc. 170 W. Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**ONS Encryption Card Firmware Algorithms** **Version 1.2 (Firmware)**	Freescale P1010	7/10/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2887)] "Firmware algorithm implementations for the ONS encryption card."
521	Cisco Systems Inc. 170 W. Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**ONS Controller Card Firmware Algorithms** **Version 1.2 (Firmware)**	Freescale MPC8568E	7/10/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2427)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1820)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2886)] "Firmware algorithm implementations for the ONS controller cards."
520	Becrypt Ltd. 90 Long Acre Covent Garden London, England WC2E 9RA United Kingdom -Mark Wilce TEL: +44 207 557 6515 FAX: +44 845 838 2060 -Nigel Lee TEL: +44 845 838 2050 FAX: +44 845 838 2060	**32/64 bit subcomponent - BeCrypt Crypto Module** **Version 3.0**	Google Nexus 7 (2012) with NVidia Tegra 3 ARM v6 w/ Android v4.2.2; Dell Vostro 1500 with Intel Centrino Duo 64-bit processor w/ Ubuntu Linux 12.04 LTS; Dell D630 with Intel Centrino Duo 32-bit processor w/ Ubuntu Linux 12.04 LTS; Dell Venue 11 Pro (7130) with Intel Core i5-4300Y 64-bit AES-NI processor w/ Microsoft Windows 8.1 Professional; Dell Vostro 1500 with Intel Centrino Duo 64-bit processor w/ Microsoft Windows 7 Enterprise Edition; Dell D630 with Intel Centrino Duo 32-bit processor w/ Microsoft Windows 7 Ultimate Edition	7/10/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2883)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2883)] "The BeCrypt Cryptographic Library provides core cryptographic functionality for BeCrypt's security products providing a capability to develop complex and flexible security applications that require cryptographic functionality for pre-OS (16-bit), 32-bit and 64-bit operating environments."
519	Toshiba Corporation 1-1, Shibaura 1-chome Minato-ku, Tokyo 105-8001 Japan -Osamu Kawashima TEL: +81-90-6171-0253 FAX: +81-45-890-2492	**Toshiba Secure Cryptographic Suite for Enterprise HDD part of Firmware** **Version 1.00 (Firmware)**	Cortex-R5	6/27/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2418)] "A library of unique software and hardware cipher solutions which are standard encryption algorithm-based to provide Toshiba enterprise HDD products and the systems using them a robust and secure data storage environment"
518	Neopost Technologies S.A. 113 Rue Jean Marin Naudin BAGNEUX, 92220 France -Nathalie TORTELLIER TEL: 33 01 45 36 30 72 FAX: 33 01 45 36 30 10	**Neopost PSD** **Version A0038116A (Firmware)** **Part # A0014227B**	n/a	6/27/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2874)] "Neopost Postal Secure Device (PSD) for low to high range of franking machines"
517	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA	**PSymantec PGP Cryptographic Engine** **Version 4.3**	sVirtualized vSphere 5.1 / ESXi 5.1 hypervisor w/ Windows Server 2012 R2 x64	6/27/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2873)]

	-Bill Zhao TEL: 650-527-0683				"The Symantec PGP Cryptographic Engine is a FIPS 140-2 validated software only cryptographic module. The module implements the cryptographic functions for Symantec Encryption products, including the Symantec Drive Encryption, Symantec Desktop Email, Symantec File Share Encryption, Symantec Encryption Desktop, and Symantec Gateway Email."
516	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -Bill Zhao TEL: 650-527-0683	**Symantec PGP Cryptographic Engine** **Version 4.3**	Virtualized vSphere 5.1 / ESXi 5.1 hypervisor w/ Windows 8.1 update 1 x64	6/27/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2872)] "The Symantec PGP Cryptographic Engine is a FIPS 140-2 validated software only cryptographic module. The module implements the cryptographic functions for Symantec Encryption products, including the Symantec Drive Encryption, Symantec Desktop Email, Symantec File Share Encryption, Symantec Encryption Desktop, and Symantec Gateway Email."
515	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -Bill Zhao TEL: 650-527-0683	**Symantec PGP Cryptographic Engine** **Version 4.3**	Dell Precision M6400 Intel Core 2 Duo w/ Linux 64-bit RHEL 6.2	6/27/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2871)] "The Symantec PGP Cryptographic Engine is a FIPS 140-2 validated software only cryptographic module. The module implements the cryptographic functions for Symantec Encryption products, including the Symantec Drive Encryption, Symantec Desktop Email, Symantec File Share Encryption, Symantec Encryption Desktop, and Symantec Gateway Email."
514	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -David Finkelstein TEL: 650-527-0714	**Symantec PGP Cryptographic Engine** **Version 4.3**	Dell Precision M6400 Intel Core 2 Duo w/ Windows 7 32 bit	6/27/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2870)] "The Symantec PGP Cryptographic Engine is a FIPS 140-2 validated software only cryptographic module. The module implements the cryptographic functions for Symantec Encryption products, including the Symantec Drive Encryption, Symantec Desktop Email, Symantec File Share Encryption, Symantec Encryption Desktop, and Symantec Gateway Email."
513	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -David Finkelstein TEL: 650-527-0714	**Symantec PGP Cryptographic Engine** **Version 4.3**	Dell Precision M6400 Intel Core 2 i7 w/ Windows 7 32 bit with AESNI	6/27/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2869)] "The Symantec PGP Cryptographic Engine is a FIPS 140-2 validated software only cryptographic module. The module implements the cryptographic functions for Symantec Encryption products, including the Symantec Drive Encryption, Symantec Desktop Email, Symantec File Share Encryption, Symantec Encryption Desktop, and Symantec Gateway Email. It include [blank in original]"
512	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -David Finkelstein TEL: 650-527-0714	**Symantec PGP Cryptographic Engine** **Version 4.3**	Dell Precision M6400 Intel Core i7 w/ Windows 7 64 bit with AESNI	6/27/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2868)] "The Symantec PGP Cryptographic Engine is a FIPS 140-2 validated software only cryptographic module. The module implements the cryptographic functions for Symantec Encryption products, including the Symantec Drive Encryption, Symantec Desktop Email, Symantec File Share Encryption, Symantec Encryption Desktop, and Symantec Gateway Email."
511	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -David Finkelstein TEL: 650-527-0714	**Symantec PGP Cryptographic Engine** **Version 4.3**	Dell Precision M6400 Intel Core i7 w/ Linux 32 bit RHEL 6.2 with AESNI	6/27/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2867)] "The Symantec PGP Cryptographic Engine is a FIPS 140-2 validated software only cryptographic module. The module implements the cryptographic functions for Symantec Encryption products, including the Symantec Drive Encryption, Symantec Desktop Email, Symantec File Share Encryption, Symantec Encryption Desktop, and Symantec Gateway Email."
510	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA	**Symantec PGP Cryptographic Engine** **Version 4.3**	Mac OS X 10.7 with AESNI w/ Apple MacBook Pro Intel Core i7	6/27/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2866)]

	-David Finkelstein TEL: 650-527-0714				"The Symantec PGP Cryptographic Engine is a FIPS 140-2 validated software only cryptographic module. The module implements the cryptographic functions for Symantec Encryption products, including the Symantec Drive Encryption, Symantec Desktop Email, Symantec File Share Encryption, Symantec Encryption Desktop, and Symantec Gateway Email."
509	Fortinet Inc. 1090 Kifer Road Sunnyvale, CA 94086-5301 USA -Alan Kaye TEL: 613-225-9381 x7416 FAX: 613-225-9951	**Fortinet FortiOS RNG Cryptographic Library** **Version 5.0 GA Patch 7 (Firmware)**	Intel Xeon	6/27/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2862)] "This document focuses on the software implementation of the Fortinet FortiOS RNG Cryptographic Library 5.0 GA Patch 7." *07/10/14: Updated implementation information;*
508	N/A	**N/A**	N/A	6/27/2014	N/A
507	RSA The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Sandy Carielli TEL: 781-515-7510	**RSA BSAFE Crypto-C Micro Edition (ME)** **Version 4.1**	Intel x86 with AES-NI w/ Windows Server 2003 Enterprise R2 (/MD); Intel x86 without AES-NI w/ Windows Server 2003 Enterprise R2 (/MD); Intel x86 with AES-NI w/ Windows Server 2008 Enterprise SP2 (/MD); Intel x86 without AES-NI w/ Windows Server 2008 Enterprise SP2 (/MD); Intel x86 with AES-NI w/ Windows 7 Enterprise SP1 (/MD); Intel x86 without AES-NI w/ Windows 7 Enterprise SP1 (/MD); Intel x64 with AES-NI w/ Windows Server 2003 Enterprise R2 (/MD); Intel x64 without AES-NI w/ Windows Server 2003 Enterprise R2 (/MD); Intel x64 with AES-NI w/ Windows Server 2008 Enterprise R2 (/MD); Intel x64 without AES-NI w/ Windows Server 2008 Enterprise R2 (/MD); Intel x64 with AES-NI w/ Windows 7 Enterprise SP1 (/MD); Intel x64 without AES-NI w/ Windows 7 Enterprise SP1 (/MD); Itanium2 w/ Windows Server 2003 Enterprise R2; Itanium2 w/ Windows Server 2008 Enterprise R2; Intel x86 with AES-NI w/ Windows Server 2003 Enterprise R2 on ESX 5.1 (/MT); Intel x86 without AES-NI w/ Windows Server 2003 Enterprise R2 (/MT); Intel x86 with AES-NI w/ Windows Server 2008 Enterprise SP2 (/MT); Intel x86 without AES-NI w/ Windows Server 2008 Enterprise SP2 (/MT); Intel x86 with AES-NI w/ Windows 7 Enterprise SP1 (/MT); Intel x86 without AES-NI w/ Windows 7 Enterprise SP1 (/MT); Intel x64 with AES-NI w/ Windows Server 2003 Enterprise R2 (/MT); Intel x64 without AES-NI w/ Windows Server 2003 Enterprise R2 (/MT); Intel x64 with AES-NI w/ Windows Server 2008 Enterprise R2 (/MT); Intel x64 without AES-NI w/ Windows Server 2008 Enterprise R2 (/MT); Intel x64 with AES-NI w/ Windows 7 Enterprise SP1 (/MT); Intel x64 without AES-NI w/ Windows 7 Enterprise SP1 (/MT); Intel x64 with AES-NI w/ Windows Server 2012 R2 Standard (/MT); Intel x64 without AES-NI w/ Windows Server 2012 R2 Standard (/MT); Intel x64 with AES-NI w/ Windows 8.1 Enterprise (/MT); Intel x64 without AES-NI w/ Windows 8.1 Enterprise (/MT); Itanium2 64-bit w/ Windows Server 2003 Enterprise R2; Itanium2 64-bit w/ Windows Server 2008 Enterprise R2; Intel x86 with AES-NI w/ Red Hat Enterprise Linux 5.5 on ESX 4.0; Intel x86 without AES-NI w/ Red Hat Enterprise Linux 5.5 on ESX 4.0; Intel x64 with AES-NI w/ Red Hat Enterprise Linux 5.5 on ESX 4.0; Intel x64 without AES-NI w/ Red Hat Enterprise Linux 5.5 on ESX 4.0; Intel x86 without AES-NI w/ Red Hat Enterprise Linux 6.1 on ESXi 4.1; Intel x86 with AES-NI w/ SUSE Linux Enterprise Server 11 on ESX 4.0; Intel x86 without AES-NI w/ SUSE Linux Enterprise Server11 on ESX 4.0; Intel x64 with AES-NI w/ Red Hat Enterprise Linux 6.1 ESXi 4.1; Intel x64 without AES-NI w/ Red Hat Enterprise Linux 6.1 on ESXi 4.1; Intel x64 with AES-NI w/ SUSE Linux Enterprise Server 11 on ESXi 4.1; Intel x64 without AES-NI w/ SUSE Linux Enterprise Server 11 on ESXi 4.1; Itanium2 64-bit w/ Red Hat Enterprise	6/27/2014	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512 , SHA-512224 , SHA-512256) (HMAC Val#1799)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2859)] "RSA BSAFE® Crypto-C ME software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. The software supports a wide range of industry standard encryption algorithms offering developers the flexibility to choose the appropriate option to meet their requirements."

			Linux 5.5; PPC 32-bit w/ Red Hat Enterprise Linux 5.3; PPC 32-bit w/ SUSE Linux Enterprise Server 11; PPC 64-bit w/ Red Hat Enterprise Linux 5.3; PPC 64-bit w/ SUSE Linux Enterprise Server 11; Intel x64 with AES-NI w/ FreeBSD 8.3 on ESXi 5.0; Intel x64 without AES-NI w/ FreeBSD 8.3 on ESXi 5.0; Intel x64 with AES-NI w/ Mac OS X 10.8; Intel x64 without AES-NI w/ Mac OS X 10.8; SPARC v8 w/ Solaris 10; SPARC v8+ w/ Solaris 11; SPARC v9 (T2) w/ Solaris 11; SPARC v9 (T4) with T4 accelerator w/ Solaris 11; SPARC v9 (T4) without T4 accelerator w/ Solaris 11; Intel x86 with AES-NI w/ Solaris 10 on ESXi 4.1; Intel x86 without AES-NI w/ Solaris 10 on ESXi 4.1; Intel x64 with AES-NI w/ Solaris 10; Intel x64 without AES-NI w/ Solaris 10; PA-RISC 2.0 32-bit w/ HPUX 11.31; PA-RISC 2.0W 64-bit w/ HPUX 11.31; Itanium2 32-bit w/ HPUX 11.31; Itanium2 64-bit w/ HPUX 11.31; PowerPC 32-bit w/ AIX 6.1 on Virtual I/O Server 2.2.2.1; PowerPC 64-bit w/ AIX 6.1 on Virtual I/O Server 2.2.2.1; PowerPC 32-bit w/ AIX 7.1 on Virtual I/O Server 2.2.2.1; PowerPC 64-bit w/ AIX 7.1 on Virtual I/O Server 2.2.2.1; IBM z196 31/32-bit w/ Red Hat Enterprise Linux 5.8 on z/VM 6.2; IBM z196 64-bit w/ Red Hat Enterprise Linux 5.8 on z/VM 6.2; ARMv7 w/ Ubuntu 12.04 LTS; ARMv7 w/ Fedora Core 17; Intel x86 w/ Android 4.0.3; ARMv7 w/ Android 2.3.6; ARMv7 w/ Android 4.1.2; ARMv7 w/ iOS 7.1; ARMv7s w/ iOS 7.1; PPC 604 w/ VxWorks 6.4; PPC 604 w/ VxWorks 6.7; ARMv4 w/ VxWorks 6.8		
506	Software House a Brand of Tyco International 6 Technology Park Drive Westford, MA 01886 USA -Lou Mikitarian TEL: 1-978-577-4125 -Rick Focke TEL: 1-978-577-4266	**iSTAR Cryptographic Engine** **Version 2.1**	ARM v7 i.MX6Q w/ Ubuntu Linux 12.04.2; Atmel 9260 w/ Windows CE v5.0	6/27/2014	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-256) (HMAC Val#1797)] "The iSTAR Cryptographic Engine provides cryptographic services used for securing data and communications for the iSTAR Edge and iSTAR Ultra Door Controllers."
505	Motorola Solutions Inc. 1301 East Algonquin Road Schaumburg, IL 60196 USA -Tom Nguyen TEL: 847-576-2352 FAX: 847-576-6150 -Kevin Sze TEL: 847-576-4294 FAX: 847-576-6150	**DRBG** **Version R01.00.00 (Firmware)**	Atmel 5185912 Family	6/27/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#819)] "Firmware implementation of the DRBG (SP 800-90A)"
504	Hewlett-Packard Company 153 Taylor Street Littleton, MA 01460 USA -Bob Pittman TEL: 1-978-264-5211 FAX: 1-978-264-5522	**HP Comware** **Version 5.2.105 (Firmware)**	RMI (Netlogic) XLS208 MIPS; RMI (Netlogic) XLS408 MIPS	6/27/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2855)] "Comware cryptographic library is a software library that provides cryptographic functions within HP devices."
503	Accellion Inc. 1804 Embarcadero Road Suite 200 Palo Alto, Ca 94303 USA -Prateek Jain TEL: 65-62445670 FAX: 65-62445678	**OpenSSL Library** **Version 1.0.1g**	Intel Xeon QuadCore w/ CentOS 6.4 on VMware ESXi 5.1.0	5/30/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2850)] "Accellion Kiteworks Cryptographic Module is a key component of Accellion's Kiteworks product that enables enterprises to securely share and transfer files. Extensive tracking and reporting tools allow compliance with SOX, HIPAA, FDA and GLB regulations while providing enterprise grade security and ease of use."
502	Kaspersky Lab UK Ltd. 1st Floor, 2 Kingdom Street Paddington London, W2 6BD United Kingdom -Oleg Andrianov TEL: +7 495 797 8700	**Kaspersky Cryptographic Library 32-bit (User Mode)** **Version 2.0**	Intel(R) Core(TM)2 Duo P9600 @ 2.53GHz w/ Windows 7 Professional 32-bit; Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz w/ Windows 7 Enterprise 64-bit; Intel(R) Core(TM) i7-3770S CPU @ 3.10GHz w/ Windows 8.1 Enterprise 64-bit; Intel(R) Core(TM)2 Duo P9600 @ 2.53GHz w/ Kaspersky Preboot OS with BIOS	5/30/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2391)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#1789)]

					"Kaspersky Cryptographic Library is a software library that provides cryptographic services for various Kaspersky Lab applications." *09/19/14: Added new tested information;* *09/24/15: Added new tested information;*
501	Qualcomm Technologies Inc. 5775 Morehouse Dr San Diego, CA 92121 USA -Lu Xiao TEL: 858-651-5477	**DRBG of QTI Cryptographic Module on Crypto 5 Core V5.2.1.** **Version v5.2.1**	Snapdragon 805 w/ Android 4.4	5/23/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2839)] "The DRBG follows NIST SP 800-90A and produces deterministic random bits with the entropy collected from hardware."
500	INSIDE Secure Arteparc Bachasson, Bât A Rue de la carrière de Bachasson, CS70025 Meyreuil, Bouches-du-Rhône 13590 France -Bob Oerlemans TEL: +31 736-581-900 FAX: +31 736-581-999	**VaultIP** **Part # 1.1**	N/A	5/23/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#2847)] "VaultIP is a Silicon IP Security Module which includes a complete set of high- and low-level cryptographic functions. It offers key management and crypto functions needed for platform and application security such as Content Protection and Mobile Payment, and can be used stand-alone or as a 'Root of Trust' to support a TEE-based platform."
499	Juniper Networks Inc. 1194 N. Mathilda Ave. Sunnyvale, CA 94089 USA -Balachandra Shanabhag TEL: +91 8041904260	**OPENSSL** **Version Junos 13.3R1 (Firmware)**	Intel Xeon C3500/C5500 Series; Intel Xeon 5200 Series; Freescale e500v2; Freescale e5500	5/23/2014	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1784)] "Comprehensive, scalable and secure routing solutions specifically designed to meet the needs of both enterprises and service providers. All of our routers - core, Multiservice edge and edge ethernet - run on one common operating system - Junos."
498	Aruba Networks Inc. 1344 Crossman Ave Sunnyvale, CA 94089 USA -Jon Green TEL: 408-227-4500 FAX: 408-227-4550	**libancrypto.so** **Version 1.0.0**	Intel Core i5 w/ Red Hat Enterprise Linux 6 32-bit; ARMv7 w/ Android 4	5/23/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2746)] "The Aruba Common Cryptographic Module (CCM) is a software crypto library that powers a variety of Aruba's networking and security products. The module does not implement any protocols directly, but provides cryptographic primitives and functions that software developers build upon to implement various security protocols."
497	Aruba Networks Inc. 1344 Crossman Ave Sunnyvale, CA 94089 USA -Jon Green TEL: 408-227-4500 FAX: 408-227-4550	**moc_crypto.sys** **Version 1.0.0**	Intel Core i5 w/ Windows 7 32-bit Kernel Mode; Intel Core i5 w/ Windows 7 64-bit Kernel Mode	5/23/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2843)] "The Aruba Common Cryptographic Module (CCM) is a software crypto library that powers a variety of Aruba's networking and security products. The module does not implement any protocols directly, but provides cryptographic primitives and functions that software developers build upon to implement various security protocols."
496	Aruba Networks Inc. 1344 Crossman Ave Sunnyvale, CA 94089 USA -Jon Green TEL: 408-227-4500 FAX: 408-227-4550	**ancrypto.dll** **Version 1.0.0**	Intel Core i5 w/ Windows 7 32-bit User Mode; Intel Core i5 w/ Windows 7 64-bit User Mode	5/23/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2744)] "The Aruba Common Cryptographic Module (CCM) is a software crypto library that powers a variety of Aruba's networking and security products. The module does not implement any protocols directly, but provides cryptographic primitives and functions that software developers build upon to implement various security protocols." *06/11/14: Added new tested information;*
495	Fortinet Inc. 1090 Kifer Road Sunnyvale, CA 94086-5301 USA -Alan Kaye TEL: 613-225-9381 x7416 FAX: 613-225-9951	**Fortinet FortiMail RNG Cryptographic Library** **Version 5.0 (Firmware)**	Intel Xeon	5/16/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2840)] "This focuses on the firmware implementation of the Fortinet FortiMail RNG Cryptographic Library v5.0 running on Intel x86 compatible processors."
494	Kingston Technology Company Inc. 17600 Newhope Street Fountain Valley, CA 92708 USA	**Kingston DT4000 G2 Cryptographic Library** **Version 1.00 (Firmware)** **Part # PS2251-15**	Phison PS2251-15	5/9/2014	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256) (HMAC Val#1779)] "Kingston's DataTraveler DT4000 G2 Series USB Flash Drive is assembled in the US for organizations that require a secure way to store

	-Jason J Chen TEL: 714-445-3449 FAX: 714-438-2765 -Joel Tang TEL: 714-445-3433 FAX: 714-438-2765				and transfer portable data. The stored data is secured by hardware-based AES-256 encryption to guard sensitive information in case the drive is lost or stolen."
493	INSIDE Secure Eerikinkatu 28 Helsinki, 00180 Finland -Serge Haumont TEL: +358 40 5808548 -Marko Nippula TEL: +358 40 762 9394	**SafeZone FIPS Cryptographic Module** **Version 1.0.3A**	ARMv7, 2.3 GHz w/ Android 4.4	5/9/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2837)] "SafeZone FIPS Cryptographic Module is a FIPS 140-2 Security Level 1 validated software cryptographic module from INSIDE Secure. The module is a toolkit which provides the most commonly needed cryptographic primitives for a large variety of applications, including but not limited to, primitives for DAR, DRM, TLS, and VPN on mobile devices."
492	SecuTech Solutions PTY LTD Suite 514, 32 Delhi Road North Ryde, NSW 2113 Australia -Fujimi Bentley TEL: 00612-98886185 FAX: 00612-98886185 -Joseph Sciuto TEL: 00612-98886185 FAX: 00612-98886185	**UniMate USB/TRRS PKI token** **Version 5.1.6 (Firmware)**	Hongsi 08k	5/9/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2836)] "The UniMate USB/TRRS (Audio Port) PKI token is a hardware cryptographic module. It provides digital signature generation/verification for online authentications and data encryption/decryption for online transactions. UniMate provides the USB interface and audio port (TRRS) that can connect the module to a computer and smart mobile device." *06/27/14: Updated implementation information;*
491	Cyphercor Inc. 555 Legget Drive Suite 130 Kanata, ON K2K 2X3 Canada -Diego Matute TEL: 613-592-5800	**LoginTC Crypto Library** **Version 1.0**	Intel Xeon w/ CentOS 6	5/2/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256 , SHA-512) (SHS Val#2375)] "The LoginTC Crypto Library is a suite of cryptographic services providing advanced cryptographic functionality for LoginTC multi-factor authentication and security solutions. Based on Bouncy Castle v1.50."
490	Xirrus Inc. 2101 Corporate Center Drive Thousand Oaks, CA 91320 USA -Mike de la Garrigue TEL: 805-262-1655 FAX: 805-262-1601	**AOS Crypto Module** **Version 6.0 (Firmware)**	Cavium Octeon CN6000 series; Cavium Octeon CN5000 series	5/2/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2374)] "Xirrus AOS crypto library implementation." *08/07/14: Added new tested information;*
489	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA -Tim Myers TEL: 800-Microsoft	**Windows Storage Server 2012 R2, Microsoft Windows RT 8.1, Microsoft Surface with Windows RT 8.1, Microsoft Surface Pro with Windows 8.1, Microsoft Surface 2, Microsoft Surface Pro 2, Microsoft Surface Pro 3, Microsoft Windows Phone 8.1, Microsoft Windows Embedded 8.1 Industry and Microsoft StorSimple 8100 SymCrypt Cryptographic Implementations** **Version 6.3.9600**	NVIDIA Tegra 4 Quad-Core w/ Microsoft Surface 2 w/ Windows RT 8.1 (ARMv7 Thumb-2); AMD Athlon 64 X2 without AES-NI w/ Windows Embedded 8.1 Industry Enterprise (x64); AMD Athlon 64 X2 without AES-NI w/ Windows Embedded 8.1 Industry Enterprise (x86); AMD A4 without AES-NI w/ Windows Embedded 8.1 Industry Enterprise (x64); AMD A4 with AES-NI and PCLMULQDQ and SSSE3 w/ Windows Embedded 8.1 Industry Enterprise (x64); AMD A4 without AES-NI w/ Windows Embedded 8.1 Industry Enterprise (x86); Intel Core i3 without AES-NI and with PCLMULQDQ and SSSE3 w/ Windows Embedded 8.1 Industry Enterprise (x64); Intel Core i7 with AES-NI and PCLMULQDQ and SSSE3 w/ Windows Embedded 8.1 Industry Enterprise (x64); Intel Core i7 without AES-NI w/ Windows Embedded 8.1 Industry Enterprise (x64); Intel Core i7 without AES-NI w/ Windows Embedded 8.1 Industry Enterprise (x86); Intel Pentium without AES-NI w/ Windows Embedded 8.1 Industry Enterprise (x64); Intel Pentium without AES-NI w/ Windows Embedded 8.1 Industry Enterprise (x86); AMD Athlon 64 X2 without AES-NI w/ Windows 8.1 Enterprise (x64); AMD Athlon 64 X2 without AES-NI w/ Windows 8.1 Enterprise (x86); AMD A4 without AES-NI w/ Windows 8.1 Enterprise (x64); AMD A4 with AES-NI and PCLMULQDQ and SSSE3 w/ Windows 8.1 Enterprise (x64); AMD A4 without AES-NI w/ Windows 8.1 Enterprise (x86); Intel Core i3 without AES-NI and with PCLMULQDQ and SSSE3 w/ Windows 8.1 Enterprise	5/2/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2832)] "The Microsoft Windows Next Generation Cryptographic algorithm implementation provides enhanced support for AES, AES DRBG, HMAC, SHS (SHA), and Triple-DES. All implementations are packaged into a library used by Microsoft and other third-party applications." *07/21/14: Added new tested information;* *03/13/15: Added new tested information;*

			(x64); Intel Core i7 with AES-NI and PCLMULQDQ and SSSE3 w/ Windows 8.1 Enterprise (x64); Intel Core i7 without AES-NI w/ Windows 8.1 Enterprise (x86); Intel Pentium without AES-NI w/ Windows 8.1 Enterprise (x64); Intel Pentium without AES-NI w/ Windows 8.1 Enterprise (x86); AMD Athlon 64 X2 without AES-NI w/ Windows Server 2012 R2 (x64); AMD A4 without AES-NI w/ Windows Server 2012 R2 (x64); AMD A4 with AES-NI and PCLMULQDQ and SSSE3 w/ Windows Server 2012 R2 (x64); Intel Core i3 without AES-NI and with PCLMULQDQ and SSSE3 w/ Windows Server 2012 R2 (x64); Intel Core i7 without AES-NI w/ Windows Server 2012 R2 (x64); Intel Core i7 with AES-NI and PCLMULQDQ and SSSE3 w/ Windows Server 2012 R2 (x64); Intel Pentium without AES-NI w/ Windows Server 2012 R2 (x64); AMD Athlon 64 X2 without AES-NI w/ Windows Storage Server 2012 R2 (x64); AMD A4 without AES-NI w/ Windows Storage Server 2012 R2 (x64); AMD A4 with AES-NI and PCLMULQDQ and SSSE3 w/ Windows Storage Server 2012 R2 (x64); Intel Core i3 without AES-NI and with PCLMULQDQ and SSSE3 w/ Windows Storage Server 2012 R2 (x64); Intel Core i7 without AES-NI w/ Windows Storage Server 2012 R2 (x64); Intel Core i7 with AES-NI and PCLMULQDQ and SSSE3 w/ Windows Storage Server 2012 R2 (x64); Intel Pentium without AES-NI w/ Windows Storage Server 2012 R2 (x64); NVIDIA Tegra 3 Quad-Core w/ Windows RT 8.1 (ARMv7 Thumb-2); Qualcomm Snapdragon S4 w/ Windows Phone 8.1 (ARMv7 Thumb-2); Qualcomm Snapdragon 400 w/ Windows Phone 8.1 (ARMv7 Thumb-2); Qualcomm Snapdragon 800 w/ Windows Phone 8.1 (ARMv7 Thumb-2); Qualcomm Snapdragon S4 w/ Windows RT 8.1 (ARMv7 Thumb-2); NVIDIA Tegra 3 Quad-Core w/ Microsoft Surface w/ Windows RT 8.1 (ARMv7 Thumb-2) ; Intel Core i5 with AES-NI and PCLMULQDQ and SSSE3 w/ Microsoft Surface Pro 2 w/ Microsoft Windows 8.1 Enterprise (x64); Intel Core i5 with AES-NI and PCLMULQDQ and SSSE3 w/ Microsoft Surface Pro w/ Windows 8.1 Pro (x64); Intel Core i5 with AES-NI and PCLMULQDQ and SSSE3 w/ Microsoft Surface Pro 2 w/ Windows 8.1 Pro (x64); Intel Xeon E5-2648Lwith AES-NI w/ Microsoft StorSimple 8100 w/ Microsoft Windows Server 2012 R2; Intel Core i7 with AES-NI and PCLMULQDQ and SSSE 3 w/ Microsoft Surface Pro 3 w/ Windows 8.1 Pro (x64)		
487	Pitney Bowes Inc. 37 Executive Drive Danbury, CT 06810 USA -Dave Riley TEL: 203-796-3208	**libprng** **Version 01.01.0009 (Firmware)** **Part # MAX32590 Rev B4**	N/A	4/9/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2369)] "Pitney Bowes X4 HSM Cryptographic Module"
486	Linear Technology Corporation 1630 McCarthy Blvd Milpitas, CA 95035 USA -Ross Yu TEL: 408-432-1900 FAX: 408-434-0507 -Yuri Zats TEL: 408-432-1900 FAX: 408-434-0507	**Dust Cryptographic Library** **Version 3 (Firmware)**	AT91SAM9G20B	4/9/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2825)] "Dust Networks Cryptographic Library 3 used in SmartMesh WirelessHART manager products."
485	OpenSSL Software Foundation Inc. 1829 Mount Ephraim Road Adamstown, MD 27101 USA -Steve Marquess TEL: 877-673-6775	**OpenSSL FIPS Object Module** **Version 2.0.7**	Freescale e500v2 (PPC) w/ Linux 2.6; Intel Core i7-3612QE (x86) without AES-NI w/ AcanOS 1.0; Intel Core i7-3612QE (x86) with AES-NI w/ AcanOS 1.0; Feroceon 88FR131 (ARMv5) w/ AcanOS 1.0; Intel Xeon E5440 (x86) without AES-NI w/ FreeBSD 8.4; Xeon E5-2430L (x86) without AES-NI w/ FreeBSD 9.1; Xeon E5-2430L (x86) with AES-NI w/ FreeBSD 9.1; Xeon E5645 (x86) without AES-NI w/ ArbOS 5.3; ASPEED AST-Series (ARMv5)	5/9/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2368)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1768)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2824)]

			w/ Linux ORACLESP 2.6; Emulex PILOT3 (ARMv5) w/ Linux ORACLESP 2.6; Xeon E5645 (x86) with AES-NI w/ ArbOS 5.3 ; Xeon E5-2430L (x86) without AES-NI w/ FreeBSD 9.2; Xeon E5-2430L (x86) with AES-NI w/ FreeBSD 9.2		BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2824)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#496) (SHS Val#2368) "The OpenSSL FIPS Object Module is a full featured general purpose cryptographic library that is distributed in source code form under an open source license. It can be downloaded from www.openssl.org/source/." *05/14/14: Added new tested information;* *05/30/14: Added new tested information and updated implementation information;* *07/03/14: Added new tested information;* *07/178/14: Added new tested information;* *07/31/14: Updated implementation information;*
484	Infotecs 41 Madison Avenue New York, New York 10010 USA -Andrey Krasikov TEL: +1 (678) 431-9502 -Philippe Dieudonné TEL: +7 (495) 737-6192	**ViPNet Common Crypto Core Library (User Space)** **Version 1.0**	Intel Core i7 w/ Windows 8.1 64-bit; ARMv7 w/ Android 4.4	4/9/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2823)] BlockCipher_No_df: (, AES-256) (AES Val#2823)] "The ViPNet Common Crypto Core Library is a software library that provides cryptographic services to a number of ViPNet applications via an API. It is available in user space and kernel driver implementations on a wide range of operational systems. User space library and kernel library use the same base source code."
483	Infotecs 41 Madison Avenue New York, New York 10010 USA -Andrey Krasikov TEL: +1 (678) 431-9502 -Philippe Dieudonné TEL: +7 (495) 737-6192	**ViPNet Common Crypto Core Library (Kernel)** **Version 1.0**	Intel Core i7 w/ Windows 8.1 64-bit	4/9/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2822)] BlockCipher_No_df: (, AES-256) (AES Val#2822)] "The ViPNet Common Crypto Core Library is a software library that provides cryptographic services to a number of ViPNet applications via an API. It is available in user space and kernel driver implementations on a wide range of operational systems. User space library and kernel library use the same base source code."
482	Morpho 18 chausee Jules Cesar Osny, France 95520 France -Omar Derrouazi TEL: +33158116971	**IDeal CitizTM v2.0 Open** **Part # SLE78C(L)FX4000P(M), SLE78C(L)FX3000P(M)**	N/A	4/9/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128) (AES Val#2818)] "The IDeal Citiz™ v2.0 Open is a single chip cryptographic module, which combines an implementation of the Sun Java Card Version 3.0.2 Classic Edition and GlobalPlatform Version 2.1.1 specifications on a dual interface chip (ISO 7816 contact and ISO 14443 contactless interface communication protocols)."
481	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**IOS Common Cryptographic Module (IC2M) Algorithm Module** **Version 2.0 (Firmware)**	AMCC PowerPC 405EX; Cavium CN5020; Cavium CN5220; Cavium CN5230; Freescale 8752E; Freescale SC8548H; Intel Xeon; MPC8358E; MPC8572C; PowerPC 405; Intel Atom C2000	3/31/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2817)] "IOS Common Crypto Module" *01/30/15: Added new tested information;*
480	RSA The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Sandy Carielli TEL: 781-515-7510	**RSA BSAFE Crypto-C Micro Edition (ME)** **Version 3.0.0.21**	MV78230 ARMv7 w/ TimeSys Linux Kernel 2.6.33RT; PJ4B-MP ARMv7 w/ TimeSys Linux Kernel 3.0.0	3/21/2014	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1759)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#491) (SHS Val#2356) "RSA BSAFE® Crypto-C ME software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. The software supports a wide range of industry standard encryption algorithms offering developers the flexibility to choose the appropriate option to meet their requirements."
479	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA	**Symantec PGP Cryptographic Engine** **Version 4.3**	Dell Precision M6400 Intel Core i7 w/ Linux 64 bit RHEL with AESNI	3/21/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2805)]

	-David Finkelstein TEL: 650-527-0714				"The Symantec PGP Cryptographic Engine is a FIPS 140-2 validated software only cryptographic module. The module implements the cryptographic functions for Symantec Encryption products, including the Symantec Drive Encryption, Symantec Desktop Email, Symantec File Share Encryption, Symantec Encryption Desktop, and Symantec Gateway Email. It includ [blank in original]"
478	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -Bill Zhao TEL: 650-527-0683	**Symantec PGP Cryptographic Engine** **Version 4.3**	Dell Precision M6400 Intel Core 2 Duo w/ Windows 7 64 bit	3/7/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2799)] "The Symantec PGP Cryptographic Engine is a FIPS 140-2 validated software only cryptographic module. The module implements the cryptographic functions for Symantec Encryption products, including the Symantec Drive Encryption, Symantec Desktop Email, Symantec File Share Encryption, Symantec Encryption Desktop, and Symantec Gateway Email."
477	Senetas Corporation Ltd. and SafeNet Inc. Level 1, 11 Queens Road Melbourne, Victoria 3004 Australia -John Weston TEL: +61 3 9868 4555 FAX: +61 3 9821 4899 -Chris Brych TEL: +1 613 221 5081 FAX: +1 613 723 5079	**CN1000 and CN3000 Series Common Crypto Library** **Version 4.4 (Firmware)**	Freescale MPC8280	3/7/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2350)] "The CN1000 and CN3000 Series Common Crypto Library Module provides FIPS 140-2 approved cryptographic algorithms for the CN1000 and CN3000 Series Encryptors. Based upon OpenSSL the Library provides an Application Programming Interface (API) to support security relevant services."
476	Senetas Corporation Ltd. and SafeNet Inc. Level 1, 11 Queens Road Melbourne, Victoria 3004 Australia -John Weston TEL: +61 3 9868 4555 FAX: +61 3 9821 4899 -Chris Brych TEL: +1 613 221 5081 FAX: +1 613 723 5079	**CN4010 and CN6010 Series Common Crypto Library** **Version 2.4 (Firmware)**	ARM Cortex A9	2/28/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2346)] "The CN4010 and CN6010 Series Common Crypto Library Module provides FIPS 140-2 approved cryptographic algorithms for the CN4010 and CN6010 Series Encryptors. Based upon OpenSSL the Library provides an Application Programming Interface (API) to support security relevant services."
475	Senetas Corporation Ltd. and SafeNet Inc. Level 1, 11 Queens Road Melbourne, Victoria 3004 Australia -John Weston TEL: +61 3 9868 4555 FAX: +61 3 9821 4899 -Chris Brych TEL: +1 613 221 5081 FAX: +1 613 723 5079	**CN6000 Series Common Crypto Library** **Version 2.4 (Firmware)**	Intel ATOM	2/28/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2345)] "The CN6000 Series Common Crypto Library Module provides FIPS 140-2 approved cryptographic algorithms for CN6000 Series Encryptors. Based upon OpenSSL the Common Crypto Library provides an Application Programming Interface (API) to support security relevant services."
474	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -David Finkelstein TEL: 650-527-0714	**Symantec PGP Cryptographic Engine** **Version 4.3**	Dell Precision M6400 Intel Core 2 Duo w/ Linux 32-bit RHEL 6.2	2/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2787)] "The Symantec PGP Cryptographic Engine is a FIPS 140-2 validated software only cryptographic module. The module implements the cryptographic functions for Symantec Encryption products, including the Symantec Drive Encryption, Symantec Desktop Email, Symantec File Share Encryption, Symantec Encryption Desktop, and Symantec Gateway Email. It includes [blank in original]"
473	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -David Finkelstein TEL: 650-527-0714	**Symantec PGP Cryptographic Engine** **Version 4.3**	Apple MacBook Pro Intel Core 2 Duo w/ Mac OS X 10.7	2/28/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2786)] "The Symantec PGP Cryptographic Engine is a FIPS 140-2 validated software only cryptographic module. The module implements the cryptographic functions for Symantec Encryption products, including the Symantec Drive Encryption, Symantec Desktop Email, Symantec File Share Encryption, Symantec Encryption Desktop, and Symantec Gateway Email. It includes [blank in original]"

472	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**IOS** **Version 1.0**	Intel Atom D2500 w/ CentOS Linux 6.4	2/21/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2785)] "IOS software cryptographic implementations used within Cisco devices to provide cryptographic functions."
471	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**IOS** **Version 1.0 (Firmware)**	Freescale MPC8358E; Freescale MPC8548E	2/21/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2784)] "IOS software cryptographic implementations used within Cisco devices to provide cryptographic functions."
470	Mocana Corporation 710 Sansome Street San Francisco, CA 94104 USA -James Blaisdell TEL: (415) 617-0055 FAX: (415) 617-0056	**Mocana Cryptographic Library** **Version 5.5.1f**	ARMv7 w/ Android 4.4	2/21/2014	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2782)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#484) (SHS Val#2337) "The Mocana Cryptographic Module is the engine of Mocana's Device Security Framework - a software framework that secures all aspects of a system. The Device Security Framework helps applications and device designers reduce development costs and dramatically enhance cryptographic performance. For details see www.mocana.com."
469	Fortinet, Inc. 1090 Kifer Road Sunnyvale, CA 94086-5301 USA -Alan Kaye TEL: 613-225-9381 x7416 FAX: 613-225-2951	**Fortinet FortiOS RNG Cryptographic Library** **Version 5.0 GA Patch 6 (Firmware)**	ARM v5 Compatible; Intel Atom; Intel Celeron; Intel i3-540 Dual Core; Intel i5-750 Quad Core; Intel Xeon	2/21/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2775)] "This document focuses on the software implementation of the Fortinet FortiOS RNG Cryptographic Library 5.0 GA Patch 6"
468	Engage Communication Inc. 9565 Soquel Drive Suite 201 Aptos, CA 95003 USA -Gian-Carlo Bava TEL: 831-688-1021 ext 106 -Shaun Tomaszewski TEL: 831-688-1021 ext 104	**BlackVault Crypto-OSS** **Version 2.0.5 (Firmware)**	ARM926EJ-S	2/14/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2327)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1732)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2768)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2768)] "The Engage Communication BlackVault cryptographic library provides a FIPS 140-2 approved Application Programming Interface (API) to the BlackVault Hardware Security Module (HSM). The library is based on OpenSSL FIPS version 2.0.5."
467	Oracle America Inc. 500 Oracle Parkway Redwood City, CA 94065 United States -Linda Gallops TEL: 704-972-5018 FAX: 704-321-9273	**T10000D DRBG Implementation** **Version 2.2 (Firmware)**	Altera NIOS II	2/7/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2762)] "The Oracle StorageTek T10000D Tape Drive blends the highest capacity, performance, reliability, and data security to support demanding, 24/7 data center operations. It delivers the world's fastest write speeds to a native 8.5 TB of magnetic tape storagel; making it ideal for data center operations with growing data volume."
466	SonicWALL Inc. 2001 Logic Drive San Jose, CA 95124 USA -Usha Sanagala TEL: 408-962-6248 FAX: 408-745-9300	**SonicOS 6.2 for NSA and SM** **Version 6.2 (Firmware)**	Cavium Octeon Plus 66XX; Cavium Octeon Plus 68XX	1/24/2014	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2322)] "The Dell SonicWALL family of firewalls tightly integrates intrusion prevention, malware protection, Application Intelligence and Control with real-time Visualization. Dell SonicWALL Reassembly-Free Deep Packet Inspection engine scans 100% of traffic and massively scales to meet needs of the most high-performance networks."
465	Cambium Networks 3800 Golf Road, Suite 360	**PTP700 DRBG**	TI TMS320C6657	1/10/2014	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES

	Rolling Meadows, IL 60008 USA -Mark Thomas TEL: +44 1364 655500 FAX: +44 1364 654625	**Version PTP700-DRBG-01-00 (Firmware)**			Val#2754)] "DRBG based on SP800-90 AES/CTR"
464	Green Hills Software 30 W Sola Street Santa Barbara, CA 93101 USA -David Sequino TEL: 206-310-6795 FAX: 978-383-0560 -Douglas Kovach TEL: 727-781-4909 FAX: 727-781-2915	**INTEGRITY Security Services Embedded Cryptographic Toolkit AES-CTR DRBG** **Version 2.0.415**	ARM Cortex A9 w/ Green Hills Software INTEGRITY Multivisor v4 for ARM	12/31/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2745)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2745)] "Green Hills Software ISS ECT is a standards-based crypto toolkit providing a flexible framework to integrate encryption, digital signatures and other security mechanisms into a wide range of applications. ISS ECT is designed to support multiple cryptographic providers with a single common API, easily targeted to a variety of Operating Systems."
463	Aruba Networks, Inc. 1344 Crossman Ave Sunnyvale, CA 94089 USA -Jon Green TEL: 408-227-4500 FAX: 408-227-4550	**libancrypto.a** **Version 1.0.0**	Intel Core i5 w/ Mac OS X 10.8; Apple A6 w/ Apple iOS 7	12/31/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2747)] "The Aruba Common Cryptographic Module (CCM) is a software crypto library that powers a variety of Aruba's networking and security products. The module does not implement any protocols directly, but provides cryptographic primitives and functions that software developers build upon to implement various security protocols."
462	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -Rose Quijano-Nguyen TEL: 650-527-0741	**Symantec Cross-Platform Cipher Engine** **Version 1.1**	Sun UltraSPARC III w/ Solaris 10; Intel Xeon X34xx w/ Windows 2012; Intel Xeon X34xx w/ RHEL 6.4 64-bit	12/20/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2315)] "The Symantec Cross-Platform Cipher Engine is designed to provide FIPS140-2 algorithm support for the Symantec Cross-Platform Cryptographic Module. This module supports Symantec Applications by providing validated Cryptographic Services. The incorporation of these algorithms make these products ideal for enterprise and government applications." *01/10/14: Updated implementation information;*
461	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**ACT-2Lite** **Part # 15-14497-02(NX315)**	N/A	12/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#2742)] "ACT-2Lite is an ASSP which is based on a smart card hardware platform with custom ROM code provided by Cisco."
460	Mocana Corporation 710 Sansome Street San Francisco, CA 94104 USA -James Blaisdell TEL: (415) 617-0055 FAX: (415) 617-0056	**Mocana Cryptographic Library** **Version 5.5.1f**	ARMv7 w/ Android 4.3; ARMv7 w/ Android 4.4; PowerQuicc II Pro w/ VxWorks 6.8; ; Freescale P2020 w/ Mentor Embedded Linux 4.0; Qualcomm MSM8974 w/ Linux 3.4; Qualcomm MSM8992 w/ Linux 3.10	12/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2741)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#479) (SHS Val#2313) "The Mocana Cryptographic Module is the engine of Mocana's Device Security Framework - a software framework that secures all aspects of a system. The Device Security Framework helps applications and device designers reduce development costs and dramatically enhance cryptographic performance. For details see www.mocana.com." *03/11/14: Added new tested information;* *01/23/15: Added new tested information;* *02/03/15: Updated implementation information;* *02/20/15: Added new tested information;* *09/17/15: Added new tested information;*
459	Utimaco Safeware AG Germanusstraße 4 Aachen, 52080 Germany -Dr. Gesa Ott TEL: ++49 241-1696-200 FAX: ++49 241-1696-199 -Dieter Bong TEL: ++49 241-1696-200 FAX: ++49 241-1696-199	**CryptoServer Se DRBG** **Version util3.0.2.0_smos3.1.2.1 (Firmware)**	Texas Instruments TMS320C6416T	12/20/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-512) (SHS Val#2308)] "DRBG Component implements deterministic random bit generation based on SMOS SHA as transition function."

458	Blue Coat Systems Inc. 420 North Mary Avenue Sunnyvale, California 94085-4121 USA -Diana Robinson TEL: +1 (845) 454-6397 -Tammy Green TEL: +1 (801) 999-2973	**Blue Coat SG VA Crypto Library** **Version 3.1.2**	Intel Xeon w/ VMware ESXi v5.1 with SGOS v6.5.2	12/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2737)] BlockCipher_No_df: (, AES-256) (AES Val#2737)] "The Blue Coat SG VA Crypto Engine v1.0 provides the necessary cryptographic services to a proprietary operating system (SGOS 6.5.2) developed specifically for use in Blue Coat's Secure Web Gateway virtual appliance."
456	Blue Coat Systems Inc. 420 North Mary Avenue Sunnyvale, California 94085-4121 USA -Diana Robinson TEL: +1 (845) 454-6397 -Tammy Green TEL: +1 (801) 999-2973	**Blue Coat SGOS Crypto Library** **Version 3.1.2 (Firmware)**	Intel Xeon E5-2418L; Intel Xeon E5-2430; Intel Xeon E5-2658;	12/18/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2722)] BlockCipher_No_df: (, AES-256) (AES Val#2722)] "The Blue Coat Crypto Library v1.0 provides the necessary cryptographic services to a proprietary operating system (SGOS 6.5.2) developed specifically for use in Blue Coat's ProxySG line of appliances."
455	Giesecke & Devrient GmbH Prinzregentenstraße 159 München, n/a 81677 Germany -Katharina Wallhäußer TEL: +49 89 4119-1397 FAX: +49 89 4119-2819	**SLE78 CTR DRBG** **Version 2.1 (Firmware)**	SLE78CLFX4000P(M) / M7892 family	12/18/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2721)] "Sm@rtCafé Expert 7.0 C1 is a Java Card 3 Platform Classic Edition compliant to GlobalPlatform CS V2.2.1 and GP V2.2 Amd D."
454	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**Brocade MLXe MR2** **Version BRCD-IP-CRYPTO-VER-3.0 (Firmware)**	Freescale MPC 7448, RISC, 1700 MHz;	12/13/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2282)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2717)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2717)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. The Brocade MLXe Series and Brocade NetIron® CER 2000 Series Ethernet Routers, Brocade NetIron CES 2000 Series Ethernet Switches provide industry-leading wire-speed port capacity without compromising the performance of advanced capabilities such as IPv6, MPLS, and MPLS Virtual Private Networks (VPNs)." *02/18/14: Update vendor information;* *02/20/14: Added new tested information;*
453	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-8101 FAX: 408-333-8101	**Brocade MLXe MR** **Version BRCD-IP-CRYPTO-VER-3.0 (Firmware)**	Freescale MPC 7447A, RISC, 1000MHz	12/13/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2281)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2716)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2716)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. The Brocade MLXe Series and Brocade NetIron® CER 2000 Series Ethernet Routers, Brocade NetIron CES 2000 Series Ethernet Switches provide industry-leading wire-speed port capacity without compromising the performance of advanced capabilities such as IPv6, MPLS, and MPLS Virtual Private Networks (VPNs)." *02/14/14: Added new tested information;*
452	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**Brocade NetIron CES and CER 2000 Series** **Version BRCD-IP-CRYPTO-VER-3.0 (Firmware)**	Freescale MPC 8544, Power QUICC III, 800 MHz	12/13/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2280)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2715)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2715)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. The Brocade MLXe Series and Brocade NetIron® CER 2000 Series Ethernet Routers, Brocade NetIron CES 2000 Series Ethernet Switches provide industry-leading wire-

					speed port capacity without compromising the performance of advanced capabilities such as IPv6, MPLS, and MPLS Virtual Private Networks (VPNs)." *02/14/14: Added new tested information;*
451	McAfee Inc. 2340 Energy Park Drive St. Paul, MN 55108 USA -Mark Hanson TEL: 651-628-1633 FAX: 651-628-2701	**McAfee Firewall Enterprise 64-bit Cryptographic Engine (Virtual)** **Version 8.3.2**	Intel Xeon w/ VMware ESXi v5.0 with SecureOS 8.3	12/13/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2714)] "The McAfee Firewall Enterprise 64-bit Cryptographic Engine (Virtual) is a software library that provides cryptographic services for applications on virtual deployments of the McAfee Firewall Enterprise Appliance."
450	McAfee Inc. 2340 Energy Park Drive St. Paul, MN 55108 USA -Mark Hanson TEL: 651-628-1633 FAX: 651-628-2701	**McAfee Firewall Enterprise 64-bit Cryptographic Engine** **Version 8.3.2 (Firmware)**	Intel Atom; Intel Core; Intel Pentium; Intel Xeon	12/13/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2713)] "The McAfee Firewall Enterprise 64-bit Cryptographic Engine is a firmware library that provides cryptographic services for applications across several versions of the McAfee Firewall Enterprise Appliances."
449	McAfee, Inc. 2340 Energy Park Drive St. Paul, MN 55108 USA -Mark Hanson TEL: 651-628-1633 FAX: 651-628-2701	**McAfee Firewall Enterprise 32-bit Cryptographic Engine (Virtual)** **Version 8.3.2**	Intel Xeon w/ VMware ESXi v5.0 with SecureOS 8.3	12/13/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2712)] "The McAfee Firewall Enterprise 32-bit Cryptographic Engine (Virtual) is a software library that provides cryptographic services for applications on virtual deployments of the McAfee Firewall Enterprise Appliance."
448	McAfee, Inc. 2340 Energy Park Drive St. Paul, MN 55108 USA -Mark Hanson TEL: 651-628-1633 FAX: 651-628-2701	**McAfee Firewall Enterprise 32-bit Cryptographic Engine** **Version 8.3.2 (Firmware)**	Intel Atom; Intel Core i3; Intel Pentium; Intel Xeon	12/13/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2711)] "The McAfee Firewall Enterprise 32-bit Cryptographic Engine is a firmware library that provides cryptographic services for applications across several versions of the McAfee Firewall Enterprise Appliances."
447	McAfee, Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Chela Diaz de Villegas TEL: 651 628-1642 FAX: 651-628-2701	**McAfee ePO Agent Handler Cryptographic Module** **Version 1.0**	Intel Xeon E5 32-bit w/ Windows 2008 R2; Intel Xeon E5 64-bit w/ Windows 2008 R2	12/6/2013	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256) (HMAC Val#1686)] "McAfee ePO Agent Handler Cryptographic Module provides cryptographic operations for McAfee ePolicy Orchestrator (ePO), a security management software that allows enterprises to unify the management of numerous end-point, network, and data security products."
446	VMware Inc. 3401 Hillview Ave Palo Alto, CA 94303 USA -Eric Betts	**VMware Java JCE (Java Cryptographic Extension) Module** **Version 1.0**	Intel Xeon E5-2430 w/ VMware vCloud Networking and Security 5.5.0a vShield Manager OS with Sun JRE 6.0 running on VMware vSphere Hypervisor (ESXi) 5.5	12/6/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-512) (SHS Val#2271)] "The VMware Java JCE (Java Cryptographic Extension) module is a versatile software library that implements FIPS-140-2 approved cryptographic services for VMware products and platforms." *12/06/13: Updated implementation information; 12/27/13: Updated implementation information;*
445	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Mark Hanson TEL: +1 651 628 1633 FAX: +1 651 628 2706	**RSA BSAFE Crypto-J** **Version 6.1**	Intel Celeron w/ McAfee Linux 2.2.1; Intel Xeon w/ McAfee Linux 2.2.1	12/6/2013	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1684)] "McAfee Firewall Enterprise Control Center simplifies the management of multiple McAfee Firewall Enterprise appliances. Control Center enables centralized management and monitoring of the McAfee Firewall Enterprise solutions, allowing network administrators to centrally define firewall policy, deploy updates and inventory their firewall products."
444	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Mark Hanson TEL: +1 651 628 1633 FAX: +1 651 628 2706	**RSA BSAFE Crypto-J** **Version 6.1**	Intel Xeon w/ McAfee Linux 2.2.1 running on VMware ESXi 5.0	12/6/2013	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1683)] "McAfee Firewall Enterprise Control Center simplifies the management of multiple McAfee Firewall Enterprise appliances. Control Center enables centralized management and monitoring of the McAfee Firewall Enterprise solutions, allowing network administrators to centrally

					define firewall policy, deploy updates and inventory their firewall products."
443	VMware Inc. 3401 Hillview Ave Palo Alto, CA 94303 USA -Eric Betts TEL: 650-427-1902	**VMware NSS Cryptographic Module** **Version 1.0**	Intel Xeon E5-2430 with AES-NI w/ VMware vCloud Networking and Security 5.5.0a Edge OS running on VMware vSphere Hypervisor (ESXi) 5.5	11/29/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2267)] "The VMware NSS Cryptographic Module is a software cryptographic library that provides FIPS-140-2 validated network security services to VMware products" *12/27/13: Updated implementation information;*
442	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**Brocade FCX 624/648 and ICX 6610 Series** **Version BRCD-IP-Crypto-Ver-3.0 (Firmware)**	Freescale MPC8544E, 800 MHz	11/29/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2265)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2697)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2697)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. The Brocade ICX6610 delivers wire-speed, non-blocking performance across all ports to support latency-sensitive. The Brocade FCX Series offers a comprehensive line of switches with specific models optimized for campus and data center deployment." *03/03/14: Added new tested information;*
441	Chunghwa Telecom Co. Ltd. Telecommunication Laboratories No.99, Dianyan Rd. Yang-Mei, Taoyuan 326 Taiwan, ROC -Yeou-Fuh Kuan TEL: +886-3-424-4333 FAX: +886-3-424-4129 -Char-Shin Miou TEL: +886-3-424-4381 FAX: +886-3-424-4129	**HiCOS Cryptographic Library** **Version 3.5 (Firmware)**	Renesas RS-4 series	11/29/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2262)] "HiCOS PKI Native Smart Card is a dual interface (ISO 7816 & ISO 14443) cryptographic smart card and supports SHA-1, SHA-256, SHA-384, SHA-512, Hash-DRBG, 3DES-3Key-MAC, 3DES-3Key encrypt/decrypt, RSA 2048 encrypt/decrypt (including RSA-CRT), RSA digital signature generation /verification(including RSA-CRT)"
440	IBM 9032 South Rita Road Tucson, AZ 85744 USA -Christine Knibloe TEL: (520) 799-2486	**IBM LTO Ultrium 6 Cryptographic Firmware Library** **Version 1.0 (Firmware)**	IBM PowerPC 405	11/22/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#2261)] "Firmware cryptographic implementation that adds secure key channel capabilities to the IBM LTO Ultrium 6 tape drive."
439	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**Brocade ICX 6450 and ICX 6450-C12 Series** **Version BRCD-IP-Crypto-Ver-3.0 (Firmware)**	ARM ARMv5TE, 800 MHz	11/22/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2260)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2690)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2690)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. Brocade ICX6450 switches deliver enterprise-class stackable switching at an entry-level price." *02/27/14: Added new tested information;*
438	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**Brocade SX800/SX1600 Series** **Version BRCD-IP-Crypto-Ver-3.0 (Firmware)**	Freescale P3041E, 1.5 GHz	11/22/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2259)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2653)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2653)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. The FastIron SX Series extends control from the network edge to the core with intelligent network services, such as Quality of Service (QoS) and provides a scalable, secure, low-latency, and fault-tolerant IP services solution for 1GbE and 10 GbE enterprise deployments." *03/03/14: Added new tested information;*

437	Brocade Communications Systems, Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**Brocade ICX 7750** **Version BRCD-IP-Crypto-Ver-3.0 (Firmware)**	Freescale P2041, 1.5GHz	11/22/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2258)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2687)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2687)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. The Brocade ICX 7750 is an Ethernet switch for campus LAN aggregation and classic Ethernet data center Top of Rack (ToR) environments." *02/27/14: Added new tested information;*
436	Brocade Communications Systems, Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**Brocade ICX 6650** **Version BRCD-IP-Crypto-Ver-3.0 (Firmware)**	Freescale MPC8544E, 800 MHz	11/22/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2257)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2686)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2686)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. The Brocade ICX 6650 is an Ethernet switch for campus LAN aggregation and classic Ethernet data center Top of Rack (ToR) environments." *02/27/14: Added new tested information;*
435	Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**CiscoSSL FIPS Object Module (Assembler)** **Version 4.1**	ARM Cortex-A9 w/ Android 4.0; Intel Xeon w/ Windows 7; Freescale PowerPC-e500 w/ Linux 2.6; Intel Xeon with AES-NI w/ Windows 7; Cavium Octeon MIPS64 w/ Linux 2.6; Intel Xeon w/ Linux 2.6; Intel Xeon with AES-NI w/ Linux 2.6	11/22/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2256)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1672)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2685)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2685)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#471) (SHS Val#2256) "The Cisco FIPS Object Module is a software library that provides cryptographic services to a vast array of Cisco's networking and collaboration products."
434	AEP Networks, Ltd. Knaves Beech Business Centre Loud Water, High Wycombe, Buckinghamshire HP10 9UT United Kingdom -Paul Kettlewell TEL: +44 (0)1628 642624 -Vicky Hayes TEL: +44 (0)1628 642623	**Advanced Configurable Crypto Environment v3** **Version 011395 v2 r3 (Firmware)**	P2020 QorIQ	11/22/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256 , SHA-512) (SHS Val#2255)] "The AEP Networks Advanced Configurable Crypto Environment v3 (ACCEv3) provides highly secure cryptographic services and key storage. It is the foundation of a range of products including the Keyper Model 9860 family."
433	Aruba Networks, Inc. 1344 Crossman Ave Sunnyvale, CA 94089 USA -Jon Green TEL: 408-227-4500 FAX: 408-227-4550	**ArubaOS OpenSSL Module** **Version ArubaOS 6.3 (Firmware)**	Qualcomm Atheros AR7161; Qualcomm Atheros AR7242; Cavium CN5010; Marvell 88F6560; Qualcomm Atheros QCA9344; Qualcomm Atheros QCA9550; Broadcom XLP416; Broadcom XLP432; Broadcom XLR732; Broadcom XLR508; Broadcom XLR516; Broadcom XLR532; Broadcom XLS204; Broadcom XLS408; Freescale QorIQ P1020	11/22/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2680)] "The Aruba MOVE Architecture forms the core network infrastructure for supporting mobile and wireless computing devices. The system enables enterprise-scale 802.11 wireless LANs (Wi-Fi), secure remote VPNs, and mobility-optimized wired networks.."
432	Lancope, Inc. 3650 Brookside Parkway, Suite 400 Alpharetta, GA 30022 USA -Jason Anderson TEL: 770-225-6519 -Jim Magers TEL: 770-225-6500	**Lancope Crypto-J library** **Version 1.1**	Intel Xeon E3 series w/ Stealthwatch v6.3; Intel Xeon E5 series w/ Stealthwatch v6.3	11/22/2013	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1665)] "RSA BSAFE Crypto-J implementations used within Lancope's StealthWatch products provide cryptographic functions"

431	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**CiscoSSL FIPS Object Module** **Version 4.1**	Cavium Octeon MIPS64 w/ Linux 2.6; Intel Xeon w/ FreeBSD 9.0; Intel Xeon with AES-NI w/ Windows 8.1; Intel Xeon w/ Windows 8.1	11/22/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2247)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#1664)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2678)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2678)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#467) (SHS Val#2247) "The Cisco FIPS Object Module is a software library that provides cryptographic services to a vast array of Cisco's networking and collaboration products." *07/31/15: Added new tested information;*
430	Allegro Software Development Corporation 1740 Massachusetts Avenue Boxborough, MA 01719 USA -Alan Presser TEL: +1 (978) 264-6600	**Allegro Cryptographic Engine** **Version 1.1.8**	Intel Core 2 Duo E8400 w/ Windows 7 Ultimate (64-bit)	11/8/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2243)] "The Allegro Cryptographic Engine (ACE) is a cryptographic library module for embedded computing systems. ACE provides software implementations of algorithms for calculations of message digests, digital signature creation and verification, bulk encryption and decryption, key generation and key exchange."
429	Box Inc. 4440 El Camino Real Los Altos, CA 94022 USA -Crispen Maung TEL: 1-877-729-4269	**Box JCA Cryptographic Module** **Version 1.0**	Intel(R) Xeon(R) w/ Scientific Linux 6.4 with Java JRE 1.6.0 running on VMware vSphere 5.0; Intel(R) Xeon(R) w/ Scientific Linux 6.4 with Java JRE 1.7.0 running on VMware vSphere 5.0	11/8/2013	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (HMAC Val#1657)] "Box JCA Cryptographic Module is a Java Cryptography Architecture provider that provides encryption, hashing and random number generation utilizing FIPS 140-2 validated algorithms." *11/15/13: Added new tested information;*
428	SafeNet Inc. 4690 Millennium Drive Belcamp, MD 21017 USA -Jim Dickens TEL: 443.327.1389 FAX: 443.327.1210 -Chris Brych TEL: 613.221.5081 FAX: 613.723.5079	**SafeXcel 3120 Chip** **Part # SF114-011206-001A, v2.9.2**	N/A	11/8/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#2664)] "The SafeNet SafeXcel-3120 is a highly integrated device designed for modest performance and high security, where power and cost-sensitivity are a priority at the network edge. The embedded ARM processor, via a digital signature, will allow customer-specific application code to execute, enabling the device to implement a complete product solution."
427	Intel Corporation 2200 Mission College Blvd. Santa Clara, California 95054 USA -Stephen T Palermo TEL: 503-523-6026 -Min Cao TEL: 086-021-61165462	**QuickAssist Technology Software Library for Cryptography on the Intel® Communications Chipset 89xx Series** **Version 1.0.0** **Part # Intel® Communication Chipset 8950**	Intel® Xeon® Processor E5-2600 v2 Product Family processor w/ Fedora 16	10/25/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-256) (AES Val#2648)] "Intel® Xeon® Processor E5-2600 v2 Product Family processor with Intel® Communications Chipset 89xx Series using Intel® QuickAssist Technology. The accelerator features are invoked using the Intel® QuickAssist Technology Cryptographic API which provides application scalability and portability across platforms."
426	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A7)** **Version 4.0**	Apple A7 w/ iOS 7	10/25/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2662)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
425	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A7)** **Version 4.0**	Apple A7 w/ iOS 7	10/25/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2660)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."

424	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A7 32bit)** **Version 4.0**	Apple A7 w/ iOS 7	10/25/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2659)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software compiled for 32bit word size."
423	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A7 32bit)** **Version 4.0**	Apple A7 w/ iOS 7	10/25/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2658)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES compiled for 32bit word size."
422	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Kernel Module (Generic, A7)** **Version 4.0**	Apple A7 w/ iOS 7	10/25/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2656)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
421	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**Brocade ICX 6450 and ICX 6450-C12 Series** **Version BRCD-IP-CRYPTO-VER-2.0 (Firmware)**	ARMv5TE, 800 MHz	10/25/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2226)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. Brocade ICX6450 switches deliver enterprise-class stackable switching at an entry-level price."
420	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**Brocade SX800/SX1600 Series** **Version BRCD-IP-CRYPTO-VER-2.0 (Firmware)**	Freescale P3041E, 1.5 GHz	10/25/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2225)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. The FastIron SX Series extends control from the network edge to the core with intelligent network services, such as Quality of Service (QoS) and provides a scalable, secure, low-latency and fault-tolerant IP services solution for 1 GbE and 10 GbE enterprise deployments."
419	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**FIPS 140-2 Certification for Brocade ICX 6650** **Version BRC-IP-CRYPTO-VER-2.0 (Firmware)**	Freescale MPC8544E, 800 MHz	10/25/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2224)] "The Brocade ICX 6500 Switch is a compact Ethernet switch that delivers industry-leading 10/40 GbE density."
418	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**FIPS 140-2 Certification for Brocade MLXe and CER 2000 Series** **Version BRCD-IP-CRYPTO_VER-2.0 (Firmware)**	Freescale MPC8544, PowerQUICC III, 800 MHz	10/25/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2223)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. The Brocade MLX Series and NetIron CER 2000 Series provide industry-leading wire-speed port capacity without compromising the performance of advanced capabilities such as IPv6, MPLS and MPLS Virtual Private Networks (VPNs)."
417	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**FIPS 140-2 Certification for Brocade MLXe and CER 2000 Series** **Version BRCD-IP-CRYPTO-VER-2.0 (Firmware)**	Freescale MPC7448, RISC, 1700 MHz	10/25/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2222)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. The Brocade MLX Series and NetIron CER 2000 Series provide industry-leading wire-speed port capacity without compromising the performance of advanced capabilities such as IPv6, MPLS and MPLS Virtual Private Networks (VPNs)."
416	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA	**FIPS 140-2 Certification for Brocade MLXe and CER 2000 Series** **Version BRCD-IP-CRYPTO-VER-2.0-0131131200 (Firmware)**	Freescale MPC 7447A, RISC, 1000MHz	10/25/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2221)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations

	-Chris Marks TEL: 408-333-8101 FAX: 408-333-8101				in software. The Brocade MLX Series and NetIron CER 2000 Series provide industry-leading wire-speed port capacity without compromising the performance of advanced capabilities such as IPv6, MPLS and MPLS Virtual Private Networks (VPNs)." *11/08/13: Updated implementation information;*
415	Intel Corporation 2200 Mission College Blvd. Santa Clara, California 95054 USA -Stephen T Palermo TEL: 503-523-6026 -Min Cao TEL: 086-021-61165462	**QuickAssist Technology Software Library for Cryptography on the Intel® Communications Chipset 89xx Series** **Version 1.0.0** **Part # Intel® Communications Chipset 8950**	Intel® Xeon® Processor E5-2600 v2 Product Family processor w/ Fedora 16	10/25/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2648)] "Intel® Xeon® Processor E5-2600 v2 Product Family processor with Intel® Communications Chipset 89xx Series using Intel® QuickAssist Technology. The accelerator features are invoked using the Intel® QuickAssist Technology Cryptographic API which provides application scalability and portability across platforms." *11/05/13: Updated implementation information;*
414	Bull SAS Rue Jean Jaurès Les Clayes sous Bois, n/a 78340 France -Jean-Luc CHARDON TEL: +33 1 30 80 79 14 FAX: +33 1 30 80 76 36 -Pierre-Jean AUBOURG TEL: +33 1 30 80 77 02 FAX: +33 1 30 80 76 36	**C2P DRBG** **Version 20121030 (Firmware)**	Freescale MPC8248	10/25/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2647)] "Bull implements this Deterministic Random Bit Generator algorithm for applications running on its CHR hardware platform providing secure cryptographic resources to products developed by Bull or other Application Providers, including the CRYPT2Pay HR and CRYPT2Protect product lines."
413	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -Rose Quijano-Nguyen TEL: 650-527-0741	**Symantec SymCrypt Cipher Engine** **Version 1.1**	Intel Xeon Quad Core w/ RHEL 6.4 x86_64 64-bit	10/25/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2646)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2646)] "The Symantec SymCrypt Cipher Engine is designed to provide FIPS140-2 algorithm support for the Symantec SymCrypt Cryptographic Module. This module supports Symantec Applications by providing validated and approved Cryptographic Services. The incorporation of these algorithms make these products ideal for enterprise and government applications."
412	Sonus Networks Inc. 4 Technology Park Drive Westford, MA 01886 USA -Sandeep Kaushik TEL: 1-855-GO-SONUS FAX: 978-614-8101 -Nui Chan TEL: 1-855-GO-SONUS FAX: 978-614-8101	**Sonus Cryptographic Library** **Version 1**	Intel Nehalem w/ Sonus Debian Linux 02.00.02-A026	10/25/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2643)] BlockCipher_No_df: (AES-128) (AES Val#2643)] "Sonus Session Border Controller FIPS-validated cryptographic software module"
411	EFJohnson Technologies 1440 Corporate Drive Irving, TX 75038-2401 USA -Marshall Schiring TEL: (402) 479-8375 FAX: (402) 479-8472 -Josh Johnson TEL: (402) 479-8394 FAX: (402) 479-8472	**EFJ Crypto** **Version 5.0 (Firmware)**	Texas Instruments TMS320VC55xx	10/25/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2213)] "(1) EFJ Crypto description: The EFJ Crypto includes SP800-90A DRBG, RSA, HMAC, SHA256, AES for use in the EFJohnson Subscriber Encryption Module."
410	Vaultive Inc. 489 5th Avenue, floor 31 New York, NY 10017 USA -Steve Coplan TEL: 212-875-1210	**Vaultive Cryptographic Library** **Version 1.0**	Intel Xeon E5 series with AES-NI w/ Ubuntu Server 12.04LTS	10/1/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2638)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2638)] "Vaultive Cryptographic Module implements several NIST-approved cryptographic algorithms. Vaultive Inc. uses the Vaultive Cryptographic Module to deliver cloud encryption solutions preserving server-side operations including indexing, searching, record sorting and format preservation without compromising security."
409	Cisco Systems Inc. 170 West Tasman Drive	**CiscoSSL FIPS Object Module (Assembler)**	ARM Cortex-A9 w/ Android 4.0; Intel Xeon w/ Windows 7; Freescale PowerPC-e500	10/1/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 ,

	San Jose, CA 95134 USA -Global Certification Team	**Version 4.0**	w/ Linux 2.6; Freescale PowerPC-e500 w/ Linux 2.6; Intel Xeon with AES-NI w/ Windows 7; Cavium Octeon MIPS64 w/ Linux 2.6; Intel Xeon w/ Linux 2.6; Intel Xeon with AES-NI w/ Linux 2.6		SHA-384 , SHA-512) (SHS Val#2210)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1630)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2637)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2637)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#456) (SHS Val#2210) "The Cisco FIPS Object Module is a software library that provides cryptographic services to a vast array of Cisco's networking and collaboration products."
408	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**CiscoSSL FIPS Object Module** **Version 4.0**	Cavium Octeon MIPS64 w/ Linux 2.6; Intel Xeon w/ FreeBSD 9.0	10/1/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2209)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1629)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2636)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2636)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#455) (SHS Val#2209) "The Cisco FIPS Object Module is a software library that provides cryptographic services to a vast array of Cisco's networking and collaboration products."
407	Microsemi Corporation One Enterprise Aliso Viejo, CA 92656 USA -Richard Newell TEL: (408) 643-6146	**Microsemi SoC Cryptographic Module Mark II** **Version 1.0 (Firmware)**	Mentor Graphics Questa Simulator 10.1c	10/1/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2628)] "The Microsemi SoC Cryptographic Module provides custom hardware/firmware acceleration of the standard cryptographic algorithms used in Microsemi FPGAs and SoC FPGAs like SmartFusion®2 and Igloo®2. They are used to securely configure the devices, and are also made available to the FPGA user via an internal bus interface for use in end applications."
406	ViaSat Inc. 6155 El Camino Real Carlsbad, CA 92009 USA -David Schmolke TEL: 760-476-2461 FAX: 760-476-4110 -Rich Quintana TEL: 760-476-2481 FAX: 760-476-4110	**ES_Cryptoservices_1.0** **Version ES_Cryptoservices_1.0 (Firmware)**	Altera Cyclone III FPGA	10/1/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2633)] "ViaSat Embeddable Security System cryptographic algorithm implementations."
405	Entrust Inc. One Lincoln Centre 5400 LBJ Freeway Suite 1340 Dallas, TX 75240 USA -Greg Wetmore TEL: 613-270-2773 FAX: 613-270-3400 -Mark Joynes TEL: 613-270-3134 FAX: 613-270-3400	**Entrust Authority™ Security Kernel** **Version 8.1Sp1 R2**	Intel Core 2 Duo E8400 w/ Microsoft Windows Server 2008 R2 Enterprise Edition	9/27/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-512) (SHS Val#2206)] "The Security Kernel is a C++ implementation of cryptographic functions accessible by an object-oriented API. Depending on configuration, the algorithms may be implemented in software, hardware or both. The industry standard Cryptoki API from PKCS #11, is used as the interface to hardware-based cryptographic modules."
404	BlackBerry 295 Phillip Street Waterloo, ON N2L3W8 Canada -Security Certifications Team TEL: 519-888-7465x72921 FAX: 905-507-4230	**BlackBerry Cryptographic Algorithm Library** **Version 6.1**	Intel Xeon X5650 w/ CentOS 5.5 Linux 32-bit; Intel Xeon X5650 w/ CentOS 5.5 Linux 64-bit; Intel Xeon X5650 w/ Windows XP 32-bit; Intel Xeon X5650 w/ Windows XP 64-bit; ARMv7 w/ QNX Neutrino 8.0	9/30/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2207)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1629)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2633)]

					Dual_EC_DRBG:[Prediction Resistance Tested: Not Enabled (P-256: SHA-256) (P-384: , SHA-384) (P-521: , SHA-512) (ECDSA Val#455) (SHS Val#2207) "The BlackBerry Cryptographic Algorithm Library is a suite of cryptographic algorithms that provides advanced cryptographic functionality to systems running BlackBerry 10 OS and components of BlackBerry Enterprise Service 10."
403	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**IOS Common Cryptographic Module (IC2M) within Cat4K** **Version Rel 1 (1.0.0) (Firmware)**	Freescale MPC8572E	9/11/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2624)] "IOS Common Cryptographic Module within cat4k"
402	Box, Inc. 4440 El Camino Real Los Altos, CA 94022 USA -Crispen Maung TEL: (650) 329-1210	**Box Upload/Download Cryptographic Module** **Version 1**	Intel(R) Xeon(R) w/ Scientific Linux 6.4 running on VMware vSphere 5.0	9/11/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2622)] BlockCipher_No_df: (, AES-256) (AES Val#2622)] "Box's cryptographic module is a C language-based implementation of cryptographic functions built using an OpenSSL FIPS Object Module. Box provides assurance that content encrypted by the product utilizes a FIPS 140-2 solution." *09/24/13: Updated implementation information;*
401	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**IOS Algorithms** **Version 1.0 (Firmware)**	Cavium CN5200; Freescale MPC8572E; Intel 82576; Freescale P1021; Freescale MPC8358E	8/30/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2620)] "IOS Firmware cryptographic implementations used within Cisco devices to provide cryptographic functions." *01/30/14: Updated implementation information;*
400	SafeNet, Inc. 4690 Millennium Drive Belcamp, MD 21017 USA -Stan Mesceda TEL: 443-327-1582 -Chris Brych TEL: 613-221-5081 FAX: 613-723-5079	**SxE Cryptographic Library** **Version 4.3 (Firmware)**	Motorola Freescale MPC8280 (PPC32)	8/30/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2196)] "The SxE Cryptographic Library provides cryptographic algorithms for the SxE family of products. Based on OpenSSL, the SxE Cryptographic Library exposes an Application Programming Interface (API) to support software based security relevant services within SafeNet's SxE product line."
399	Motorola Solutions Inc. 6480 Via Del Oro San Jose, CA 95119 USA -Ashot Andreasyan TEL: 408-826-3203 FAX: 408-528-2883	**OpenSSL Crypto library-DRBG** **Version v1_0_1_1 (Firmware)**	Free Scale MPC-7457; Free Scale MPC-7457	8/29/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2057)] "The 1.0.1c crypto library is used for protecting security parameters and key exchange protocol messages; authenticating a user; generating cryptographic and key encryption keys in GGM8000 and s6000 transport gateways."
398	Harris Corporation 1680 University Avenue Rochester, NY 14610 USA -Robert Magnant TEL: 585-242-3785 FAX: 585-241-8459 -Elias Theodorou TEL: 585-242-3785 FAX: 585-241-8459	**RF-7800W OU47x, OU49x, OU50x** **Version 2.00 (Firmware)**	Broadcom XLS108	8/29/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-256) (SHS Val#2190)] "This is a firmware library that provides the cryptographic functions used on Harris' industry leading reliable, secure and high performance Broadband Ethernet Radio (BER) products: RF-7800W-OU50x, -OU47x, -OU49x."
397	Toshiba Corporation 1-1, Shibaura 1-chome Minato-ku, Tokyo 105-8001 Japan -Akihiro Kimura TEL: +81-45-890-2856 FAX: +81-45-890-2593	**Toshiba Secure Cryptographic Suite for Enterprise SSD** **Version 1 (Firmware)**	Cortex-R4	8/16/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2183)] "A library of unique software and hardware cipher solutions which are standard encryption algorithm-based to provide Toshiba enterprise SSD products and the systems using them a robust and secure data storage environment."
396	RSA Security Inc. 177 Bovet Road, Suite 200 San Mateo, CA 94402 USA	**RSA BSAFE® Crypto-J Software Module** **Version 4.1**	PowerPC (32bit) w/ Linux 2.6 with Sun JRE 5.0; ARM9 (32bit) w/ Linux 2.6 with Sun JRE 6.0	8/16/2013	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1609)] **Dual_EC_DRBG**:[Prediction Resistance Tested:

	-Kathy Kriese TEL: 650-931-9781				Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#447) (SHS Val#2186) "RSA BSAFE Crypto-J security software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. It supports a wide range of industry standard encryption algorithms offering Java developers the flexibility to choose the option most appropriate to meet their requirements."
395	Integral Memory PLC. Unit 6 Iron Bridge Close Iron Bridge Business Park Off Great Central Way London, Middelsex NW10 0UF United Kingdom -Patrick Warley TEL: +44 (0)20 8451 8700 FAX: +44 (0)20 8459 6301 -Samik Halai TEL: +44 (0)20 8451 8704 FAX: +44 (0)20 8459 6301	**AES Module** **Version 1.0 (Firmware)**	PS2251-13 and PS2251-15	8/16/2013	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256) (HMAC Val#1608)] "The Integral Memory AES USB 3.0 drives are removable storage devices which encrypt data transferred onto them. They offer Premium AES 256 bit security, and come in various sizes."
394	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Mark Hanson TEL: 651-628-1633 FAX: 651-628-2706	**McAfee Core Cryptographic Module BSAFE** **Version 1.0**	Intel Core i5 with AES-NI and RdRand w/ Windows 8 running in 64-bit UEFI mode; Intel Core i3 without AES-NI w/ McAfee Endpoint Encryption Preboot OS; Intel Core i5 with AES-NI w/ McAfee Endpoint Encryption Preboot OS; Intel Core i7 with AES-NI w/ McAfee Endpoint Encryption Preboot OS; Intel Core i3 without AES-NI, with RdRand w/ Windows 8 running in 64-bit UEFI mode; Intel Core i7 with AES-NI and RdRand w/ Windows 8 running in 64-bit UEFI mode; Intel Core i5 without AES-NI or RdRand w/ Windows 8 running in 32-bit UEFI mode; Intel Atom without AES-NI or RdRand w/ Windows 8 running in 32-bit UEFI mode; Intel Core i3 with AES-NI and RdRand w/ MacOS X Mountain Lion v10.8; Intel Core i5 with AES-NI and RdRand w/ MacOS X Lion v10.7; Intel Core i7 with AES-NI and RdRand w/ MacOS X Mountain Lion v10.8; Intel Core i5 with AES-NI but not RdRand w/ Windows Vista 32-bit ; Intel Core i7 with AES-NI but not RdRand w/ Windows Vista 64-bit; Intel Core i5 with AES-NI but not RdRand w/ Windows 7 32-bit; Intel Core i5 with AES-NI and RdRand w/ Windows 8 32-bit; Intel Core i5 with AES-NI and RdRand w/ Windows 8 64-bit; Intel Core 2 Duo without AES-NI or RdRand w/ Macintosh platform running EFI preboot; Intel Xeon without AES-NI or RdRand w/ Macintosh platform running EFI preboot; Intel Core i3 with AES-NI and RdRand w/ Macintosh platform running EFI preboot; Intel Core i5 with AES-NI and RdRand w/ Macintosh platform running EFI preboot; Intel Core i7 with AES-NI and RdRand w/ Macintosh platform running EFI preboot; Intel Core i3 without AES-NI or RdRand w/ Windows XP 32-bit; Intel Core i3 without AES-NI or RdRand w/ Windows 7 64-bit; Intel Core i7 with AES-NI and RdRand w/ Windows 7 64-bit; Intel Core i7 with AES-NI and RdRand w/ Windows 8 64-bit; Intel Atom without AES-NI or RdRand w/ Windows 8 32-bit; Intel Core 2 Duo without AES-NI or RdRand w/ MacOS X Lion v10.7; Intel Xeon without AES-NI or RdRand w/ MacOS X Mountain Lion v10.8;	8/16/2013	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (HMAC Val#1604)] "This Cryptographic algorithm module provides cryptographic functionality for McAfee's Endpoint Encryption product range." *11/19/13: Updated implementation;* *12/17/13: Added new tested information;*
393	FRAMA AG Unterdorf Lauperswil, Bern CH-3438 Switzerland -Beat Waelti TEL: +41-34-49698-98 FAX: +41-34-49698-00	**PSD-II by FRAMA** **Version V2.0.6 (Firmware)** **Part # FRM-II Version 1.2**	firmware: running on built-in Fujitsu MB91302APM1R micro controller	8/16/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2179)] "The PSD-II (Postal Security Device-II) is a hardware/firmware cryptographic module to be used in automated franking machines."
392	Senetas Corporation Ltd. and SafeNet Inc. Level 1, 11 Queens Road	**CN1000 and CN3000 Series Common Crypto Library** **Version 0.98 (Firmware)**	Freescale MPC8280	7/22/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2178)]

	Melbourne, Victoria 3004 Australia -John Weston TEL: +61 3 9868 4555 FAX: +61 3 9821 4899 -Chris Brych TEL: +1 613 221 5081 FAX: +1 613 723 5079				"The CN1000 and CN3000 Series Common Crypto Library Module provides FIPS 140-2 approved cryptographic algorithms for the CN1000 and CN3000 Series Encryptors. Based upon OpenSSL the Library provides an Application Programming Interface (API) to support security relevant services." *09/30/13: Updated vendor information;*
391	Senetas Corporation Ltd. and SafeNet Inc. Level 1, 11 Queens Road Melbourne, Victoria 3004 Australia -John Weston TEL: +61 3 9868 4555 FAX: +61 3 9821 4899 -Chris Brych TEL: +1 613 221 5081 FAX: +1 613 723 5079	**CN6000 Series Common Crypto Library** **Version 0.98 (Firmware)**	Intel ATOM	7/22/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2177)] "The CN6000 Series Common Crypto Library Module provides FIPS 140-2 approved cryptographic algorithms for CN6000 Series Encryptors. Based upon OpenSSL the Common Crypto Library provides an Application Programming Interface (API) to support security relevant services." *09/30/13: Updated vendor information;*
390	Senetas Corporation Ltd. and SafeNet Inc. Level 1, 11 Queens Road Melbourne, Victoria 3004 Australia -John Weston TEL: +61 3 9868 4555 FAX: +61 3 9821 4899 -Chris Brych TEL: +1 613 221 5081 FAX: +1 613 723 5079	**CS Series Common Crypto Library** **Version 0.98 (Firmware)**	Intel Core 2 Duo LGA775; AMD Geode LX800	7/22/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2176)] "The CS Series Common Crypto Library Module provides FIPS 140-2 approved cryptographic algorithms for the CS10 and CS100 Encryptors. Based upon OpenSSL the Library provides an Application Programming Interface (API) to support security relevant services."
389	Vidyo Inc. 433 Hackensack Avenue Hackensack, NJ 07601 USA -Adi Regev TEL: 201-467-4636	**Cryptographic Security Kernel** **Version 1.0**	quad-core Nvidia Tegra 3 w/ Android 4.1.1; TI dual-core OMAP4470 w/ Kindle 8.4.3; dual-core Nvidia Tegra 2 w/ Android 4.1.1;quad-core Cortex A9 (T30L) w/ Android 4.2.2; quad-core Cortex-A9 w/ Android 4.1.2; dual-core ARM Cortex-A9 w/ Android 4.0.4; single-core ARM Cortex-A8 w/ Android 4.1.2; ARMv7s Apple A6X w/ iOS 6.1; ARMv7s Apple A6 w/ iOS 6.1	7/22/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2576)] "Vidyo creates HD video conferencing products that leverage their patented Adaptive Video Layering Architecture technology, which provides continuous HD video streaming regardless of network conditions. The Vidyo Cryptographic Security Kernel supplies the cryptographic services necessary to support Vidyo's secure video and data transmissions."
388	Certicom Corp. 4701 Tahoe Blvd. Building A Missisauga, ON L4W 0B5 Canada -Certicom Sales TEL: 1-905-507-4220 FAX: 1-905-507-4230 -Ian Laidlaw TEL: 1-289-261-4277 FAX: 1-905-507-4230	**Security Builder® FIPS Core** **Version 6.1**	Intel x86 (Xeon X5650) w/ CentOS Linux 32-bit; Intel x64 (Xeon X5650) w/ CentOS Linux 64-bit; Intel x86 (Xeon X5650) w/ Windows XP 32-bit; Intel x64 (Xeon X5650) w/ Windows XP 64-bit; ARMv7 w/ QNX Neutrino 8.0	7/15/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2164)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1585)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2568)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-256) (P-384:) (P-521: , SHA-512) (ECDSA Val#442) (SHS Val#2164) "Security Builder® FIPS Core provides application developers with cryptographic tools to easily integrate encryption, digital signatures and other security mechanisms into C-based apps for FIPS 140-2 and Suite B security. It can also be used with Certicom's PKI, IPSec and SSL modules."
387	Blue Ridge Networks 14120 Parke Long Court, Suite 103 Chantilly, VA 20151 USA -Nancy Canty TEL: 703-633-7331	**BorderGuard Cryptographic Module** **Version 2.0 (Firmware)**	AMCC 440GX	7/5/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#429)] "Cryptographic algorithms implemented in the BorderGuard DPF1 firmware."
386	Blue Coat Systems Inc. 420 North Mary Avenue Sunnyvale, California 94085-4121 USA -Diana Robinson TEL: +1 (845) 454-6397 -Tammy Green TEL: +1 (801) 999-2973	**SGOS 6.5 Cryptographic Library** **Version 3.1.1 (Firmware)**	AMD64 Opteron (Istanbul); AMD64 Opteron (Shanghai); Intel Clarkdale; Intel Lynnfield; VIA NANO	7/5/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2560)] BlockCipher_No_df: (, AES-256) (AES Val#2560)] "The SGOS 6.5 Cryptographic Library provides the necessary cryptographic services to Blue Coat's proprietary operating system (SGOS 6.5), developed specifically for use on their family of Unified Security and Optimization solutions for business assurance."

385	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**CiscoSSL FIPS Object Module (Assembler)** **Version 2.1**	ARMv7 w/ Android 4.0; PowerPC, Freescale's PowerQUICC III Processor Family w/ Linux 2.6	7/5/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2157)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1578)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2558)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2558)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#440) (SHS Val#2157) "The Cisco FIPS Object Module is a software library that provides cryptographic services to a vast array of Cisco's networking and collaboration products."
384	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**ACT-2Lite** **Part # 15-14497-02(AT90S072)**	N/A	7/5/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#2556)] "ACT-2Lite is an ASSP which is based on a smart card hardware platform with custom ROM code provided by Cisco." *12/20/13: Updated implementation information;*
383	Pulse Secure LLC. 2700 Zanker Road, Suite 200 San Jose, CA 95134 USA -Yvonne Sang TEL: 408-372-9600	**Secure Pulse Cryptographic Module** **Version 1.0**	Intel Pentium E2160 (x86) w/ IVE OS 1.1; Intel Xeon E5530 (x86) w/ IVE OS 1.1 on VMware ESX; Intel Xeon x5670 (x86) with AES-NI w/ IVE OS 1.1 on VMware ESXi; Intel Core i5-2430M (x86) 64-bit with AES-NI w/ Microsoft Windows 7; Intel Core i5-2430M (x86) 32-bit with AES-NI w/ Microsoft Windows 7; Intel Core i7-3615QM (x86) with AES-NI w/ OS X 10.8; Intel Xeon x5670 (x86) w/ IVE OS 1.1 on VMware ESXi; Intel Core i7-3615QM (x86) w/ OS X 10.8	7/5/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2153)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1573)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2553)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2553)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#438) (SHS Val#2153) "The Secure Pulse Cryptographic Module provides secure cryptographic services. It enables dynamic SSL VPN, NAC, mobile security, online meetings and collaboration, and application acceleration while removing the complexities of device type and security state, location, identity, and adherence to policies." *01/26/15: Updated vendor information;*
382	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**Cisco IOS-XE** **Version 3.7.2tS (Firmware)**	Freescale Semiconductor 8548 Power QUICC; Intel Xeon	6/28/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2549)] "The ASR 1000 Routers accelerate services by offering performance and resiliency with optimized, intelligent services." *07/03/13: Updated implementation information;*
381	Cisco Systems Inc. 170 W. Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**ONS Encryption Card Firmware Algorithms** **Version 1.0 (Firmware)**	Freescale P1010	6/28/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2548)] "Firmware algorithm implementations for the ONS encryption cards."
380	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A6)** **Version 4.0**	Apple A6 w/ iOS 7	6/28/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2547)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
379	Cisco Systems Inc. 170 W. Tasman Drive San Jose, CA 95134 USA	**ONS Controller Card Firmware Algorithms** **Version 1.0 (Firmware)**	Freescale MPC8568E	6/28/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2147)] **HMAC_Based DRBG**: [Prediction Resistance

	-Global Certification Team				Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1567)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2546)] "Firmware algorithm implementations for the ONS controller cards."
378	AFORE Solutions Inc. 2680 Queensview Drive Unit 150 Ottawa, ON K2B 8J9 Canada -Tim Bramble TEL: 613-224-5995 ext 232 FAX: 613-224-5410 -Hans Johnsen TEL: 613-224-5995 ext 257 FAX: 613-224-5410	**CloudLink Crypto Module** **Version 1.0**	Intel Xeon E5-2420 w/ Linux Ubuntu 12.04 with VMWare ESXi 5.1.0	6/28/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2146)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1566)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2545)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2545)] "The CloudLink Cryptographic Module is a general purpose cryptographic library which provides cryptographic services for all CloudLink application modules." *02/21/14: Updated implementation information;*
377	BlackBerry 295 Phillip Street Waterloo, ON N2L3W8 Canada -Eric Jen TEL: +1 561-289-0214	**BlackBerry Algorithm Library for Secure Work Space** **Version 1.0**	Intel Xeon 3430 w/ Ubuntu 12.04; Intel Xeon 3430 w/ Ubuntu 12.04 on ESXi 5.1; AMD Opteron 275 w/ Ubuntu 12.04; AMD Opteron 275 w/ Ubuntu 12.04 on ESXi 5.1; ARMv7-based A5 processor w/ iOS 5.0; ARM v7s -- Apple A6 w/ iOS 6.0; ARMv7-based Qualcomm Snapdragon processor w/ Android v4.1	6/28/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2145)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1565)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2544)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#436) (SHS Val#2145) "The BlackBerry Algorithm Library for Secure Work Space provides a suite of cryptographic services utilized by the BlackBerry Cryptographic Library for the BlackBerry Secure Work Space (BBSWS). BBSWS provides the secure operation and management of iOS and Android devices when used in conjunction with BlackBerry® mobile device management solutions."
376	Kanguru Solutions 1360 Main Street Millis, MA 02054 USA -Nate Cte TEL: 508-376-4245 FAX: 508-376-4462	**Kanguru Defender HDD 3000** **Version V01.04.0000.0000 (Firmware)**	TSI-1480 OX3010	6/20/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2144)] "The Kanguru Defender HDD 3000 is a hardware encrypted USB security device designed for secure data storage. It is also used as a platform to run secure virtual operating systems and applications."
375	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Generic, i7 32bit)** **Version 4.0**	Intel i7 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2541)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
374	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Generic, i5 32bit)** **Version 4.0**	Intel i5 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2540)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software compiled for 32bit word size."
373	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (AES-NI with optimized block chaining modes, i7 32bit)** **Version 4.0**	Intel i7 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2539)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS compiled for 32bit word size."

372	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (AES-NI with optimized block chaining modes, i5 32bit)** **Version 4.0**	Intel i5 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2538)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS compiled for 32bit word size."
371	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Assembler AES, i7 32bit)** **Version 4.0**	Intel i7 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2533)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES compiled for 32bit word size."
370	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Assembler AES, i5 32bit)** **Version 4.0**	Intel i5 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2532)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES compiled for 32bit word size."
369	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Generic, i7)** **Version 4.0**	Intel i7 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2531)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
368	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (AES-NI with optimized block chaining modes, i7)** **Version 4.0**	Intel i7 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2529)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
367	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Assembler AES, i7)** **Version 4.0**	Intel i7 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2527)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
366	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Generic, i5)** **Version 4.0**	Intel i5 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2524)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
365	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (AES-NI with optimized block chaining modes, i5)** **Version 4.0**	Intel i5 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2521)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
364	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module (Assembler AES, i5)** **Version 4.0**	Intel i5 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2519)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
363	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (Generic, i7)** **Version 4.0**	Intel i7 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2518)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks.

					The testing applies to kernel space and generic, non-optimized software."
362	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (AES-NI with optimized block chaining modes, i7)** **Version 4.0**	Intel i7 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2516)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
361	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (Assembler AES, i7)** **Version 4.0**	Intel i7 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2515)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and assembler optimized AES."
360	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (Generic, i5)** **Version 4.0**	Intel i5 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2514)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
359	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (AES-NI with optimized block chaining modes, i5)** **Version 4.0**	Intel i5 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2512)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
358	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module (Assembler AES, i5)** **Version 4.0**	Intel i5 w/ OSX 10.9	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2511)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and assembler optimized AES."
357	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A5)** **Version 4.0**	Apple A5 w/ iOS 7	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2509)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
356	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Generic, A4)** **Version 4.0**	Apple A4 w/ iOS 7	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2508)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
355	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A6)** **Version 4.0**	Apple A6 w/ iOS 7	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2501)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
354	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A5)** **Version 4.0**	Apple A5 w/ iOS 7	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2500)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
353	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module (Assembler AES, A4)** **Version 4.0**	Apple A4 w/ iOS 7	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2499)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks.

					The testing applies to user space and assembler optimized AES."
352	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Kernel Module (Generic, A6)** **Version 4.0**	Apple A6 w/ iOS 7	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2498)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
351	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Kernel Module (Generic, A5)** **Version 4.0**	Apple A5 w/ iOS 7	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2497)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
350	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Kernel Module (Generic, A4)** **Version 4.0**	Apple A4 w/ iOS 7	6/20/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2496)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
349	Freescale Semiconductor Inc. 7700 West Parmer Lane Austin, TX 78729 USA -Geoffrey Waters TEL: 512-996-5815 FAX: 512-996-7866 -Tom Tkacik TEL: 480-814-3299 FAX: 480-814-3660	**RNG4 4.2** **Version CAVP_RNG4_4.2_C290R1 (Firmware)**	Chronologic VCS simulator, vcs D-2010.06-04	6/20/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256) (SHS Val#2112)] "Freescale's RNG4 4.2 is included in multiple QorIQ Integrated Communications Processor, including: T4240r2, T2080, T1040, and the C29x family of security co-processors."
348	Freescale Semiconductor Inc. 7700 West Parmer Lane Austin, TX 78729 USA -Geoffrey Waters TEL: 512-996-5815 FAX: 512-996-7866 -Tom Tkacik TEL: 480-814-3299 FAX: 480-814-3660	**RNG4 4.1** **Version CAVP_RNG4_4.1_P5040R1 (Firmware)**	Chronologic VCS simulator, vcs D-2010.06-04	6/20/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256) (SHS Val#2111)] "Freescale's RNG4 4.1 is included in multiple QorIQ Integrated Communications Processor, including: T4240r1, P5040, and QorIQ Qonverge products B4860r1."
347	OpenPeak Inc. 1750 Clint Moore Road Boca Raton, FL 33487 USA -Eric Jen TEL: +1 561-893-7881 -Howard A. Kwon TEL: +1 561 893 7930 FAX: +1 561 208 8026	**OpenPeak Cryptographic Security Module** **Version 1.0.1**	Intel Xeon 3430 w/ Ubuntu 12.04; Intel Xeon 3430 w/ Ubuntu 12.04 on ESXi 5.1; AMD Opteron 275 w/ Ubuntu 12.04; AMD Opteron 275 w/ Ubuntu 12.04 on ESXi 5.1; ARM v7 -- Apple A5 w/ iOS 5.0; ARMv7-based A6 processor w/ iOS 6.0; IARMv7-based Qualcomm Snapdragon processor w/ Android v4.1	6/20/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2107)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1531)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2489)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#417) (SHS Val#2107) "The OpenPeak Cryptographic Security Library provides advanced cryptographic functionalities for the OpenPeak Cryptographic Security Module (OCSM). The OCSM provides a secure encrypted container for enterprise-managed applications, content and data to enable a highly secure mobile workspace."
346	Hewlett Packard India Software Operations Pvt Ltd Sy. No. 192, Whitefield Road Mahadevpura Post Bangalore, Karnataka 560048 India -Rahul Philip Mampallil TEL: +91 80 33841568 -Karthik Bhagawan TEL: +91 80 25166873 FAX: +91 80 28533522	**HP-UX Kernel Cryptographic Module** **Version 1.0**	Intel Itanium w/ HP-UX 11i v3	6/7/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256) (SHS Val#2106)] "HP-UX Kernel Crypto Module (HP-UX KCM) is a kernel-space shared library in the HP-UX OS containing core cryptographic algorithms in one central place. It implements asymmetric, symmetric, message authentication, and digest operations used by various HP-UX products. It is available on HP-UX 11i v3 OS on HP Integrity Platform."

345	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Mark Hanson TEL: +1 651 628 1633 FAX: +1 651 628 2706	**McAfee Linux OpenSSL** **Version 1.01**	Xeon w/ MLOS v2.2 running on VMware ESXi 4.1; Xeon w/ MLOS v2.2 running on VMware ESXi 5.0	6/7/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2105)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1529)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2487)] "McAfee Linux cryptographic modules provide cryptographic services for McAfee Linux and security appliance products built upon this platform. McAfee Linux is an operating system built with a focus on the needs of security appliances."
344	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Mark Hanson TEL: +1 651 628 1633 FAX: +1 651 628 2706	**McAfee Linux OpenSSL** **Version 1.01 (Firmware)**	Celeron; Intel Core i3; Xeon	6/7/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2104)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1528)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2486)] "McAfee Linux cryptographic modules provide cryptographic services for McAfee Linux and security appliance products built upon this platform. McAfee Linux is an operating system built with a focus on the needs of security appliances."
343	RSA The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Damon Hopley TEL: 781-515-6355	**RSA BSAFE Crypto-C Micro Edition (ME)** **Version 3.0.0.20**	PowerPC e500v2 w/ VxWorks General Purpose Platform 6.8	5/31/2013	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1527)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#414) (SHS Val#2103) "RSA BSAFE® Crypto-C ME software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. The software supports a wide range of industry standard encryption algorithms offering developers the flexibility to choose the appropriate option to meet their requirements."
342	OpenSSL Software Foundation Inc. 1829 Mount Ephraim Road Adamstown, MD 27101 USA -Steve Marquess TEL: 877-673-6775	**OpenSSL FIPS Object Module** **Version 2.0.5**	Freescale i.MX27 926ejs (ARMv5TEJ) w/ eCos 3; Freescale i.MX25 (ARMv4) w/ QNX 6.4; Apple A6X Soc (ARMv7s) w/ iOS 6.1; Intel Xeon E3-1220 w/ VMware Horizon Workspace 1.5 under vSphere; Intel Xeon E3-1220 w/ AES-NI w/ VMware Horizon Workspace 1.5 under vSphere; AM335x Cortex-A8 (ARMv7) w/ Ubuntu 13.04; ARM926 (ARMv5TEJ) w/ Linux 3.8; AM335x Cortex-A8 (ARMv7) with NEON w/ Ubuntu 13.04; Intel Xeon E5-2430L (x86) without AES-NI w/ Linux 3.4 64-bit under Citrix XenServer; Intel Xeon E5-2430L (x86) with AES-NI w/ Linux 3.4 64-bit under Citrix XenServer; Intel Xeon E5-2430L (x86) without AES-NI w/ Linux 3.4 64-bit on under VMware ESX; Intel Xeon E5-2430L (x86) with AES-NI w/ Linux 3.4 64-bit under VMware ESX; Intel Xeon E5-2430L (x86) without AES-NI w/ Linux 3.4 64-bit under Microsoft Hyper-V; Intel Xeon E5-2430L (x86) with AES-NI w/ Linux 3.4 64-bit under Microsoft Hyper-V; Apple A5 / ARM Cortex-A9 (ARMv7) without NEON w/ iOS 6.0; Apple A5 / ARM Cortex-A9 (ARMv7) with NEON w/ iOS 6.0; Intel Xeon E5-2430L (x86) with AES-NI w/ PexOS 1.0 on x86 under vSphere; Intel Xeon E5-2430L (x86) without AES-NI w/ PexOS 1.0 on x86 under vSphere	5/31/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-512) (SHS Val#2102)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1526)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2484)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2484)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#413) (SHS Val#2102) "The OpenSSL FIPS Object Module is a full featured general purpose cryptographic library that is distributed in source code form under an open source license. It can be downloaded from www.openssl.org/source/." *08/06/13: Updated implementation information;* *08/13/13: Added new tested information;* *10/25/13: Added new tested information;* *11/14/13: Added new tested information;*
341	Cisco Systems Inc. 170 West Tasman Dr. San Jose, CA 95134 USA -Global Certification Team	**Adaptive Security Appliance OS** **Version 9.1.5 (Firmware)**	Intel Core i3-540; Intel Xeon 3400; Intel Xeon 5500; Intel Xeon 5600; Intel Pentium G6900	5/24/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#2100)] "Cisco ASA Security Appliance Series deliver robust user and application policy enforcement, multi-vector attack protection, and secure connectivity services in cost-effective, easy-to-deploy solutions. The ASA 5500 Series Adaptive Security

					Appliances provide comprehensive security, performance, and reliability for network environment." *10/08/2014: Implementation version number changed*
340	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Mark Hanson TEL: +1 651 628 1633 FAX: +1 651 628 2706	**RSA Bsafe Crypto-J** **Version 4.1 (Firmware)**	Intel Celeron; Intel Xeon	5/24/2013	**Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (ECDSA Val#410) (SHS Val#2099) "McAfee Firewall Enterprise Control Center simplifies the management of multiple McAfee Firewall Enterprise appliances. Control Center enables centralized management and monitoring of the McAfee Firewall Enterprise solutions, allowing network administrators to centrally define firewall policy, deploy updates and inventory their firewall products."
339	Cisco Systems, Inc. 170 West Tasman Dr. San Jose, CA 95134 USA -Global Certification Team	**Cavium Nitrox PX (CN1520)** **Part # CN1520-350BG256-G, v1.2**	N/A	5/24/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1793)] "Cisco ASA Security Appliance Series deliver robust user and application policy enforcement, multi-vector attack protection, and secure connectivity services in cost-effective, easy-to-deploy solutions. The ASA 5500 Series Adaptive Security Appliances provide comprehensive security, performance, and reliability for network environment."
338	Juniper Networks, Inc 1194 N. Mathilda Ave Sunnyvale, CA 94089 USA -Sharath Sridhar TEL: +91 80 30538736 FAX: +91 80 30538824	**OpenSSL** **Version Junos 12.1R6.6 (Firmware)**	ARM v5, Marvell's Feroceon processor Family; PowerPC, Freescale's PowerQUICC III Processor Family	5/24/2013	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1518)] "Comprehensive, scalable switching solutions specifically designed to meet the needs of both enterprises and service providers. All of our switches - modular and fixed platforms - run on one common operating system- Junos."
337	Silicon Motion Technology Corp. 8F-1, No. 36, Taiyuan St. Jhubei City, Hsinchu County 30265 Taiwan -Cash Lo TEL: +886-3-5526888 FAX: +886-3-5526988	**Silicon Motion Cryptographic Library** **Version 1.0 (Firmware)**	Cadence NC-verilog hardware simulator v10.20	5/24/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256) (SHS Val#2093)] "Silicon Motion Crypto Library is a hardware cryptographic library providing core cryptographic functionality for Silicon Motion security products which are capable to develop complex and flexible security applications."
336	Cisco Systems Inc. 170 West Tasman Dr. San Jose, CA 95134 USA -Global Certification Team	**Cavium Nitrox PX (CN1610)** **Part # CN1610-350BG233**	N/A	5/24/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#2091)] "Cisco ASA Security Appliance Series deliver robust user and application policy enforcement, multi-vector attack protection, and secure connectivity services in cost-effective, easy-to-deploy solutions. The ASA 5500 Series Adaptive Security Appliances provide comprehensive security, performance, and reliability for network environment."
335	whiteCryption Corporation 920 Stewart Drive Suite #100 Sunnyvale, CA 94085 USA -Alex Bessonov TEL: 408-616-1647	**whiteCryption SKB - DrbgSha256** **Version 4.6.0**	Nvidia Tegra 4 w/ Android 4.2	5/24/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2089)] "WhiteCryption Secure Key Box (SKB) is a C/C++ library that provides cryptographic algorithms. SKB's unique white-box implementation is specifically designed to hide and protect cryptographic keys at all times. It allows safe deployment in insecure environments."
334	Toshiba Corporation 1-1, Shibaura 1-chome Minato-ku, Tokyo 105-8001 Japan -Hiroshi Ito TEL: +81-45-776-5624 FAX: +81-45-776-4104	**Toshiba Secure Cryptographic Suite for Mobile HDD** **Version FN001S (Firmware)**	Cortex-R4	5/24/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256) (SHS Val#2081)] "A library of unique software and hardware cipher solutions which are standard encryption algorithm-based to provide Toshiba mobile HDD products and the systems using them a robust and secure data storage environment." *04/24/14: Updated vendor information;*
333	McAfee Inc. 2821 Mission College Blvd.	**RSA Bsafe Crypto-J**	Intel Xeon w/ McAfee Linux 2.2 running on VMware ESXi 5.0	5/24/2013	**Dual_EC_DRBG**:[Prediction Resistance Tested:

	Santa Clara, CA 95054 USA -Mark Hanson TEL: +1 651 628 1633 FAX: +1 651 628 2706	**Version 4.1**			Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (ECDSA Val#401) (SHS Val#2079) "McAfee Firewall Enterprise Control Center simplifies the management of multiple McAfee Firewall Enterprise appliances. Control Center enables centralized management and monitoring of the McAfee Firewall Enterprise solutions, allowing network administrators to centrally define firewall policy, deploy updates and inventory their firewall products."
332	Cisco Systems Inc. 170 West Tasman Dr. San Jose, CA 95134 USA -Global Certification Team	**Adaptive Security Appliance Onboard Acceleration** **Part # CN1620-400BG233-P-G**	N/A	5/24/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1794)] "Cisco ASA Security Appliance Series deliver robust user and application policy enforcement, multi-vector attack protection, and secure connectivity services in cost-effective, easy-to-deploy solutions. The ASA 5500 Series Adaptive Security Appliances provide comprehensive security, performance, and reliability for network environment."
331	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Windows 64-bit x86-64 for 64 bits** **Version 8.2.2.0**	Intel Core i7-2600 with AES-NI w/ Microsoft Windows Server 2008 64-bit	5/24/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2172)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2172)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
330	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Windows 64-bit x86-64 for 32 bits** **Version 8.2.2.0**	Intel Core i7-2600 with AES-NI w/ Microsoft Windows Server 2008 64-bit	5/24/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2171)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2171)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
329	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL zSeries-64 for 64 bits** **Version 8.2.2.0**	IBM zSeries z196 64-bit with CPACF hardware support w/ Red Hat Enterprise Linux Server 5	5/24/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1905)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2214)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2214)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
328	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL zSeries-64 for 32 bits** **Version 8.2.2.0**	IBM zSeries z196 64-bit with CPACF hardware support w/ Red Hat Enterprise Linux Server 5	5/24/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1904)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2213)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2213)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
327	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia	**ICC Algorithmic Core on RHEL x86-64 for 64 bits** **Version 8.2.2.0**	Intel Core i7-2600 with AES-NI w/ Red Hat Enterprise Linux Server 5	5/24/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2164)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2164)]

	-Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420				"ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
326	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL x86-64 for 32 bits** **Version 8.2.2.0**	Intel Core i7-2600 with AES-NI w/ Red Hat Enterprise Linux Server 5	5/24/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2163)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2163)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
325	Juniper Networks Inc 1194 N. Mathilda Ave Sunnyvale, CA 94089 USA -Sharath Sridhar TEL: +91 80 30538736 FAX: +91 80 30538824	**SSH_IPSEC** **Version Junos 12.1R6.6 (Firmware)**	PowerPC, Freescale's PowerQUICC III Processor Family; ARM v5, Marvell's Feroceon processor Family	5/24/2013	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-256) (HMAC Val#1505)] "Comprehensive, scalable switching solutions specifically designed to meet the needs of both enterprises and service providers. All of our switches - modular and fixed platforms - run on one common operating system- Junos." *06/10/13: Updated implementation information;*
324	Juniper Networks Inc 1194 N. Mathilda Ave Sunnyvale, CA 94089 USA -Sharath Sridhar TEL: +91 80 30538736 FAX: +91 80 30538824	**QuickSec** **Version Junos 12.1R6.6 (Firmware)**	PowerPC, Freescale's PowerQUICC III Processor Family; ARM v5, Marvell's Feroceon processor Family	5/24/2013	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1504)] "Comprehensive, scalable switching solutions specifically designed to meet the needs of both enterprises and service providers. All of our switches - modular and fixed platforms - run on one common operating system- Junos." *06/10/13: Updated implementation information;*
323	Aviat Networks 5200 Great America Parkway Santa Clara, California 95054 USA Ruth French TEL: +44 1698 717200	**Secure Management** **Version 7.7 (Firmware)**	Motorola MPC866	5/10/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256) (SHS Val#2075)] "Eclipse Intelligent Node Unit (INUe). The module provides data security by encrypting the payload traffic on the microwave link between up to three radios. It also provides the Strong Encryption Suite for secure module management and uses AES encryption to secure SNMP v3 management traffic."
322	Oracle America, Inc. 500 Oracle Parkway Redwood City, CA 94065 United States -Linda Gallops TEL: 704-972-5018 FAX: 704-321-9273	**T10000C CTR DRBG** **Version 2.1 (Firmware)**	ARM 962EJS	5/10/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2407)] "The Oracle StorageTek T10000C Tape Drive blends the highest capacity, performance, reliability, and data security to support demanding, 24/7 data center operations. It delivers the world's fastest write speeds to a native 5 TB of magnetic tape storage; making it ideal for data center operations with growing data volume."
321	Samsung Electronics Co., Ltd R4 416, Maetan 3-dong, Yeongtong-gu Suwon-si, Gyeonggi-do 443-742 Korea -Kyung-Hee Lee TEL: +82-10-9397-1589	**Samsung OpenSSL Cryptographic Module** **Version SecOpenSSL2.0.3**	ARMv7 w/ Android Jelly Bean 4.2	5/10/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2069)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1496)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2411)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2411)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#396) (SHS Val#2069) "General purpose cryptographic services available for Android used by Samsung devices to provide secure cryptography. Salt length 0, 1 and 2 has been tested for RSASSA-PSS." *01/16/14: Updated implementation information;*

320	Authora Inc. 1319 Dexter Ave. N., Suite 010 Seattle, WA 98109 USA -Tia Walker TEL: 206.783.8000 FAX: 206.217.0623	**Authora Cryptographic Algorithm Implementation** **Version 1.0**	Intel Core w/ Windows Server 2008	5/10/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2068)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1495)] "Authora Cryptographic Algorithm Implementation implements advanced cryptographic algorithms, including symmetric and asymmetric cryptography, as well as key generation and random number generation. It is used by a family of Authora products including Authora Edge and Zendit."
319	N/A	**N/A**	N/A	5/10/2013	N/A
318	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -John Bordwine TEL: 703-885-3854	**Symantec DLP Crypto Engine** **Version 1.0**	Intel i5 w/ Microsoft Windows 7 32-bit; Intel i5 w/ Microsoft Windows Server 2008 R2 64-bit; Intel i5 w/ Apple Mac OS X 10.7 64-bit; Intel i5 w/ Apple Mac OS X 10.7 32-bit	4/30/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2060)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1490)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2397)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2397)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#395) (SHS Val#2060) "Cryptographic engine for Symantec DLP"
317	Motorola Solutions, Inc. 6480 Via Del Oro San Jose, CA 95119 USA -Ashot Andreasyan TEL: 408-826-3203 FAX: 408-528-2883	**Open SSL Crypto library-DRBG** **Version v1_0_1_0 (Firmware)**	Free Scale MPC-7457; Free Scale MPC-8568E	4/30/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2057)] "The 1.0.1c crypto library is used for protecting security parameters and key exchange protocol messages; authenticating a user; generating cryptographic and key encryption keys in GGM8000 and s6000 transport gateways." *08/27/13: Updated implementation information;*
316	OpenSSL Software Foundation Inc. 1829 Mount Ephraim Road Adamstown, MD 27101 USA -Steve Marquess TEL: 877-673-6775	**OpenSSL FIPS Object Module** **Version 2.0.4**	MIPS 24Kc w/ OpenWRT 2.6	4/30/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2056)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1485)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2394)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2394)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#394) (SHS Val#2056) "The OpenSSL FIPS Object Module is a full featured general purpose cryptographic library that is distributed in source code form under an open source license. It can be downloaded from www.openssl.org/source."
315	Juniper Networks, Inc. 1194 N. Mathilda Ave. Sunnyvale, CA 94089 USA -Tim Huntley	**JUNOS 12.1 X44 for SRX Series Platforms, Routing Engine** **Version 12.1**	Cavium Octeon CN5020 w/ JUNOS 12.1X44-D15.5-Domestic (SRX100); Cavium Octeon CN5020 w/ JUNOS 12.1X44-D15.5-FIPS (SRX100); Cavium Octeon CN5230 w/ JUNOS 12.1X44-D15.5-Domestic (SRX240); Cavium Octeon CN5230 w/ JUNOS 12.1X44-D15.5-FIPS (SRX240); Cavium Octeon CN6335 w/JUNOS 12.1X44- D15.5-Domestic (SRX550); Cavium Octeon CN6335 w/ JUNOS 12.1X44- D15.5-FIPS (SRX550); Cavium Octeon CN5645 w/ JUNOS 12.1X44- D15.5-Domestic (SRX650); Cavium Octeon CN5645 w/	4/30/2013	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256) (HMAC Val#1482)] "Juniper Networks, Inc. JUNOS 12.1 X44 for SRX Series Platforms supports the definition of and enforces information flow policies among network nodes. The routers provide for stateful inspection of every packet that traverses the network and provide central management to manage the network security policy." *09/10/13: Updated implementation information;*

			JUNOS 12.1X44- D15.5-FIPS (SRX650); Motorola MPC8544E, PowerQUIC III Processor w/ JUNOS 12.1X44- D15.5-Domestic (SRX1400); Motorola MPC8544E, PowerQUIC III Processor w/ JUNOS 12.1X44- D15.5-FIPS (SRX1400); Intel 1.3GHz CPU Celeron M w/ JUNOS 12.1X44- D15.5-Domestic (SRX5000 with SPC-2); Intel 1.3GHz CPU Celeron M w/ JUNOS 12.1X44- D15.5-FIPS (SRX5000 with SPC-2); Intel 1.3GHz CPU Celeron M w/ JUNOS 12.1X44- D15.5-Domestic (SRX5000 with SPC-4); Intel 1.3GHz CPU Celeron M w/ JUNOS 12.1X44- D15.5-FIPS (SRX5000 with SPC-4);		
314	IBM 9032 South Rita Road Tucson, AZ 85744 USA -Christine Knibloe TEL: (520) 799-2486	**TS1140 Cryptographic Firmware Library** **Version P/N: 35P2401 (Firmware)**	PPC 405	4/23/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#2051)] "Firmware cryptographic implementation that adds secure key channel capabilities to the IBM TS1140."
313	CoCo Communications 800 5th Ave Seattle, WA 98104 USA -David Weidenkopf TEL: 206-812-5783	**CoCo OpenSSL AES-NI Algorithms for Intel x86** **Version 2.1**	x86 32-bit with AES-NI w/ Vyatta 6.4	4/23/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2381)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2381)] "The CoCo OpenSSL Crypto Module is an OpenSSL cryptographic library that provides cryptographic services to its calling applications." *03/31/014: Updated implementation information;*
312	Lexmark International Inc. 740 West New Circle Road Lexington, KY 40550 USA -Graydon Dodson TEL: (859) 232-6483	**Crypto Module (user)** **Version 2.10**	Marvell 88PA6170C1 (ARMv7 dual core) w/ Lexmark Linux v3.0.0	4/23/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2049)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1479)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2379)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2379)] "The Crypto Module (user/kernel) provides cryptographic services to the firmware in Lexmark products."
311	Hewlett–Packard Development Company L.P. 3000 Hanover Street Palo Alto, CA 94304-1185 USA -Mihai Damian TEL: 1-650-236-5870 -Sameer Popli TEL: 1-650-236-5874	**HP NSVLE C API Library** **Version 0.3**	Intel(R) Xeon(R) E5-2658 w/ Debian Linux HPTE Version 5.0.0	4/5/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2375)] "Hewlett-Packard's NonStop platform is used in complex computing environments, where business-critical applications need 24 x 7 availability, extreme scalability, and fault-tolerance. NonStop plays an important role in major industries and markets, including finance, healthcare, telecommunications, manufacturing, retail, and government."
310	Riverbed Technology Inc. 199 Fremont Street San Francisco, CA 94105 USA -Joe Tomasello TEL: 415-344-5756 -Andy Pang TEL: 415-247-7341	**Riverbed Cryptographic Security Module** **Version 1.0**	Intel Xeon (x86-64) w/ RiOS 8.0 32-bit; Intel Xeon (x86-64) w/ RiOS 8.0 64-bit; Intel Xeon E3-1220v2 (x86_64) w/ RiOS 8.0 64-bit running on VMware ESXi 5.1; Intel Xeon E3-1220v2 (x86_64) w/ AES-NI w/ RiOS 8.0 64-bit running on VMware ESXi 5.1; Intel Xeon E3-1220v2 (x86_64) w/ Stingray OS 4.0 running on VMware ESXi 5.1; Intel Xeon E3-1220v2 (x86_64) w/ AES-NI w/ Stingray OS 4.0 running on VMware ESXi 5.1; Intel Xeon E31220 (x86_64) w/ AES-NI w/ RiOS 8.0 64-bit; AMD Opteron 4122 (x86_64) w/ Granite OS 2.0; Intel Xeon E31220 (x86_64) w/ Granite OS 2.0 on VMware ESXi 5.1; Intel Xeon E31220 (x86_64) w /AES-NI w/ Granite OS 2.0 on VMware ESXi 5.1; Intel Xeon E5620 w/ Whitewater OS 3.0; Intel Xeon E5620 with AES-NI w/ Whit; ewater OS 3.0; Intel Xeon E31220 (x86) w/ Whitewater OS 3.0 under VMware ESXi 5.1; Intel Xeon E31220 (x86) with AES-NI w/ Whitewater OS 3.0 under VMware ESXi 5.1; AMD Opteron 2376 w/ Interceptor OS 4.5 ; Intel Xeon E31220 w/ RiOS 8.6 32-bit; Intel Xeon E31220 w/ RiOS 8.6 64-bit; Intel Xeon E5-2430L w/	4/12/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2049)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1479)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2379)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#392) (SHS Val#2049) "The Riverbed Cryptographic Security Module provides the cryptographic functionality for a variety of Riverbed's platforms including Steelhead and Granite appliances. These network appliances deliver a scalable Wide Area Data Services (WDS) solution, transparently and securely optimizing performance across an enterprise network." *08/28/13: Added new tested information;* *12/13/13: Added new tested information;*

			RiOS 8.6 64-bit under VMware ESXi 5.1; Intel Xeon E5-2430L with AES-NI w/ RiOS 8.6 64-bit under VMware ESXi 5.1; Intel Xeon E31220 with AES-NI w/ RiOS 8.6 64-bit; Intel Xeon w/ Steelhead Mobile Controller 4.6; Intel Xeon with AES-NI w/ Steelhead Mobile Controller 4.6; Intel Xeon E5-2430L w/ Steelhead Mobile Controller 4.6 under VMware ESXi 5.1; Intel Xeon E5-2430L with AES-NI w/ Steelhead Mobile Controller 4.6 under VMware ESXi 5.1		*09/10/14: Added new tested information; 09/17/14: Added new tested information;*
309	Cummings Engineering Consultants Inc. 145 S. 79th St., Suite 26 Chandler, AZ 85226 USA -Darren Cummings TEL: 480-809-6024	**Cummings Engineering's Secure Mobility Suite B Crypto Module** **Version 1.1**	ARM Cortex A8 (ARMv7) w/ Apple iOS 5.0; Intel Core i7-3615QM w/ Apple OS X 10.7	4/5/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2045)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1475)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2373)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2373)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#391) (SHS Val#2045) "The cryptographic module used by the Cummings Engineering suite of products which allow for efficient and effective deployment of robust secure communications capability on commercial off the shelf (COTS) devices, such as Smartphones and Tablets, as well as speciality communications devices."
308	SAP AG Albert-Einstein-Allee 3 Bensheim, NRW 64625 Germany -Stephan André TEL: +49-6251-708-1730 FAX: +49-6227-78-55975 -Thomas Rothe TEL: +49-6251-708-2339 FAX: +49-6227-78-55989	**SAP NW SSO 2.0 Secure Login Library Crypto Kernel** **Version 2.0.0.1.32 32/64-bit**	Intel Xeon w/ Mac OS X 10.7 64-bit	4/5/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2372)] "SAP NW SSO 2.0 Secure Login Library Crypto Kernel v2.0.0.1.32 is a shared library, i.e. it consists of software only. SAP NW SSO 2.0 Secure Login Library Crypto Kernel provides an API in terms of C++ methods for key management and operation of cryptographic functions."
307	SAP AG Albert-Einstein-Allee 3 Bensheim, NRW 64625 Germany -Stephan André TEL: +49-6251-708-1730 FAX: +49-6227-78-55975 -Thomas Rothe TEL: +49-6251-708-2339 FAX: +49-6227-78-55989	**SAP NW SSO 2.0 Secure Login Library Crypto Kernel** **Version 2.0.0.1.32 64-bit**	Intel Xeon with AES-NI w/ Linux 2.6.32; AMD Opteron w/ Linux 2.6.32; IBM POWER7 (PowerPC) w/ Linux 2.6.32 on hypervisor VMware ESX 5.0.0; AMD Opteron w/ Linux 2.6.16; IBM S/390 (2817) w/ Linux 2.6.5 on hypervisor VMware ESX 4.1.0; IBM POWER6 (PowerPC) w/ Linux 2.6.16 on hypervisor VMware ESX 4.1.0; AMD Opteron w/ Linux 2.6.5; IBM S/390 (2817) w/ Linux 2.6.5 on hypervisor VMware ESX 4.1.0; IBM POWER5 (PowerPC) w/ Linux 2.6.5 on hypervisor VMware ESX 5.0.0; Intel Itanium 2 w/ Linux 2.6.5; Intel Itanium 2 w/ Linux 2.4.19; Intel Xeon w/ Solaris 5.10 64-bit; SPARC64 V w/ Solaris 5.10 64-bit; UltraSPARC III+ w/ Solaris 5.9 64-bit; SPARC64 III w/ Solaris 5.8 64-bit; Alpha 21264B (EV6) w/ True64 Unix 5.1; Intel Xeon w/ Mac OS X 10.7 64-bit; Intel Core i5 with AES-NI w/ Windows 7 Enterprise SP1 64-bit; AMD Opteron w/ Windows Server 2008 R2 on hypervisor VMware ESX 4.1.0; HP 9000/800/rp3440 (PA-RISC2.0) w/ HP-UX 11.31 64-bit; Intel Itanium 2 w/ HP-UX 11.31 64-bit; Intel Itanium 2 w/ HP-UX 11.23 64-bit; HP 9000/800/L3000-7x (PA-RISC2.0) w/ HP-UX 11.11 64-bit; HP 9000/800/L3000-5x (PA-RISC2.0) w/ HP-UX 11.00 64-bit; IBM POWER7 (PowerPC) w/ AIX 6.1 64-bit on hypervisor VMware ESX 4.1.0; IBM POWER4 (PowerPC) w/ AIX 5.2 64-bit; IBM POWER4 (PowerPC) w/ AIX 5.1 64-bit	4/5/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2371)] "SAP NW SSO 2.0 Secure Login Library Crypto Kernel v2.0.0.1.32 is a shared library, i.e. it consists of software only. SAP NW SSO 2.0 Secure Login Library Crypto Kernel provides an API in terms of C++ methods for key management and operation of cryptographic functions."
306	SAP AG Albert-Einstein-Allee 3 Bensheim, NRW 64625 Germany -Stephan André TEL: +49-6251-708-1730	**SAP NW SSO 2.0 Secure Login Library Crypto Kernel** **Version 2.0.0.1.32 32-bit**	Intel Pentium III w/ Linux 2.6.27 on hypervisor VMware ESX 4.1.0; Intel Xeon with AES-NI w/ Linux 2.6.32; Intel Pentium III w/ Linux 2.6.5; Intel Xeon w/ Linux 2.4.21; Intel Xeon w/ Linux 2.4.18; Intel Xeon w/ Solaris 5.10 64-bit;	4/5/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2370)] "SAP NW SSO 2.0 Secure Login Library Crypto Kernel v2.0.0.1.32 is a shared library, i.e. it consists of software only. SAP NW SSO 2.0 Secure

	FAX: +49-6227-78-55975 -Thomas Rothe TEL: +49-6251-708-2339 FAX: +49-6227-78-55989		SPARC64 V w/ Solaris 5.10 64-bit; UltraSPARC III+ w/ Solaris 5.9 64-bit; SPARC64 III w/ Solaris 5.8 64-bit; Intel Xeon w/ Mac OS X 10.7 64-bit; Intel Core i5 with AES-NI w/ Windows 7 Enterprise SP1 64-bit; AMD Opteron w/ Windows Server 2008 R2 on hypervisor VMware ESX 4.1.0; HP 9000/800/rp3440 (PA-RISC2.0) w/ HP-UX 11.31 64-bit; HP 9000/800/L3000-7x (PA-RISC2.0) w/ HP-UX 11.11 64-bit; HP 9000/800/L3000-5x (PA-RISC2.0) w/ HP-UX 11.00 64-bit; IBM POWER7 (PowerPC) w/ AIX 6.1 64-bit on hypervisor VMware ESX 4.1.0; IBM POWER4 (PowerPC) w/ AIX 5.2 64-bit; IBM POWER4 (PowerPC) w/ AIX 5.1 64-bit		Login Library Crypto Kernel provides an API in terms of C++ methods for key management and operation of cryptographic functions."
305	CoCo Communications 800 5th Ave Seattle, WA 98104 USA -David Weidenkopf TEL: 206-812-5783	**CoCo OpenSSL Algorithms for Intel x86** **Version 2.1**	x86 32bit w/ Vyatta 6.4	4/5/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2040)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1471)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2367)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2367)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#390) (SHS Val#2040) "The CoCo OpenSSL Crypto Module is an OpenSSL cryptographic library that provides cryptographic services to its calling applications." *03/31/14: Updated implementation information;*
304	CoCo Communications 800 5th Ave Seattle, WA 98104 USA -David Weidenkopf TEL: 206-812-5783	**CoCo OpenSSL Algorithms for AMD Geode** **Version 2.1**	AMD Geode 32bit w/ Red Hat Enterprise Linux 6	4/5/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2039)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1470)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2366)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2366)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#389) (SHS Val#2039) "The CoCo OpenSSL Crypto Module is an OpenSSL cryptographic library that provides cryptographic services to its calling applications." *04/30/13: Updated implementation information;* *03/31/14: Updated implementation information;*
303	CipherCloud Inc. 99 Almaden Blvd., Suite 720 San Jose, CA 95113 USA -Varun Badhwar TEL: 1 (415) 683-0062	**Cryptographic Module for CipherCloud Gateway** **Version 1.0**	Intel Xeon E5645 w/ CentOS 6.3 with Java JRE 1.6.0	3/29/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2339)] "The CipherCloud Encryption gateway provides FIPS approved cryptographic algorithms to protect sensitive data stored in public cloud environments, while preserving advanced operations such as searching, sorting and reporting." *08/02/13: Updated implementation information;*
302	HGST Inc. 5601 Great Oaks Parkway San Jose, California 95119 US -Rajesh Kukreja TEL: 408-717-6261 FAX: 408-717-9494 -Jithendra Bethur TEL: 408-717-5951 FAX: 408-717-9494	**TcgCryptoLib** **Version SOCFWLIB-0015 (Firmware)**	ARM Cortex R4	3/29/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2365)] "HGST SEDs implement TCG Storage specifications. They satisfy the performance & security requirements of demanding enterprise applications. Embedded FIPS 140-2 modules have hardware encryption, cryptographic erase, independently authorized data bands and authenticated, protected FW download."

					10/21/13: Updated the implementation with new test;
301	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101 -Sunil Chitnis TEL: 408-333-2444 FAX: 408-333-4887	**FIPS 140-2 Certification for Brocade® MLXe® and CER 2000 Series** **Version BRCD-IP-CRYPTO-VER-2.0 (Firmware)**	Freescale MPC 7448, RISC, 1700 MHZ; Freescale MPC 7447, RISC, 1000 MHZ; Freescale MPC 8544, PowerQUICC III, 800 MHZ	3/22/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2031)] "The Brocade cryptographic library implements crypto operations in software. The Brocade MLX Series is highly optimized for IP Ethernet deployments, providing symmetric scaling and industry-leading wire-speed port capacity without compromising the performance of advanced capabilities such as IPv6, MPLS, and MPLS Virtual Private Networks (VPNs)."
300	Feitian Technologies Co. Ltd Floor 17, Tower B, Huizhi Mansion, No.9 Xueqing Road Haidian, Beijing 100085 China -Tibi TEL: (+86)010-62304466-821 FAX: (+86)010-62304477 -PENG Jie TEL: (+86)010-62304466-419 FAX: (+86)010-62304477	**FEITIAN-FIPS-Cryptographic Library V1.0.0** **Version 1.0.0 (Firmware)** **Part # SLE78CLFX4000PM**	Infineon SLE78CLFX4000PM	3/22/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128)] "FEITIAN-FIPS-Cryptographic Library V1.0.0 implements AES, TDES, CMAC, TDES MAC, SHA1, SHA256, SHA512, DRBG, RSA, and KDF, and operates on Infineon SLE78CLFX4000PM for FEITIAN-FIPS-JCOS V1.0.0, which is smart card complied with Java Card 2.2.2 and Global Platform 2.2.1." *03/29/13: Updated implementation information; 02/05/15: Updated vendor information;*
299	Samsung Electronics Co., Ltd R4 416, Maetan 3-dong, Yeongtong-gu Suwon-si, Gyeonggi-do 443-742 Korea -Ross Choi TEL: 972-761-7628 -Kyung-Hee Lee TEL: +82-10-6640-8499	**Samsung OpenSSL Cryptographic Module** **Version SecOpenSSL2.0.3**	ARMv7 w/ Android Jelly Bean 4.1	3/8/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2026)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1458)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2351)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2351)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#386) (SHS Val#2026) "General purpose cryptographic services available for Android used by Samsung devices to provide secure cryptography. Salt length 0, 1 and 2 has been tested for RSASSA-PSS." *01/16/14: Updated implementation information;*
298	Haivision Inc. 4445 Garand Montreal, Quebec H4R 2H9 Canada -Jean Dube TEL: 514-334-5445 x8263	**Haivision Crypto Module** **Version 2.1.1**	ARM v5TEJ w/ Linux 2.6	2/26/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2349)] "OpenSSL FIPS Object Module 2.0 (CMVP Cert. #1747)"
297	GoldKey Security Corporation 26900 E. Pink Hill Rd Independence, MO 64057 USA -GoldKey Sales & Customer Service TEL: (816) 220-3000 -Jon Thomas TEL: 567-270-3830	**GoldKey Cryptographic Algorithms** **Version 7.13 (Firmware)**	Arca2S	2/21/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-256) (AES Val#2347)] "Cryptographic algorithm implementation for GoldKey Products" *03/18/13: Updated implementation information; 03/27/13: Updated implementation information; 10/25/13: Updated implementation information; 07/23/14: Updated implementation informaiton;*
296	Cavium Inc. 2315 N. First Street San Jose, CA 95131 USA -Tasha Castaneda TEL: 1-408-943-7100 -YJ Kim TEL: 1-408-943-7100	**OCTEON II CN6700/CN6800 Series Die** **Part # CN6740/ CN6750/ CN6760/ CN6860/ CN6870/ CN6880, -SCP and -AAP options Version #-Y22**	N/A	2/21/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2346)] "The Octeon II CN 6XXX family of multi-core MIPS64 processors targets datacenter, routers, switches, control plane, base stations, and UTM applications. Part numbers: CN6010 CN6020 CN6120 CN6130 CN6220 CN6230 CN6330 CN6335 CN6630 CN6635 CN6640 CN6645 CN6740 CN6750 CN6760 CN6860 CN6870 CN6880, all with -SCP and -AAP options."
295	Cavium Inc.	**OCTEON II CN6600 Series Die**	N/A	2/21/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not

	2315 N. First Street San Jose, CA 95131 USA -Tasha Castaneda TEL: 1-408-943-7100 -YJ Kim TEL: 1-408-943-7100	**Part # CN6630/ CN6635/ CN6640/ CN6645, -SCP and -AAP options Version # -Y**			Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2345)] "The Octeon II CN 6XXX family of multi-core MIPS64 processors targets datacenter, routers, switches, control plane, base stations, and UTM applications. Part numbers: CN6010 CN6020 CN6120 CN6130 CN6220 CN6230 CN6330 CN6335 CN6630 CN6635 CN6640 CN6645 CN6740 CN6750 CN6760 CN6860 CN6870 CN6880, all with -SCP and -AAP options."
294	Cavium Inc. 2315 N. First Street San Jose, CA 95131 USA -Tasha Castaneda TEL: 1-408-943-7100 -YJ Kim TEL: 1-408-943-7100	**OCTEON II CN6000/CN6100 Series Die** **Part # CN6010/ CN6020/ CN6120/ CN6130, -SCP and -AAP options**	N/A	2/21/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2344)] "The Octeon II CN 6XXX family of multi-core MIPS64 processors targets datacenter, routers, switches, control plane, base stations, and UTM applications. Part numbers: CN6010 CN6020 CN6120 CN6130 CN6220 CN6230 CN6330 CN6335 CN6630 CN6635 CN6640 CN6645 CN6740 CN6750 CN6760 CN6860 CN6870 CN6880, all with -SCP and -AAP options."
293	Cavium Inc. 2315 N. First Street San Jose, CA 95131 USA -Tasha Castaneda TEL: 1-408-943-7100 -YJ Kim TEL: 1-408-943-7100	**OCTEON II CN6200/ CN6300 Series Die** **Part # CN6220/ CN6230/ CN6330/ CN6335, -SCP and -AAP options Version # -Y**	N/A	2/19/2013	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2343)] "The Octeon II CN 6XXX family of multi-core MIPS64 processors targets datacenter, routers, switches, control plane, base stations, and UTM applications. Part numbers: CN6010 CN6020 CN6120 CN6130 CN6220 CN6230 CN6330 CN6335 CN6630 CN6635 CN6640 CN6645 CN6740 CN6750 CN6760 CN6860 CN6870 CN6880, all with -SCP and -AAP options."
292	OpenSSL Software Foundation Inc. 1829 Mount Ephraim Road Adamstown, MD 27101 USA -Steve Marquess TEL: 877-673-6775	**OpenSSL FIPS Object Module** **Version 2.0.3**	Freescale i.MX53xA (ARMv7) with NEON w/ Windows Embedded Compact 7; Freescale i.MX53xD (ARMv7) with NEON w/ Windows Embedded Compact 7; Qualcomm Snapdragon APQ8060 (ARMv7) with NEON w/ Android 4.0	2/19/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2019)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1451)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2342)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2342)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#383) (SHS Val#2019) "The OpenSSL FIPS Object Module is a full featured general purpose cryptographic library that is distributed in source code form under an open source license. It can be downloaded from www.openssl.org/source/." *02/21/13: Added new tested information;* *02/26/13: Updated implementation information* *04/10/13: Added new tested information;* *04/24/13: Updated implementation information;*
291	Advance Computing and Engineering Solutions. (ACES) H. No. 156, St 5, F11-1 Islamabad, n/a 44000 Pakistan -Dr. Mehreen Afzal TEL: +923009878534 FAX: +92-51-2224453 -Dr. Mureed Hussain TEL: +923238556816 FAX: +92-51-2224453	**Tahir Pak Crypto Library** **Version 2.1.1**	DELL PowerEdge T110 II 11th Generation Server w/ RHEL 5.3 evaluated at EAL4+	2/19/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2341)] "TPCL (Tahir Pak Crypto Library) provides FIPS approved Cryptographic functions to consuming applications via an Application Programming Interface (API)." *03/12/13: Updated implementation information;*
290	Kony, Inc. 7380 West Sand Lake Rd. #390 Orlando, FL 32819 USA -Matthew Terry TEL: 407-730-5669 FAX: 407-404-3738	**Kony Cryptographic Library** **Version 2.0**	Qualcomm QSD 8250 (ARMv7) w/ Android 2.2; Qualcomm QSD 8250 (ARMv7) with NEON w/ Android 2.2; TI OMAP 3621 (ARMv7) w/ Android 3.0; TI OMAP 3621 (ARMv7) with NEON w/ Android 3.0; TI DM3730 (ARMv7) w/ Android 4.0; TI DM3730 (ARMv7) with NEON w/ Android 4.0; ARM Cortex-A8 (ARMv7) with NEON w/ Apple iOS 5.0; ARMv7 Cortex-A8 (ARMv7) with NEON w/ Apple iOS 6.0; ARM Cortex-A8 (ARMv7) without NEON w/	2/19/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#2016)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1448)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2338)]

			Apple iOS 5.0; ARM Cortex-A8 (ARMv7) without NEON w/ Apple iOS 6.0		BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2338)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#382) (SHS Val#2016) "The Kony Cryptographic Library v2.0 is a full featured cryptographic module used in Kony mobile and multi-channel application platforms and the KonyOne Platform." *08/09/13: Added new tested information; 08/27/13: Updated implementation information; 08/30/13: Updated vendor information;*
289	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Palani Karuppan TEL: 408-525-2747 -Muukund Chikerali	**DRBG** **Version CTR-DRBG-7.0.0 (Firmware)** **Part # Cavium Octeon Plus 5600 family**	Cavium Octeon Plus 5600 Family	1/31/2013	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2330)] "The SP800-90 DRBG is implemented internally within Cisco. It is a CTR DRBG using AES256 as the block cipher. The crypto provider (for AES256) is OpenSSL0 0.9.8g-7.0.0 and the entropy provider is the hardware RNG on the Cavium Octeon Plus 5600 family data plane processor." *02/07/13: Updated vendor information;*
288	Lancope Inc. 3650 Brookside Parkway, Suite 400 Alpharetta, GA 30022 USA -Jim Magers	**Lancope Crypto-J library** **Version 1.0**	Intel Xeon E5 series w/ Stealthwatch v6.3; Intel Xeon E3 series w/ Stealthwatch v6.3	1/25/2013	**Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1) (ECDSA Val#380) "The Lancope Crypto-J library relies on the RSA BSAFE Crypto-J module to protect sensitive data as it is stored using encryption techniques to provide a persistent level of protection. The library provides encrypted management and internal communications for Lancope's Stealthwatch products."
287	Cleversafe Inc. 222 South Riverside Plaza Suite 1700 Chicago, Illinois 60606 US -Brenda Litin TEL: (312) 423-6640 -Jason Resch TEL: (312) 423-6640	**Cleversafe Dispersed Storage Access Framework SDK** **Version dsaf-sdk-2.2.12370**	Intel Xeon w/ Ubuntu 10	1/18/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256 , SHA-512) (SHS Val#1998)] "This package contains the Dispersed Storage Access Framework (DSAF) Software Development Kit (SDK). It contains all of the documentation and libraries required to build applications that can store to and retrieve data from a simple object vault on a dsNet(TM) System."
286	Allegro Software Development Corporation 1740 Massachusetts Avenue Boxborough, MA 01719 USA -Larry LaCasse TEL: +1 (978) 264-6600	**Allegro Cryptographic Engine** **Version 1.1**	Intel Core 2 Duo w/ Windows 7 Ultimate (64-bit)	1/18/2013	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1997)] "The Allegro Cryptographic Engine (ACE) is a cryptographic library module for embedded computing systems. ACE provides software implementations of algorithms for calculations of message digests, digital signature creation and verification, bulk encryption and decryption, key generation and key exchange"
285	Uplogix Inc. 7600 B North Capital of Texas Highway Suite 220 Austin, TX 78731 USA -Martta Howard TEL: 512-857-7043 FAX: 512-857-7002	**NSS** **Version 3.12.11 (Firmware)**	AMD Geode LX; Intel Celeron D; Intel Atom E6xx	12/21/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1976)] "Uplogix Local Managers utilize Mozilla's Network Security Services for general purpose cryptographic functionality. NSS provides the algorithms necessary to secure Uplogix' SSH and TLS implementations. See http://www.uplogix.com"
284	Mocana Corporation 710 Sansome Street San Francisco, CA 94104 USA -Mocana Sales TEL: 415-617-0055 FAX: 415-617-0056	**Mocana Cryptographic Library** **Version 5.5fi**	FreeScale QorIQ P2 w/ VxWorks 6.8	12/21/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#372) (SHS Val#1974) "The Mocana Cryptographic Loadable Kernel Module (Software Version 5.5fi) is a hybrid, multi-chip standalone cryptographic module that runs on a general purpose computer. The primary purpose of this module is to provide FIPS

					Approved cryptographic routines to consuming applications via an Application Programming Interface."
283	SafeNet Inc. 4690 Millennium Drive Belcamp, MD 21017 USA -Chris Brych TEL: 613-221-5081 FAX: 613-723-5079	**SafeNet Software Cryptographic Library** **Version 1.0**	Intel Xeon E3-1220v2 w/ AES-NI w/ Windows Server 2008R2 64-bit; Intel Xeon E3-1220v2 w/ Windows Server 2008 64-bit; Intel Core i5-2430M w/ AES-NI w/ Windows 7 64-bit; Intel Core i5-2430M w/ Windows 7 32-bit; Intel Xeon E3-1220v2 w/ AES-NI w/ NetBSD 4.1 32-bit on VMware ESX; ARMv7 w/ NEON w/ Android 4.0; Intel Xeon E3-1220v2 w/ AES-NI w/ RHEL 6.2 64-bit; Intel Xeon 3050 w/ CentOS 5.6 32-bit	12/7/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1967)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1402)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2286)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#370) (SHS Val#1967) "The SafeNet Software Cryptographic Library is SafeNet's cryptographic service provider that provides extended high performance cryptographic services for SafeNet's broad range of Data Protection products."
282	N/A	**N/A**	N/A	11/21/2012	N/A
281	SafeLogic Inc 530 Lytton Ave, Ste 200 Palo Alto, CA 94301 USA -SafeLogic Inside Sales	**CryptoComply Server Engine** **Version 2.1**	Intel i7 w/ CentOS 6.3; Intel i7 w/ Mac OS X 10.8; Intel i7 w/ RHEL 6.3; Intel i7 w/ SUSE Linux Enterprise 11 SP2; Intel i7 w/ Windows 2008 R2; PowerPC P2020 w/ CentOS 6.3;	11/21/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1954)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1391)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2273)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2273)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#368) (SHS Val#1954) "CryptoComply | Server is a standards-based "Drop-in Compliance" solution for servers and appliances. The module features robust algorithm support, including Suite B algorithm compliance. CryptoComply offloads secure key management, data integrity, data at rest encryption, and secure communications to a trusted implementation." *01/16/14: Added new tested information;*
280	Chunghwa Telecom Co. Ltd. Telecommunication Laboratories No.99, Dianyan Rd. Yang-Mei, Taoyuan 326 Taiwan, ROC -Yeou-Fuh Kuan TEL: +886-3-424-4333 FAX: +886-3-424-4129 -Char-Shin Miou TEL: +886-3-424-4381 FAX: +886-3-424-4129	**HiCOS v3.4 PKI Native Smart Card** **Version 2.2 (Firmware)**	Renesas RS45C	11/15/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1953)] "HiCOS PKI Native Smart Card supports SHA-1, SHA-256, SHA-384, SHA-512, Hash-DRBG, 3DES-3Key-MAC, 3DES-3Key encrypt/decrypt, RSA 2048 encrypt/decrypt (including RSA-CRT), RSA digital signature generation /verification(including RSA-CRT) and APDU command/response encryption and/or MAC"
279	Allegro Software Development Corporation 1740 Massachusetts Avenue Boxborough, MA 01719 USA -Larry LaCasse TEL: +1 (978) 264-6600	**Allegro Cryptographic Engine** **Version 1.1**	Dell Optiplex 775, Intel Core 2 Duo w/ Windows 7 Ultimate	11/15/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1952)] "The Allegro Cryptographic Engine (ACE) is a cryptographic library module for embedded computing systems. ACE provides software implementations of algorithms for calculations of message digests, digital signature creation and verification, bulk encryption and decryption, key generation and key exchange."
278	Panzura Inc. 22 Great Oaks Blvd #150 San Jose, CA 95119 USA -Rich Weber TEL: (408) 578-8888	**Panzura Cryptographic Module** **Version 4.2**	Intel Xeon E5620 (x86) with AES-NI w/ Panzura Cloud Controller 8.0; Intel Xeon E5620 (x86) with AES-NI w/ Panzura Cloud Controller 8.0 on VMware ESX; Intel Xeon E5620 (x86) w/ Panzura Cloud Controller 8.0 on VMware ESX	11/15/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1951)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1389)]

					CTR_DRBG: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2269)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2269)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#366) (SHS Val#1951) "The Panzura Cyrptographic Module provides validated cryptographic services for multiple Panzura products."
277	SafeNet Inc. 4690 Millennium Drive Belcamp, MD 21017 USA -Jim Dickens TEL: 443-327-1389 FAX: 443-327-1210 -Chris Brych TEL: 613-221-5081 FAX: 613-723-5079	**SafeXcel 3120 Chip** **Part # SF914-35005-002A, v2.8.5**	N/A	10/23/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#2262)] "The SafeNet SafeXcel-3120 is a highly integrated device designed for modest performance and high security, where power and cost-sensitivity are a priority at the network edge. The embedded ARM processor, via a digital signature, will allow customer-specific application code to execute, enabling the device to implement a complete product solution." *10/31/12: Updated implementation information;*
276	Senetas Corporation Ltd. Level 1, 11 Queens Road Melbourne, Victoria 3004 Australia -John Weston TEL: +61 3 9868 4555 FAX: +61 3 9821 4899 -Julian Fay TEL: +61 3 9868 4555 FAX: +61 3 9821 4899	**CN6000 Series Cryptographic Library** **Version 0.98 (Firmware)**	Intel ATOM	10/23/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1945)] "Senetas Corporation's CN6000 Series Crypto Library Module provides FIPS 140-2 approved cryptographic algorithms for the CN6000 Series Encryptor. Based upon OpenSSL the CN6000 Series Crypto Library provides an Application Programming Interface (API) to support security relevant services."
275	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**CiscoSSL FIPS Object Module** **Version 2.0**	Intel Core i5-650 with AES-NI (x64) w/ Microsoft Windows 7; Intel Core i5-2520M with AES-NI (x64) w/ Mac OS X 10.7; Intel Xeon E5504 (x64) w/ FreeBSD 9.0; Intel Xeon E5649 with AES-NI (x64) w/ Linux 2.6; Cavium CN5230 (MIPS) (x64) w/ Linux 2.6; Snapdragon S3 APQ8060 (ARM) w/ Android 4.0; Freescale 8548 (PowerPC) w/ Linux 2.6; Apple A5X (ARM) w/ Apple iOS 5.1; ARMv7 w/ Android 4.0; PowerPC, Freescale's PowerQUICC III Processor Family w/ Linux 2.6	10/17/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1942)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1382)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2255)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2255)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#362) (SHS Val#1942) "The Cisco FIPS Object Module is a software library that provides cryptographic services to a vast array of Cisco's networking and collaboration products." *07/03/13: Added new tested information;*
274	Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**IOS-XE Cryptographic Implementation** **Version 1.0 (Firmware)**	MPC8572E	10/17/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2252)] "IOS-XE Firmware cryptographic implementations used within Cisco devices to provide cryptographic functions."
273	RSA the Security Division of EMC Level 11, 345 Queen Street Brisbane, Queensland 4000 Australia -Stefan Pingel TEL: +61-730325211 FAX: +61-730325299 -Peter Robinson TEL: +61-730325253 FAX: +61-730325299	**RSA BSAFE® Crypto-J JSAFE and JCE Software Module** **Version 6.1 and 6.1.1.0.1**	AMD Athlon 64 X2 Dual-Core Processor 3800+ w/ Microsoft Windows 7 (64-bit) with Sun JRE 7.0; Intel T7300 Core 2 Duo w/ Android 2.2 ARM (32-bit) JRE 6.0	10/17/2012	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1378)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (SHS Val#1938) "RSA BSAFE Crypto-J security software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. It supports a wide range of industry standard encryption algorithms offering Java developers

					the flexibility to choose the option most appropriate to meet their requirements." *11/22/13: Updated implementation information; 07/10/14: Updated implementation information;*
272	RSA The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Damon Hopley TEL: 781-515-6355	**RSA BSAFE Crypto-C Micro Edition (ME)** **Version 3.0.0.17**	PowerPC 460 (32-bit) w/ Timesys Linux 2.6.26.8-rt16	10/17/2012	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1377)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#356) (SHS Val#1937) "RSA BSAFE® Crypto-C ME software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. The software supports a wide range of industry standard encryption algorithms offering developers the flexibility to choose the appropriate option to meet their requirements."
271	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101 -Sunil Chitnis TEL: 408-333-2444 FAX: 408-333-4887	**FIPS 140-2 Certification for MLXe with a MR2 Management Modules** **Version Brocade Ironware with NIFIPS05200_0222121200 (Firmware)**	Freescale MPC 7448	10/17/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1936)] "The Brocade cryptographic library implements crypto operations in software. The Brocade MLX Series is highly optimized for IP Ethernet deployments, providing symmetric scaling and industry-leading wire-speed port capacity without compromising the performance of advanced capabilities such as IPv6, MPLS, and MPLS Virtual Private Networks (VPNs)."
270	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101 -Sunil Chitnis TEL: 408-333-2444 FAX: 408-333-4887	**FIPS 140-2 Certification for MLXe with a MR Management Modules** **Version Brocade Ironware with NIFIPS05200_0222121200 (Firmware)**	Freescale MPC 7447	10/5/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1935)] "The Brocade cryptographic library implements crypto operations in software. The Brocade MLX Series is highly optimized for IP Ethernet deployments, providing symmetric scaling and industry-leading wire-speed port capacity without compromising the performance of advanced capabilities such as IPv6, MPLS, and MPLS Virtual Private Networks (VPNs)."
269	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101 -Sunil Chitnis TEL: 408-333-2444 FAX: 408-333-4887	**FIPS 140-2 Certification for CER 2000 Series** **Version Brocade Ironware with NIFIPS05200_0222121200 (Firmware)**	Freescale MPC 8544	10/5/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1934)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. Brocade® NetIron® CER 2000 Series routers allow service providers to save space, power, and cooling while extending wire-speed IP and Multi-Protocol Label Switching (MPLS) services to the network edge."
268	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Chris Marks TEL: 408-333-0480 FAX: 408-333-8101	**FIPS for Brocade IP Products** **Version FIFIPS07400_1002121000 (Firmware)**	Feroceon 88FR131 rev1 (v5b)	10/5/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1933)] "The Brocade crypotgraphic library used in Brocade IP products implements crypto operations in software. The Brocade One-strategy helps simplify networking infrastructures through innovative technologies and solutions."
267	Stonesoft Corporation Itälahdenkatu 22A Helsinki, FI-00210 Finland -Klaus Majewski TEL: +358-9-476711 -Jorma Levomäki TEL: +358-9-476711	**Stonesoft Cryptographic Library** **Version 1.1**	Intel X3450 w/ GNU / Linux (Debian) 6.0	10/5/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2241)] "Stonesoft Cryptographic Library is a software module that provides cryptographic services for Stonesoft network security products." *09/25/13: Updated implementation information;*
266	Stonesoft Corporation Itälahdenkatu 22A Helsinki, FI-00210 Finland	**Stonesoft Cryptographic Library** **Version 1.1**	Intel Atom 425 w/ GNU / Linux (Debian) 6.0	10/5/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2240)]

	-Klaus Majewski TEL: +358-9-476711 -Jorma Levomäki TEL: +358-9-476711				"Stonesoft Cryptographic Library is a software module that provides cryptographic services for Stonesoft network security products." *09/20/13: Updated implementation information;*
265	Juniper Networks Inc. 1194 North Mathilda Ave. Sunnyvale, CA 94089 USA -Sharath Sridhar TEL: +91 80 30538736 FAX: +91 80 30538824	**OpenSSL** **Version Junos 12.1R3 (Firmware)** **Part # EX-3300**	Marvell Feroceon ARM v5 w/ Junos 12.1R3; Freescale e500v2 Power PC w/ Junos 12.1R3	10/5/2012	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1367)] "Comprehensive, scalable switching solutions specifically designed to meet the needs of both enterprises and service providers. All of our switches - modular and fixed platforms - run on one common operating system- Junos."
264	OpenSSL Software Foundation Inc. 1829 Mount Ephraim Road Adamstown, MD 27101 USA -Steve Marquess TEL: 877-673-6775	**OpenSSL FIPS Object Module** **Version 2.0.2**	PowerPC-e500 w/ NetBSD 5.1; Intel Xeon 5500 (x86-64) w/ NetBSD 5.1; Intel Xeon E3-1220v2 (x86) w/ RHEL 6 32-bit under vSphere; Intel Xeon E3-1220v2 (x86) w/ Windows 2008 32-bit under vSphere; Intel Xeon E3-1220v2 (x86) w/ RHEL 6 64-bit under vSphere; Intel Xeon E3-1220v2 (x86) w/ Windows 2008 64-bit under vSphere; Intel Core i5-2430M (x86) w/ Windows 7 64-bit with AES-NI; TI DM3730 (ARMv7) w/ Android 4.1; TI DM3730 (ARMv7) with NEON w/ Android 4.1; Nvidia Tegra 3 (ARMv7) w/ Android 4.2; Nvidia Tegra 3 (ARMv7) with NEON w/ Android 4.2; ARM Cortex A8 (ARMv7) with NEON w/ Apple iOS 5.0; Qualcomm MSM8X60 (ARMv7) with NEON w/ VMware Horizon Mobile 1.3 under VMware; Intel Core i7-3615QM w/ Apple OS X 10.7	10/5/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1923)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1363)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2234)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2234)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#347) (SHS Val#1923) "The OpenSSL FIPS Object Module is a full featured general purpose cryptographic library that is distributed in source code form under an open source license. It can be dowloaded from www.openssl.org/source/." *12/31/12: Added new tested information;* *02/06/13: Update implementation information;* *02/21/13: Added new tested information;* *03/11/13: Updated implementation information;*
263	Juniper Networks Inc 1194 N. Mathilda Ave Sunnyvale, CA 94089 USA -Balachandra Shanabhag TEL: +91-80-41904260	**OpenSSL** **Version JUNOS-FIPS 12.1R3 (Firmware)**	Freescale Power PC; Intel(R) Pentium(R) M; Intel Pentium III	10/5/2012	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1362)] "Comprehensive, scalable and secure routing solutions specifically designed to meet the needs of both enterprises and service providers. All of our routers - core, Multiservice edge and edge ethernet - run on one common operating system- Junos."
262	Intel Corporation 2200 Mission College Blvd. Santa Clara, California 95054 USA -Joel Schuetze TEL: 503-523-6026 -Min Cao TEL: 086-021-61165462	**QuickAssist Technology Software Library for Cryptography on the Intel® Communications Chipset 89xx Series** **Version 1.0.0** **Part # Intel® Communication Chipset 8920**	Intel® Communications Chipset 89xx Series w/ Intel® Celeron® Processor 725C w/ Fedora 16	10/5/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-256) (AES Val#2223)] "Intel® Celeron® Processor 725C with Intel® Communications Chipset 89xx Series using Intel® QuickAssist Technology. The accelerator features are invoked using the Intel® QuickAssist Technology Cryptographic API which provides application scalability and portability across platforms." *AES128 - Prediction Resistance was enabled with blockcipher use df; AES256 - Prediction Resistance was enabled with blockcipher No df;* *10/10/12: Updated implementation information;*
261	Vocera Communications Inc. 525 Race Street San Jose, CA 95126 USA -Thirumalai Bhattar TEL: 408-882-5841 -Arun Mirchandani TEL: 408-880-5100	**Wireless Communications Cryptographic Library** **Version 2.0**	Texas Instruments OMAP5912 w/ Vocera Embedded Linux v1.1	10/5/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1) (SHS Val#1914)] "The Wireless Communications Cryptographic Library provides cryptographic services to Vocera's Communications Badge product. The Vocera Communications Badge is a wearable device that enables secure two-way voice conversation without the need to remember a phone number or use a handset."
260	Apricorn, Inc. 12191 Kirham Rd Poway, CA 92064 USA	**Apricorn FIPS Module 140-2** **Version 4.0 (Firmware)** **Part # Apricorn APR26k22**	Apricorn APR26k22	9/28/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1911)] "Micro Controller to USB 2.0/3.0 SATA bridge ASIC."

	-Robert Davidson TEL: 858-513-2000 FAX: 858-513-2020				*10/05/12: Updated implementation information;*
259	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA -Tim Myers TEL: 800-Microsoft FAX: (none)	**Windows 8, Windows RT, Windows Server 2012, Surface Windows RT, Surface Windows 8 Pro, Windows Phone 8 and Windows Storage Server 2012 Cryptography Next Generation (CNG) Implementations** **Version 6.2.9200**	Qualcomm Snapdragon S4 w/ Windows RT (ARMv7 Thumb-2); NVIDIA Tegra 3 Quad-Core w/ Windows RT (ARMv7 Thumb-2); Intel Core i7 with AES-NI w/ Windows 8 Enterprise (x64); Intel Pentium D w/ Windows 8 Enterprise (x64); AMD Athlon 64 X2 Dual Core w/ Windows 8 Enterprise (x86); Intel Pentium D w/ Windows Server 2012 (x64); Intel Core i7 with AES-NI w/ Windows Server 2012 (x64); Qualcomm Snapdragon S4 w/ Windows Phone 8 (ARMv7 Thumb-2); Intel x64 Processor with AES-NI w/ Surface Windows 8 Pro (x64) ; Intel Core i7 without AES-NI w/ Windows Storage Server 2012; Intel Core i7 with AES-NI w/ Windows Storage Server 2012	9/26/2012	**Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-256) (ECDSA Val#341) (SHS Val#1903) "The Microsoft Windows Cryptographic Primitives Library is a general purpose, software-based, cryptographic module which can be dynamically linked into applications by developers to permit the use of FIPS 140-2 Level 1 compliant cryptography." *11/29/12: Added new tested information;* *01/16/13: Updated and added new tested implementation information;* *05/31/13: Added new tested information;* *06/20/13: Updated implementation information;*
258	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA -Tim Myers TEL: 800-Microsoft FAX: (none)	**Windows 8, Windows RT, Windows Server 2012, Surface Windows RT, Surface Windows 8 Pro, Windows Phone 8 and Windows Storage Server 2012 Next Generation Symmetric Cryptographic Algorithms Implementations (SYMCRYPT)** **Version 6.2.9200**	Qualcomm Snapdragon S4 w/ Windows RT (ARMv7 Thumb-2); NVIDIA Tegra 3 Quad-Core w/ Windows RT (ARMv7 Thumb-2); Intel Core i7 with AES-NI w/ Windows 8 Enterprise (x64); Intel Pentium D w/ Windows 8 Enterprise (x64); AMD Athlon 64 X2 Dual Core w/ Windows 8 Enterprise (x86); Intel Core i7 with AES-NI w/ Windows Server 2012 (x64); Intel Pentium D w/ Windows Server 2012 (x64); Qualcomm Snapdragon S4 w/ Windows Phone 8 (ARMv7 Thumb-2); Intel x64 Processor with AES-NI w/ Surface Windows 8 Pro (x64) ; Intel Core i7 without AES-NI w/ Windows Storage Server 2012; Intel Core i7 with AES-NI w/ Windows Storage Server 2012	9/13/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2197)] "The Next Generation Cryptographic algorithms provide enhanced support for AES, Triple-DES, SHS, HMAC, and AES DRBG. All implementations are packaged into a library, and it is used by Microsoft and other third-party applications." *11/28/12: Added new tested information;* *01/16/13: Updated and added new tested implementation information;* *04/25/13: Updated and added new tested implementation information;* *06/20/13: Updated implementation informaton;*
257	Cocoon Data Holdings Limited. Level 4 152-156 Clarence St Sydney, NSW 2000 Australia -Simon Wild TEL: +61 2 8412 8200 FAX: +61 2 8412 8202 -Stephen Thompson TEL: +61 2 8412 8200 FAX: +61 2 8412 8202	**Cocoon Data Secure Objects C++ Cryptographic Module Version 1.8** **Version 1.8**	2 X 2.4 GHz Quad-Core Intel Xeon w/ OS X; 2 X 2.4 GHz Quad-Core Intel Xeon w/ Windows XP Professional (x86); 2 X 2.4 GHz Quad-Core Intel Xeon w/ Windows XP Professional (x64); 2 X 2.4 GHz Quad-Core Intel Xeon w/ Ubuntu 10.04.02 (x86); 2 X 2.4 GHz Quad-Core Intel Xeon w/ Ubuntu 10.04.02 (x64); Core 2 Duo T667 2.2 GHz w/ Windows XP 32-bit; Service Pack 3 w/ MSVC2012; Core2 Duo T6670 2.2 GHz w/ Windows XP 32-bit; Service Pack 3 w/ MSVC2010; Core2 Duo T6670 2.2GHz w/ Windows 7 32-bit w/ MSVC2010 redistributable; Core i5 M450 2.4GHz w/ Windows 7 64-bit w/ MSVC2010 redistributable; Core2 Duo T6670 2.2 GHz w/ Windows 7 32-bit w/ MSVC2012 redistributable; Core i5 M450 2.4GHz w/ Windows 764-bit w/ MSVC2012 redistributable; Core i7 3615QM 2.3GHz w/ Ubuntu 12.04 LTS 32-bit on VMWare Fus. 4.1.3 on OSX; Core i7-3615QM 2.3Ghz w/ Ubuntu 12.04 LTS 64-bit on VMWare Fus. 4.1.3 on OSX; Dual CPU Xeon 5160 3GHz w/ Ubuntu 12.04 LTS 64-bit; Intel CPU Xeon 5110 1.6GHz w/ Ubuntu 12.04 LTS 32-bit; Core i7-3615QM 2.3GHz w/ RHEL 6.3 64-bit on VMWare Fus. 4.1.3 on OSX 10.8.2; Dual CPU Xeon 5160 3GHz w/ Redhat Enterprise Linux Server 6.3 64-bit; Intel CPU Xeon 5110 1.6GHz w/ RHEL 6.3 32-bit on VMWare Fusion 4.1.3 on OSX 10.8.2; Dual CPU Xeon 5110 1.5GHz w/ Redhat Enterprise Linux Server 6.3 32-bit; 2.3GHz Intel Core i7 w/ Mac OSX 10.8.2	8/30/2012	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1) (HMAC Val#1344)] "The Cocoon Data Secure Objects C++ Cryptographic Module Version 1.8 has been implemented as part of the Cocoon Data Secure Objects solution, an encryption-based access control system for protecting the confidentiality and integrity of electronic files." *03/27/13: Added new tested information and updated implementation information;*
256	Hewlett-Packard Longdown Avenue Stoke Gifford, Bristol BS34 8QZ United Kingdom -Laura Loredo TEL: +44 117 312 9341	**OpenSSL** **Version OpenSSL 1.0.1c/FIPS 2.0/CN22745 (Firmware)**	ARM966E	8/27/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2190)] "The Hewlett Packard LTO-6 Tape Drive is a multi-chip standalone module composed of hardware and firmware components, providing cryptographic services to a host." *09/07/12: Updated implementation information;*
255	Check Point Software Technologies 5 Ha'solelim Street Tel Aviv, 67897 Israel	**Check Point Crypto Core** **Version 2.0**	Intel® Core i7 @ 2.40 GHz with AES-NI w/ Pre-Boot EFI (via rEFIt on Mac OS X 10.7) 64-bits; Intel® Core i5-2400 @ 3.10 GHz with AES-NI w/ Microsoft Windows 7 User Space 32-bits; Intel® Core i5-2400	8/22/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2182)]

	-Malcolm Levy TEL: +972-37534561		@ 3.10 GHz with AES-NI w/ Microsoft Windows 7 Kernel Space 32-bits; Intel® Core i5-2400 @ 3.10 GHz with AES-NI w/ Microsoft Windows 7 User Space 64-bits; Intel® Core i5-2400 @ 3.10 GHz with AES-NI w/ Microsoft Windows 7 Kernel Space 64-bits; Intel® Core i7 @ 2.40 GHz with AES-NI w/ Mac OS X 10.7 User Space 32-bits; Intel® Core i7 @ 2.40 GHz with AES-NI w/ Mac OS X 10.7 Kernel Space 32-bits; Intel® Core i7 @ 2.40 GHz with AES-NI w/ Mac OS X 10.7 User Space 64-bits; Intel® Core i7 @ 2.40 GHz with AES-NI w/ Mac OS X 10.7 Kernel Space 64-bits; Intel® Core i7 @ 2.40 GHz w/ Pre-Boot EFI (via rEFIt on Mac OS X 10.7) 64-bits; Intel(R) Core 2 Duo CPU E6550 @ 2.33GHz w/ Microsoft Windows 7 User Space 32-bits; Intel(R) Core 2 Duo CPU E6550 @ 2.33GHz w/ Microsoft Windows 7 Kernel Space 32-bits; Intel® Core 2 Duo Processor E6600 @ 2.40GHz w/ Microsoft Windows 7 User Space 64-bits; Intel® Core 2 Duo Processor E6600 @ 2.40GHz w/ Microsoft Windows 7 Kernel Space 64-bits; Intel® Core i7 @ 2.40 GHz w/ Mac OS X 10.7 User Space 32-bits; Intel® Core i7 @ 2.40 GHz w/ Mac OS X 10.7 Kernel Space 32-bits; Intel® Core i7 @ 2.40 GHz w/ Mac OS X 10.7 User Space 64-bits; Intel® Core i7 @ 2.40 GHz w/ Mac OS X 10.7 Kernel Space 64-bits		"Check Point Crypto Core 2.X is a 140-2 Level 1 cryptographic module for Windows platforms, Check Point Pre-Boot Environment and Mac OS X. The module provides cryptographic services accessible in pre-boot mode, kernel mode and user mode on the respective platforms through implementation of platform specific binaries"
254	Integral Memory PLC. Unit 6 Iron Bridge Close Iron Bridge Business Park Off Great Central Way London, Middelsex NW10 0UF United Kingdom -Patrick Warley TEL: +44 (0)20 8451 8700 FAX: +44 (0)20 8459 6301 -Samik Halai TEL: +44 (0)20 8451 8704 FAX: +44 (0)20 8459 6301	**Integral AES 256 Bit Crypto SSDLock** **Version S5FDM018 (Firmware)**	PS3108 or PS3105	8/13/2012	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256) (HMAC Val#1335)] "The Integral AES 256 bit Crypto SSD is removable storage devices which encrypts documents transferred onto them. The Integral 256 bit Crypto SSD comes in 4 GB, 8 GB, 16 GB, 32 GB 64 GB 128 GB, 256 GB, 512 GB and 1 TB versions." *05/16/13: Updated implementation information;*
253	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Windows 64-bit x86-64 for 32 bits** **Version 8.2.2.0**	Intel Core i7-2600 w/ Microsoft Windows Server 2008 64-bit	8/13/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1889)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1333)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2179)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2179)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *09/26/12: Updated implementation information;* *05/08/13: Updated implementation information;*
252	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Windows 64-bit x86-64 for 64 bits** **Version 8.2.2.0**	Intel Core i7-2600 w/ Microsoft Windows Server 2008 64-bit	8/13/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1886)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1331)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2170)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2170)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *09/26/12: Updated implementation information;* *05/08/13: Updated implementation information;*

251	IBM® Corporation Seabank Centre 12-14 Marine Parade Southport QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Windows 32-bit x86-64 for 32 bits** **Version 8.2.2.0**	AMD Opteron X86_64 w/ Microsoft Windows Server 2008 32-bit	8/13/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1885)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1330)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2169)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2169)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *09/26/12: Updated implementation information; 05/08/13: Updated implementation information;*
250	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Solaris UltraSparc-64 for 64 bits** **Version 8.2.2.0**	Sun UltraSPARC T1 64-bit w/ Sun Solaris 10	8/8/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1884)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1329)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2167)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2167)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *09/26/12: Updated implementation information; 05/08/13: Updated implementation information;*
249	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Solaris UltraSparc-64 for 32 bits** **Version 8.2.2.0**	Sun UltraSPARC T1 64-bit w/ Sun Solaris 10	8/8/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1883)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1328)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2166)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2166)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *09/26/12: Updated implementation information; 05/08/13: Updated implementation information;*
248	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL zSeries-64 for 64 bits** **Version 8.2.2.0**	IBM zSeries z196 64-bit w/ Red Hat Enterprise Linux Server 5	8/8/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1882)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1327)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2165)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2165)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."

					09/26/12: Updated implementation information; 05/08/13: Updated implementation information;
247	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL zSeries-64 for 32 bits** **Version 8.2.2.0**	IBM zSeries z196 64-bit w/ Red Hat Enterprise Linux Server 5	8/8/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1881)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1326)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2162)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2162)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *09/26/12: Updated implementation information; 05/08/13: Updated implementation information;*
246	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL x86-64 for 64 bits** **Version 8.2.2.0**	Intel Core i7-2600 w/ Red Hat Enterprise Linux Server 5	8/8/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1880)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1325)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2161)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2161)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *09/26/12: Updated implementation information; 05/08/13: Updated implementation information;*
245	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL x86-64 for 32 bits** **Version 8.2.2.0**	Intel Core i7-2600 w/ Red Hat Enterprise Linux Server 5	8/8/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1879)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1324)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2160)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2160)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *09/26/12: Updated implementation information;*
244	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL PPC64 for 64 bits** **Version 8.2.2.0**	IBM PowerPC 970 w/ Red Hat Enterprise Linux Server 5	8/8/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1878)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1323)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2159)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2159)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."

					09/26/12: Updated implementation information; 05/08/13: Updated implementation information;
243	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL PPC64 for 32 bits** **Version 8.2.2.0**	IBM PowerPC 970 w/ Red Hat Enterprise Linux Server 5	8/8/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1877)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1322)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2158)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2158)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *09/26/12: Updated implementation information; 05/08/13: Updated implementation information;*
242	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL 32-bit x86-64 for 32 bits** **Version 8.2.2.0**	AMD Opteron X86_64 w/ Red Hat Enterprise Linux Server 5	8/8/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1876)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1321)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2157)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2157)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *09/26/12: Updated implementation information; 05/08/13: Updated implementation information;*
241	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on AIX PowerPC-64 for 64 bits** **Version 8.2.2.0**	IBM PowerPC 5 64-bit w/ IBM AIX 6.1	8/8/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1875)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1320)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2156)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2156)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider." *09/26/12: Updated implementation information; 05/24/13: Updated implementation information;*
240	IBM® Corporation Seabank Centre 12 - 14 Marine Parade Southport, QLD 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420	**ICC Algorithmic Core on AIX PowerPC-64 for 32 bits** **Version 8.2.2.0**	IBM PowerPC 5 64-bit w/ IBM AIX 6.1	8/8/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1874)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1319)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2155)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2155)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."

					09/26/12: Updated implementation information; 05/08/13: Updated implementation information;
239	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Bipin Agarwal TEL: 408-333-4830 FAX: 408-333-4885	**FIPS for Brocade IP Products** **Version FIFIPS07300_0314121830 (Firmware)**	Freescale MPC 8544E	8/8/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1871)] "The Brocade cryptographic library used in Brocade IP products implements crypto operations in software. The Brocade One strategy helps simplify networking infrastructures through innovative technologies and solutions."
238	Marvell Semiconductor, Inc. 5488 Marvell Lane Santa Clara, CA 95054 USA -Minda Zhang TEL: (508) 573-3255 FAX: (508) 573-3311	**Armada PXA-2128** **Version 3.1.9 (Firmware)** **Part # Armada PXA-2128**	Marvell® PJ4 application processor family (ARMv7 class)	8/3/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1857)] "Armada PXA2128 is an application processor SoC (http://www.marvell.com/application-processors/armada/pxa2128/). It has a dedicated security hardware module, known as WTM, that runs secure firmware kernel to perform device trusted boot, access control, authentication, key management, DRM, disk encryption, and FIPS certified cryptographic operations."
237	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**IOS Common Cryptographic Module (IC2M)** **Version Rel 1 (Firmware)**	PMC RM5261A MIPS 350MHz; Intel Woodcrest 2.13GHz; Power-PC 405 250MHz	7/30/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2134)] "IOS Common Cryptographic Module (IC2M) firmware version Rel 1 covers Rel 1(1.0.0), Rel 1(1.0.1) and Rel 1(1.0.2)" *12/07/12: Updated implementation information; 04/23/13: Updated implementation information;*
236	CREDANT Technologies, Inc. 15303 Dallas Parkway Suite 1420 Addison, TX 75001 USA -Chris Burchett TEL: 972-458-5407 FAX: 972-458-5454 -Brad Conte TEL: 972-458-5400 FAX: 972-458-5454	**Credant Cryptographic Kernel (User Mode)** **Version 1.8**	Intel Core 2 Duo w/ Windows 7 Enterprise x64 Edition (64-bit); Intel Core 2 Duo w/ Windows 7 Enterprise (32-bit); Intel Core i7 w/ Mac OS X Lion 10.7.3 (64-bit); Intel Core i7 w/ Mac OS X Lion 10.7.3 (32-bit); Intel Core 2 Duo w/ Ubuntu Linux 11.04 (64-bit); Intel Core 2 Duo w/ Ubuntu Linux 11.04 (32-bit)	7/18/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2131)] "CREDANT CmgCryptoLib is a software cryptographic library that implements Triple-DES, AES, DRBG SP 800-90, SHA-2, SHA-1, HMAC-SHA2, and HMAC-SHA-1 algorithms for CREDANT Mobile Guardian (CMG) products."
235	CREDANT Technologies Inc. 15303 Dallas Parkway Suite 1420 Addison, TX 75001 USA -Chris Burchett TEL: 972-458-5407 FAX: 972-458-5454 -Brad Conte TEL: 972-458-5400 FAX: 972-458-5454	**Credant Cryptographic Kernel (Kernel Mode)** **Version 1.8**	Intel Core 2 Duo w/ Windows 7 Enterprise x64 Edition (64-bit); Intel Core 2 Duo w/ Windows 7 Enterprise (32-bit); Intel Core i7 w/ Mac OS X Lion 10.7.3 (64-bit); Intel Core i7 w/ Mac OS X Lion 10.7.3 (32-bit)	7/18/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2130)] "CREDANT CmgCryptoLib is a software cryptographic library that implements Triple-DES, AES, DRBG SP 800-90, SHA-2, SHA-1, HMAC-SHA2, and HMAC-SHA-1 algorithms for CREDANT Mobile Guardian (CMG) products."
234	SafeLogic Inc 530 Lytton Ave, Ste 200 Palo Alto, CA 94301 USA -SafeLogic Inside Sales	**CryptoComply Mobile Engine for iOS** **Version 2.1**	A5X w/ iOS 5.1; A5X w/ iOS 6; A5X w/ iOS 7	7/18/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1850)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1297)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2126)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2126)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#320) (SHS Val#1850) "CryptoComply | Mobile is a standards-based "Drop-in Compliance" solution for mobile devices. The module features robust algorithm support, including Suite B algorithm compliance. CryptoComply offloads functions for secure key management, data integrity, data at rest encryption, and secure communications."

					10/31/12: Added new tested information; *11/14/12: Updated vendor information;* *09/25/13: Added new tested information;*
233	SafeLogic Inc 530 Lytton Ave, Ste 200 Palo Alto, CA 94301 USA -SafeLogic Inside Sales	**CryptoComply Mobile Engine for Android** **Version 2.1**	ARM Cortex-A9 w/ Android Version 4.0	7/18/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1849)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1296)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2125)] BlockCipher_No_df: (, AES-192 , AES-256) (AES Val#2125)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#319) (SHS Val#1849) "CryptoComply | Mobile is a standards-based "Drop-in Compliance" solution for mobile devices. The module features robust algorithm support, including Suite B algorithm compliance. CryptoComply offloads functions for secure key management, data integrity, data at rest encryption, and secure communications." *08/01/12: Added new tested information;* *11/14/12: Updated vendor information;*
232	Thales E-Security Ltd Jupiter House Station Road Cambridge, CB5 8JJ UK -Thales Certification Team TEL: +44 1223 723600 FAX: +44 1223 723601 -Thales Sales TEL: 888 744 4976	**nShield Algorithm Library** **Version 2.51.10 (Firmware)**	Freescale PowerPC	7/13/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2122)] "The nShield algorithm library provides cryptographic functionality for Thales's nShield Hardware Security Modules" *12/17/12: Updated implementation information;*
231	Inside Secure 41 Parc Club du Golf 13856, Aix-en-Provence France -Ewart Gray TEL: +44 (0) 1355 803727 FAX: +44 (0) 1355 242743 -David Cunningham TEL: +44 (0) 1355 803554 FAX: +44 (0) 1355 242743	**VaultIC441/421/405** **Version 1.0.1 (Firmware)** **Part #** **VaultIC441M/VaultIC421M/VaultIC405M**	Inside Secure VaultIC441M/VaultIC421M/VaultIC405M	7/5/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#2119)] "VaultIC (R) are security modules designed to secure applications such as anti-cloning, physical access control, personal access control for multimedia and web applications, hardware authentication, user strong authentication, SSL support, PKCS#11 to Microsoft (R) CSP applications, PKI, DRM, trusted computing and IP protection." *07/18/12: Updated implementation information;*
230	SAP AG Albert-Einstein-Allee 3 Bensheim, NRW 64625 Germany -Stephan André TEL: +49-6251-708-1730 FAX: +49-6227-78-55975 -Thomas Rothe TEL: +49-6251-708-2339 FAX: +49-6227-78-55989	**SAP NW SSO 2.0 Secure Login Library Crypto Kernel** **Version 2.0.0.1**	Intel Core i5 660 3,33 GHz w/ Windows 7 Enterprise SP1	7/5/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2118)] "SAP NW SSO 2.0 Secure Login Library Crypto Kernel v2.0.0.1 is a shared library, i.e. it consists of software only. SAP NW SSO 2.0 Secure Login Library Crypto Kernel provides an API in terms of C++ methods for key management and operation of cryptographic functions."
229	OpenSSL Software Foundation Inc. 1829 Mount Ephraim Road Adamstown, MD 27101 USA -Steve Marquess TEL: 877-673-6775	**OpenSSL FIPS Object Module** **Version 2.0.1**	ARMv7 w/ Apple iOS 5.1; ARMv5TEJ w/ Microsoft Windows CE 6.0 R2; ARMv7 w/ Microsoft Windows CE 5.0	6/29/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1840)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1288)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2116)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2116)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-

					521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#315) (SHS Val#1840) "The OpenSSL FIPS Object Module is a full featured general purpose cryptographic library that is distributed in source code form under an open source license. It can be downloaded from www.openssl.org/source/."
228	IBM Corporation 11400 Burnet Road Austin, TX 78758 USA -Tom Benjamin TEL: 512-286-5319 -Kevin Driver TEL: 512-286-6017	**IBM Java JCE 140-2 Cryptographic Module** **Version 1.7**	Intel Core 2 Duo w/ Windows 7 32-bit; Intel Core 2 Duo w/ Solaris 11.0; IBM PowerPC Power6 w/ IBM AIX 7.1	6/29/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1830)] "The IBM Java JCE (Java Cryptographic Extension) FIPS provider (IBMJCEFIPS) for Multi-platforms is a scalable, multipurpose cryptographic module that supports many FIPS approved cryptographic operations. This gives Java applications access to the FIPS algorithms via the standard JCE framework that is part of all JVM's at the 1.4.0 level and higher."
227	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module** **Version 3.0**	Intel i7 w/ OSX 10.8	6/29/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2104)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
226	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module** **Version 3.0**	Intel i5 w/ OSX 10.8	6/29/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2103)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
225	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module** **Version 3.0**	Apple A4 w/ iOS 6	6/29/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2102)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
224	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Kernel Module** **Version 3.0**	Apple A5 w/ iOS 6	6/29/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2101)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
223	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module** **Version 3.0**	Apple A5 w/ iOS 6	6/29/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2100)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and generic, non-optimized software."
222	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Kernel Module** **Version 3.0**	Apple A4 w/ iOS 6	6/29/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2099)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
221	Mocana Corporation 710 Sansome Street San Francisco, CA 94104 USA -Sales TEL: 415-617-0055 FAX: 415-617-0056	**Mocana Cryptographic Library** **Version 5.5fs**	PowerQUICC III w/ Integrity 5.0; ARMv7 w/ IOS 5; ARMv7 w/ iOS6	6/29/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2096)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#307) (SHS Val#1820) "The Mocana Cryptographic Module is the engine of Mocana's Device Security Framework - a software framework that secures all aspects of a system. The Device Security Framework helps applications and device designers reduce development costs and dramatically enhance

					cryptographic performance. For details see www.mocana.com." *03/25/13: Added new tested information; 03/27/13: Updated vendor information;*
220	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module** **Version 3.0**	Intel i7 w/ OSX 10.8	6/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2094)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
219	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module** **Version 3.0**	Intel i7 w/ OSX 10.8	6/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2092)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
218	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module** **Version 3.0**	Intel i5 w/ OSX 10.8	6/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2090)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
217	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Module** **Version 3.0**	Intel i5 w/ OSX 10.8	6/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2088)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
216	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module** **Version 3.0**	Intel i7 w/ OSX 10.8	6/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2087)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
215	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module** **Version 3.0**	Intel i7 w/ OSX 10.8	6/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2085)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
214	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module** **Version 3.0**	Intel i7 w/ OSX 10.8	6/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2084)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and assembler optimized AES."
213	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module** **Version 3.0**	Intel i5 w/ OSX 10.8	6/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2083)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and generic, non-optimized software."
212	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple OSX CoreCrypto Kernel Module** **Version 3.0**	Intel i5 w/ OSX 10.8	6/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2081)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and the AES-NI Intel instruction set with an accellerated implementation for CBC and XTS."
211	Apple Inc.	**Apple OSX CoreCrypto Kernel Module**	Intel i5 w/ OSX 10.8	6/25/2012	**CTR_DRBG**: [Prediction Resistance Tested:

	1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Version 3.0**			Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2080)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to kernel space and assembler optimized AES."
210	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module** **Version 3.0**	Apple A5 w/ iOS 6	6/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2075)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
209	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -Shawn Geddis	**Apple iOS CoreCrypto Module** **Version 3.0**	Apple A4 w/ iOS 6	6/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2072)] "Cryptographic library offering various cryptographic mechanisms to Apple frameworks. The testing applies to user space and assembler optimized AES."
208	Marvell Semiconductor Inc. 5488 Marvell Lane Santa Clara, CA 95054 USA -Robert Carden TEL: 408-222-5000 -Lei Poo TEL: 408-222-5000	**einstein_bcm_microcode_production** **Version 1.00.16 (Firmware)** **Part # 88229185**	88229185	6/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-128 , AES-256) (AES Val#1678)] "Marvell's Einstein2 SoC is a highly integrated System-On-Chip (SoC) controller solution customized for NAND Flash drives. It features a NAND Flash interface controller with a highly efficient architecture, and advanced correction capabilities. Einstein2 SoC supports many FIPS Approved Cryptographic Algorithms, including AES, SHA, HMAC, RSA and RNG."
207	Hewlett-Packard Company 19091 Pruneridge Ave., MS 4441 Cupertino, CA 95014 USA -Theresa Conejero TEL: 408-447-2964 FAX: 408-447-5525	**HP ESKM DRBG** **Version 5.0.0 (Firmware)**	Intel Xeon E5-2640	6/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2069)] "HP Enterprise Secure Key Manager (ESKM) provides key generation, retrieval, and management for encryption devices and solutions. ESKM is a hardened security appliance with secure access control, administration, and logging. ESKM supports high availability with automatic multi-site clustering, replication, and failover."
206	Totemo AG Totemo AG Freihofstrasse 22 CH-8700 Kusnacht Kusnacht, n/a Switzerland -Marcel Mock TEL: +41 (0) 44 914 9900	**Totemo Cryptographic Module (TCM)** **Version 2.0**	Intel Xeon E5504 processor w/ Totemo Appliance OS 2.0 v0711 with JRE 7.0	6/15/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1800)] "The Totemo Cryptographic Module supplies the cryptographic services required by the Totemo Security Platform (TSP) and the Totemo products which provides secure email, file transfer, and mobile messaging solutions. These solutions secure all types of communication without any infrastructure prerequisites." *06/14/12: Update implementation information and added new tested information;*
205	N/A	**N/A**	N/A	6/7/2012	N/A
204	N/A	**N/A**	N/A	6/7/2012	N/A
203	AuthenTec Inc. Boxtelseweg 26A Vught, 5261 NE The Netherlands -Bob Oerlemans TEL: +31 73 6581 900	**SafeZone FIPS Cryptographic Module** **Version 1.0.3**	ARMv7 w/ Android 4.0; ARMv7 w/ Android 2.3; ARMv7 w/ Linux (kernel 2.6)	6/5/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2041)] "SafeZone FIPS Cryptographic Module is a FIPS 140-2 Security Level 1 validated software cryptographic module from AuthenTec Inc. The module is a toolkit which provides the most commonly needed cryptographic primitives for a large variety of applications, including but not limited to, primitives needed for DAR, DRM, TLS, and VPN on mobile devices."
201	Mocana Corporation 710 Sansome Street San Francisco, CA 94104 USA -Mocana Sales TEL: 415-617-0055 FAX: 415-617-0056	**Mocana Cryptographic Library** **Version 5.5f**	ARMv7 w/ Android 4.0; ARMv7 w/ Android 2.2; ARMv7 w/ Android 2.3; ARMv7 w/ Android 4.1; Intel Core 2 Duo w/ Ubuntu Linux 32 bit; Intel Core 2 Duo w/ Ubuntu Linux 64 bit; FreeScale QorIQ P2 w/ VxWorks 6.8	5/31/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2039) (AES Val#2272)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-

					521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#298) (SHS Val#1785) "The Mocana Cryptographic Module is the engine of Mocana's Device Security Framework - a software framework that secures all aspects of a system. The Device Security Framework helps applications and device designers reduce development costs and dramatically enhance cryptographic performance. For details see www.mocana.com." *11/15/12: Added new tested information;* *11/27/12: Updated implementation information;* *12/27/12: Updated vendor information;*
200	3S Group Incorporated 125 Church Street, N.E., Suite 204 Vienna, VA 22180 USA -Satpal S. Sahni TEL: 703-281-5015 FAX: 703-281-7816	**3SGX** **Version 1.0 (Firmware)**	Cavium Octeon	5/25/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-384) (SHS Val#1784)] "3SGX is a high performance PCIe cryptograhic module that provides complete cryptographic support to large numbers of users or applications simultaneously. 3SGX is the core of 3S Group's hardare security appliances, ideal for enterprise key management, virtualization and cloud server solutions that demand high throughput."
199	Check Point Software Technologies Ltd. 9900 Belward Campus Dr. Suite 250 Rockville, MD 20850 USA -David Abrose TEL: +972 37534561 -Malcolm Levy TEL: +972 37534561	**Check Point Security Gateway** **Version R7x with R7x hotfix (Firmware)**	Intel Xeon	5/25/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1783)] "Check Point Security Gateway is a security gateway that provides firewall, VPN, and intrusion prevention functionality within a network environment."
198	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**7600 Series Routers IOS Cryptographic Implementation** **Version 1.0 (Firmware)**	Freescale MPC8548	5/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2036)] "IOS cryptographic implementation for the 7600 series routers."
197	Cavium Inc. 2315 N. First Street San Jose, CA 95131 USA -Mike Scruggs TEL: (408) 943-7100 FAX: (408) 577-1992 -TA (TAR) Ramanujam TEL: (408) 943-7383 FAX: (408) 577-1992	**Nitrox III DRBG** **Version Nitrox III DRBG, r69306 (Firmware)** **Part # Nitrox III series die, v1.1**	Cavium Nitrox III	5/25/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1780)] "NITROX III chips implement SHA1/SHA2, 3DES/AES256 CBC, ModMul/ModEx/RSA, GCM and CTR modes, and SP800-90A DRBG. Perf: 5 to 30 Gbps encrypt/hash; 35K to 200K RSA 1024b ops/sec; 6K to 35K RSA 2048b ops/sec. NITROX III microcode also implements protocol-specific acceleration for IPSec and SSL."
196	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**5915 Embedded Services Routers IOS Cryptographic Implementation** **Version 1.0 (Firmware)**	Freescale MPC8358E	5/25/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2031)] "Cisco C5915 is a PCI-104-based small form factor chassis less moderate performance router, part of the Embedded Services Router family. It is a follow-on to the 3251 Mobile Access Router card, offered to market through integration partners and mostly deployed for transportation customers, public safety agencies, and global defense organizations." *07/18/12: Updated implementation information;* *08/01/12: Updated implementation information;*
195	Vidyo Inc. 433 Hackensack Avenue Hackensack, NJ 07601 USA -Adi Regev TEL: 201-467-4636	**Cryptographic Security Kernel** **Version 1.0**	Intel Core i5 with AES-NI w/ 32-bit Windows XP; Intel Core i5 with AES-NI w/ 64-bit Windows 7; Intel Core i5 with AES-NI w/ 32-bit Windows 7; Intel Xeon E3 with AES-NI w/ 64-bit Linux Ubuntu 10.04; Intel Xeon E3 with AES-NI w/ 32-bit Linux Ubuntu 10.04; Intel Core i5 with AES-NI w/ 64-bit Mac OS X 10.7.3; Intel Core i5 with AES-NI w/ 32-bit Mac OS X 10.7.3; Intel Core i5 with AES-NI w/ 64-bit Mac OS X 10.6.8; Intel Core i5 with AES-NI w/ 32-bit Mac OS X 10.6.8	5/17/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2028)] "Vidyo creates HD video conferencing products that leverage their patented Adaptive Video Layering Architecture technology, which provides continuous HD video streaming regardless of network conditions. The Vidyo Cryptographic Security Kernel supplies the cryptographic services necessary to support Vidyo's secure video and data transmissions."
194	Vidyo Inc. 433 Hackensack Avenue Hackensack, NJ 07601 USA	**Cryptographic Security Kernel** **Version 1.0**	Intel Core Duo w/ 32-bit Mac OS X 10.6.8; Intel Core 2 Duo w/ 64-bit Mac OS X 10.6.8; Intel Core 2 Duo w/ 32-bit Mac OS X 10.7.3; Intel Core 2 Duo w/ 64-bit Mac OS X 10.7.3; Intel Xeon E50xx w/	5/17/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128) (AES Val#2027)]

	-Adi Regev TEL: 201-467-4636		32-bit Linux Ubuntu 10.04; Intel Xeon E50xx w/ 64-bit Linux Ubuntu 10.04; Intel Core 2 Duo w/ 64-bit Windows 7; Intel Core Duo w/ 32-bit Windows 7; Intel Core Duo w/ 32-bit Windows XP;		"Vidyo creates HD video conferencing products that leverage their patented Adaptive Video Layering Architecture technology, which provides continuous HD video streaming regardless of network conditions. The Vidyo Cryptographic Security Kernel supplies the cryptographic services necessary to support Vidyo's secure video and data transmissions."
193	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA -Kevin Michelizzi TEL: (425) 707-1227 FAX: (425) 936-7329 -Chien-Her Chin TEL: (425) 706-5116 FAX: (425) 936-7329	**Windows Embedded Compact Cryptographic Primitives Library (bcrypt.dll)** **Version 7.00.1687**	Sigma Designs SMP8654 (MIPSII_FP) w/ Windows Embedded Compact 7; Sigma Designs SMP8654 (MIPSII) w/ Windows Embedded Compact 7; ARMv7 (Texas Instruments EVM3530) w/ Windows Embedded Compact 7; ARMv6 (Samsung SMDK6410) w/ Windows Embedded Compact 7; ARMv5 (Freescale i.MX27) w/ Windows Embedded Compact 7; i586 (MSTI PDX-600) w/ Windows Embedded Compact 7;	5/9/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#2023)] "The cryptographic module BCRYPT.DLL encapuslates several different cryptographic algorithms in an easy-to-use module, accessible via the Microsoft CNG (Cryptography Next Generation) API. It permits the use of general-purpose FIPS 140-2 compliant cryptography in Windows Embedded Compact components and applications, through its documented interfaces."
192	RSA, The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Damon Hopley TEL: 781-515-6355	**RSA BSAFE Crypto-C Micro Edition (ME)** **Version 3.0.0.16**	PowerPC 604 (32-bit) w/ Wind River VxWorks 6.0	5/9/2012	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1222)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#293) (SHS Val#1768) "RSA BSAFE® Crypto-C ME software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. The software supports a wide range of industry standard encryption algorithms offering developers the flexibility to choose the appropriate option to meet their requirements."
191	RSA, The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Damon Hopley TEL: 781-515-6355	**RSA BSAFE Crypto-C Micro Edition** **Version 4.0.1**	Intel Celeron w/ Microsoft Windows XP SP3 - x86 (32-bit); AMD Athlon XP1800+ w/ Microsoft Windows XP SP3 - x86 (64-bit); AMD Athlon 64 X2 w/ Microsoft Windows Server 2003 - x86 (32-bit); AMD Athlon 64 X2 4000+ w/ Microsoft Windows Server 2003 - x86(64-bit); Intel Itanium 2 w/ Microsoft Windows Server 2003 - Itanium 64-bit (Visual Studio 2005 SP1); Intel Itanium 2 w/ Microsoft Windows Server 2003 - Itanium 64-bit (Visual Studio 2010); AMD Athlon 64 X2 w/ Red Hat Enterprise Server 5.5 - x86 (32-bit); AMD Athlon 64 X2 w/ Red Hat Enterprise Server 5.5 - x86 (64-bit); Intel Itanium II w/ Red Hat Enterprise Server 5.5 - Itanium 64-bit; AMD Athlon 64 X2 w/ Red Hat Enterprise Linux 6.0 - x86 (32-bit); AMD Athlon 64 X2 w/ Red Hat Enterprise Linux 6.0 - x86(64-bit); PowerPC POWER3-II w/ Red Hat Enterprise Linux 5.0 - PPC 32-bit; PowerPC POWER3-II w/ Red Hat Enterprise Linux 5.0 - PPC 64-bit; Intel Core 2 Duo w/ Apple Mac OS X 10.6 Snow Leopard - x86 (32-bit); Intel Core 2 Duo w/ Apple Mac OS X 10.6 Snow Leopard - x86 (64-bit); Sun UltraSparc Iie w/ Solaris 10 - SPARC v8; Sun UltraSparc IIe w/ Solaris 10 - SPARC v8+; Sun UltraSparc IIIi w/ Solaris 10 - SPARC v9; Intel Celeron w/ Solaris 10 - x86 (32-bit); AMD Athlon 64 X2 w/ Solaris 10 - x86 (64-bit); HP PA-8600 w/ HP-UX 11.23 - PA RISC 2.0; HP PA-8600 w/ HP-UX 11.23 - PA-RISC 2.0W; Intel Itanium 2 w/ HP-UX 11.31 - Itanium 32-bit; Intel Itanium 2 w/ HP-UX 11.31 - Itanium 64-bit; PowerPC POWER5 w/ IBM AIX 5.3 - PPC 32-bit; PowerPC POWER5 w/ IBM AIX 5.3 - PPC 64-bit; PowerPC POWER5 w/ IBM AIX 6.1 - PPC 32-bit; PowerPC POWER5 w/ IBM AIX 6.1 - PPC 64-bit; PowerPC POWER7 w/ IBM AIX 7.1 - PPC 32-bit; PowerPC POWER7 w/ IBM AIX 7.1 - PPC 64-bit; Intel Core i7 M620 w/ Microsoft Windows 7 - x86 (64-bit) w/ AES-NI; Intel Core i7 M620 w/ Microsoft Window XP - x86 (32-bit) w/ AES-NI; Intel Core i5 2500 w/ Solaris 10 - x86 (64-bit) w/ AES-NI; Intel Core i5 2500 w/ Solaris 10 - x86 (32-bit)w/ AES-NI; Intel Core i7 w/ Red Hat	5/9/2012	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1221)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#292) (SHS Val#1767) "RSA BSAFE® Crypto-C ME software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. The software supports a wide range of industry standard encryption algorithms offering developers the flexibility to choose the appropriate option to meet their requirements."

			Enterprise Linux v5.5 - x86 (32-bit)w/ AES-NI; Intel Core i7 w/ Red Hat Enterprise Linux v6.0 - x86 (64-bit) w/ AES-NI; Sun Sparc T4 w/ Solaris 10 - SPARC T4		
190	GE Healthcare 3000 N Grandview Blvd Waukesha, WI 53188 USA -Krishna Inavolu TEL: 262-391-8589 FAX: 262-548-2910 -Stephanie Swenor TEL: 262-424-8931 FAX: 262-544-3889	**Mocana Cryptographic Library** **Version 5.4F (Firmware)**	Intel Core 2 Duo	5/7/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#2016)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#2016)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#291) (SHS Val#1766) "Mocana Cryptographic Library Version 5.4F."
189	SonicWALL Inc. 2001 Logic Drive San Jose, CA 95124 USA -Usha Sanagala TEL: 408-962-6248 FAX: 408-745-9300	**SonicOS 5.9.0 for NSA and TZ Series** **Version 5.9.0 (Firmware)**	Cavium Octeon Plus CN50XX; Cavium Octeon Plus CN56XX; Cavium Octeon Plus CN58XX	5/7/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1765)] "SonicWALL® Next-Generation Firewalls deliver superior gateway protection, inspection for SSL encrypted sessions, granular application intelligence and control. With SonicWALL Firewalls, IT can visualize applications running across a network-- allocating bandwidth for what's essential and limiting or blocking what's not." *05/17/12: Updated implementation information;*
188	Thales e-Security 2200 North Commerce Parkway Suite 200 Weston, FL 33326 USA -Joe Warren TEL: 321-264-2928	**Thales Datacryptor** **Version 5.0 (Firmware)**	PowerPC Core 405	4/30/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-384) (SHS Val#1764)] "The Thales Datacryptor protects the confidentiality and integrity of sensitive data travelling over public networks."
187	Chunghwa Telecom Co. Ltd. Telecommunication Laboratories 12, Lane 551, Min-Tsu Road SEC.5 Yang-Mei, Taoyuan, Taiwan 326 Taiwan, ROC -Yu-Ling Cheng TEL: +866-3-4245883 FAX: +886-3-4244147 -Ming-Hsin Chang TEL: +886-3-4245885 FAX: +886-3-4244147	**HiPKI SafGuard 1200 FPGA_lib** **Part # EP4CGX150DF27C7N**	N/A	4/30/2012	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1215)] "HiPKI SafGuard 1200 Cryptographic Library provides highly-secure cryptographic services,identity-based challenge-response authentication, and key storage for PKI Applications in the HiPKI Safguard 1200 HSM"
186	N/A N/A N/A, N/A N/A -N/A TEL: N/A FAX: N/A -N/A TEL: N/A FAX: N/A	**N/A** **Version N/A** **Part # N/A**	N/A	4/30/2012	"N/A"
185	Kaseya US Sales LLC 901 N. Glebe Road, Suite 1010 Arlington, VA 22203 USA -Bill Durant TEL: 415-694-5700	**Kaseya IT Systems Management Cryptographic Engine OSL** **Version 1.0**	Intel Core 2 Duo w/ MAC OS X v10.6.8; Intel Core 2 Duo w/ Red Hat Enterprise Linux v5.5 32 bit; Intel Core 2 Duo w/ Red Hat Enterprise Linux v5.5 64 bit; Intel Core 2 Duo w/ Windows Server 2008; Intel Core 2 Duo w/ Windows 7 (32 bit); Intel Core 2 Duo w/ Windows 7 (64 bit)	4/19/2012	**CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1989)] BlockCipher_No_df: (, AES-256) (AES Val#1989)] "The Kaseya IT Systems Management Platform uses encryption to secure communications between its client and server components. It is an ideal Systems Management solution for government systems and other infrastructures requiring a high assurance implementation." *04/27/12: Updated implementation information;*
184	Red Hat Inc. 1801 Varsity Drive Raleigh, NC 27606 USA	**NSS library softtoken** **Version 3.12.9**	Intel x86 (64-bit) w/ Red Hat Enterprise Linux 6.2	4/19/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1742)]

	-Irina Boverman TEL: 978 392 1000				"User space library provided by the Mozilla Foundation for general purpose cryptographic usage. The testing covers the cipher implementations found in the softtoken component of the NSS library."
183	Red Hat Inc. 1801 Varsity Drive Raleigh, NC 27606 USA -Irina Boverman TEL: 978 392 1000	**NSS library softtoken** **Version 3.12.9**	AMD Opteron (64-bit) w/ Red Hat Enterprise Linux 6.2	4/19/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1741)] "User space library provided by the Mozilla Foundation for general purpose cryptographic usage. The testing covers the cipher implementations found in the softtoken component of the NSS library."
182	Marvell Semiconductor Inc. 5488 Marvell Lane Santa Clara, CA 95054 USA -Minda Zhang TEL: (508) 573-3255 FAX: (508) 573-3311	**Armada PXA-610** **Version 2.1.9 (Firmware)** **Part # Armada PXA-610**	Armada PXA-610	4/9/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1737)] "Armada PXA-610 is an application processor SoC (http://www.marvell.com/application processors/armada-600/). It has a dedicated security hardware module, known as WTM, that runs secure firmware kernel to perform device trusted boot, access control, authentication, key management, DRM, disk encryption, and FIPS certified cryptographic operations."
181	Pitney Bowes Inc. 37 Executive Drive Danbury, CT 06810 USA -Dave Riley TEL: 203-796-3208	**appPrng** **Version 02000004 (Firmware)**	ARM 7 TDMI	4/9/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1733)] "The Pitney Bowes Cygnus X-3 Hardware Security Module (HSM) employs strong cryptographic and physical security techniques for the protection of funds in Pitney Bowes Postage systems."
180	Curtiss-Wright Controls, Inc. 2600 Paramount Place, Suite 200 Fairborn, OH 45324 USA -Paul Davis TEL: 937-252-5601 x:1261 FAX: 937-252-2729 -Matt Young TEL: 937-252-5601 x:1363 FAX: 937-252-2729	**Curtiss-Wright Controls FSM Cryptographic Engine** **Part # 1.11**	N/A	4/2/2012	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (HMAC Val#1191)] "The Flash Storage Module (FSM) AES cryptographic engine uses 256-bit encryption keys and performs real-time encryption of all data written to or read from solid state drives. The FSM cryptographic engines provides maximum data-at-rest security in commercial and military applications."
179	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**IOS-XE Cryptographic Implementation** **Version 3.3(1)SG (Firmware)**	Freescale MPC8572E	4/2/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1977)] "IOS-XE Firmware cryptographic implementations used within Cisco devices to provide cryptographic functions." *06/04/12: Added new tested information; 08/03/12: Updated implementation information;*
178	Certicom Corp. 4701 Tahoe Blvd. Building A Missisauga, ON L4W 0B5 Canada -Certicom Sales TEL: 905-507-4220 FAX: 905-507-4230 -Kris Orr TEL: 289-261-4104 FAX: 905-507-4230	**Security Builder FIPS Core** **Version 6.0.2**	64-bit Intel Core i5-2300 w/ Red Hat Linux 5.6; 64-bit Intel Core i5-2300 w/ Windows 7	3/26/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1729)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1189)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1975)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-256) (P-384: , SHA-384) (P-521: , SHA-512) (ECDSA Val#285) (SHS Val#1729) "Security Builder FIPS Core provides application developers with cryptographics tools to easily integrate encryption, digital signatures and other security mechanisms into C-based apps for FIPS 140-2 and Suite B security. It can also be used with Certicom's PKI, IPSec SSL and DRM modules."
177	ClevX LLC 9306 NE 125th Street Kirkland, WA 98034 USA	**Random Number Generator** **Version v2 (Firmware)**	Microchip 16LF1825	3/21/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1728)] "Components are part of firmware of the iStorage datashur encrypted drive. A random number

	-Simon Johnson TEL: 253-232-2366				generator (RNG) is implemented consisting of a non-deterministic source of entropy that becomes the seed for the deterministic hash_DRBG algorithm. The RNG is used for creating encryption keys used in the AES hashing function implemented in a 2nd chip."
176	Diversinet Corp. 2235 Sheppard Avenue East Atria II Suite 1700 Toronto, Ontario M2J5B5 Canada -Salah Machani TEL: 4167562324 Ext. 321 FAX: 4167567346 -Hussam Mahgoub TEL: 4167562324 Ext. 222 FAX: 4167567346	**Diversinet Java Crypto Module for Mobile** **Version 2.0**	Qualcomm Snapdragon w/ Android OS v2.2	3/16/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#1966)] "Diversinet Java Crypto Module for Mobile is shipped with Diversinet MobiSecure Client SDK for Java based run-time environments on Smartphones and tablets including, Android OS-, BlackBerry OS- and Java ME MIDP-based. The Crypto Module implements several cryptography algorithms including Triple DES, AES, SHA, HMAC, DRBG and RSA."
175	Diversinet Corp. 2235 Sheppard Avenue East Atria II Suite 1700 Toronto, Ontario M2J5B5 Canada -Salah Machani TEL: 4167562324 Ext. 321 FAX: 4167567346 -Hussam Mahgoub TEL: 4167562324 Ext. 222 FAX: 4167567346	**Diversinet Java Crypto Module** **Version 2.0**	Intel Xeon E5530 w/ Windows Server 2008 RC2 (64bit) and JDK 1.6	3/16/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#1965)] "Diversinet Java Crypto Module is a JCA (Java Cryptography Architecture) Provider shipped with Diversinet MobiSecure Products. The Crypto Module implements several JCE (Java Cryptography Extension) algorithms including Triple DES, AES, SHA, HMAC, DRBG and RSA. The Crypto Module is packaged in a signed Java Archive (JAR) file."
174	Thales e-Security Meadow View House Crendon Industrial Estate Long Crendon Aylesbury, Buckinghamshire HP18 9EQ U.K. -Datacryptor-Certifications TEL: +44 (0)1844 201800 FAX: +44 (0)1844 208550	**Datacryptor Dual_EC_DRBG** **Version V1.8 (Firmware)**	Motorola Coldfire processor - single core	3/16/2012	**Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-384: SHA-384) (SHS Val#1717) "Thales e-Security implements this algorithm for applications running on its Secure Generic Sub System (SGSS) providing secure cryptographic resources to the Datacryptor® 2000 and the Datacryptor® Advanced Performance network encryption products for IP, Frame Relay and Link (including E1/T1) networks." *09/10/12: Updated vendor information;* *09/17/12: Updated vendor information;*
173	Hagiwara Solutions Co., Ltd. 2-5-12 Nishiki Naka-ku, Nagoya, Aichi 460-0003 Japan -Yoshihiro Kito TEL: +81-53-455-6700 FAX: +81-53-455-6701 -Masaki Takikawa TEL: +81-53-455-6700 FAX: +81-53-455-6701	**TRUESSD Crypto Engine - Hash_DRBG** **Version 1.0 (Firmware)**	HS200S-F	3/7/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256) (SHS Val#1714)] "The TRUESSD Crypto Engine is the hardware-based data encryption and decryption engine. This cryptographic engine provides the secure data protection found in Hagiwara Solutions storage products."
172	RSA The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Damon Hopley TEL: 781-515-6355	**RSA BSAFE Crypto-C Micro Edition (ME)** **Version 3.0.0.15**	Intel Celeron M(Dothan) w/ NetBSD 2.1; PMC Sierra RM7035C w/ NetBSD 2.1	3/7/2012	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1177)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#281) (SHS Val#1713) "RSA BSAFE® Crypto-C ME software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. The software supports a wide range of industry standard encryption algorithms offering developers the flexibility to choose the appropriate option to meet their requirements." *03/21/12: Added new tested information;*
171	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA	**Brocade ServerIron ADX** **Version 12.3.03 (Firmware)**	Freescale MPC8572E	2/23/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1703)] "Our Goal is to receive FIPS 140-2 SL2 certification on the above platforms. For this, we

	-Michael Williamson TEL: 408 333 5691 -Farzam Tajbakhsh TEL: 408 333 7443				have identified the cryptographic boundary to be the management module (with access to E2PROM on backplane). The software is to be updated to use NSS/NSPR as the cryptographic engine."
170	Entrust Inc. One Lincoln Centre 5400 LBJ Freeway Suite 1340 Dallas, TX 75240 USA -Entrust Sales TEL: 888-690-2424	**Entrust Authority™ Java Toolkit** **Version 8.0**	Intel Core 2 Duo E8400 w/ Microsoft Windows Server 2008 R2 with Oracle J2RE 6; Intel Core 2 Duo E8400 w/ Microsoft Windows Server 2008 R2 with Oracle J2RE 7	2/21/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1700)] "The Java toolkit is an implementation of cryptographic functions accessible by an object-oriented API. Depending on configuration, the algorithms may be implemented in software, hardware, or both. The industry standard Cryptopki API from PKCS #11, is used as the interface to hardware-based cryptographic modules."
169	FRAMA AG Unterdorf Lauperswil, Bern CH-3438 Switzerland -Beat Waelti TEL: +41-34-49698-98 FAX: +41-34-49698-00	**PSD-II by FRAMA** **Version V2.0.4 (Firmware)** **Part # FRM-II Version 1.2**	firmware: running on built-in Fujitsu MB91302APM1R micro controller	2/21/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1699)] "The PSD-II (Postal Security Device-II) is a hardware/firmware cryptographic module to be used in automated franking machines."
168	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**OpenSSL** **Version OpenSSL-fips-2.0-test-20110925**	Freescale MPC8347 w/ Linux 2.6.36	1/26/2012	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1928)] "All cryptographic implementations are in software by way of OpenSSL, whose version is 1.1.0-SNAP-20110615." *11/01/12: Updated vendor information;*
167	Entrust Inc. One Lincoln Centre 5400 LBJ Freeway Suite 1340 Dallas, TX 75240 USA -Entrust Sales TEL: 888-690-2424	**Entrust Authority™ Security Kernel** **Version 8.1sp1**	Intel Core 2 Duo E8400 w/ Windows Server 2008 R2 Enterprise Edition	1/19/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1689)] "The Security Kernel is a C++ implementation of cryptographic functions accessible by an object-oriented API. Depending on configuration, the algorithms may be implemented in software, hardware or both. The industry standard Cryptoki API from PKCS #11, is used as the interface to hardware-based cryptographic modules."
166	Catbird Networks Inc. 1800 Green Hills Road, Suite 113 Scotts Valley, CA 95066 USA -Michael Berman TEL: 831-440-8152	**Catbird vSecurity Crypto Module v1.0** **Version v1.0**	Intel Core i5 with AES-NI w/ CentOS 6.0	1/19/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1688)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1157)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1922)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1922)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#274) (SHS Val#1688) "The cryptographic module used by Catbird's comprehensive security and compliance solutions for virtualized data centers."
165	Red Hat Inc. 1801 Varsity Drive Raleigh, NC 27606 USA -Robert Relyea TEL: 650-254-4236	**Network Security Services (NSS) Cryptographic Module** **Version 3.12.9.1**	Intel Core i7 w/ Red Hat Enterprise Linux v6.2 64-bit; Intel Core i7 with AES-NI w/ Red Hat Enterprise Linux v6.2 64-bit; Intel Core i7 w/ Red Hat Enterprise Linux v6.2 32-bit	1/19/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1675)] "Network Security Services (NSS) is a set of open source C libraries designed to support cross-platform development of security-enabled applications. NSS implements major Internet security standards. NSS is available free of charge under a variety of open source compatible licenses. See http://www.mozilla.org/projects/security/pki/nss/." *01/26/12: Updated implementation information;*
164	ClevX LLC 9306 NE 125th Street Kirkland, WA 98034 USA	**Random Number Generator** **Version v2 (Firmware)**	Microchip 16LF1825	1/5/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1682)] "Components are part of firmware that make up the SDG family of encrypted drives. A random

	-Simon Johnson TEL: 253-232-2366				number generator (RNG) is implemented consisting of a non-deterministic source of entropy that becomes the seed for the deterministic hash_DRBG algorithm. The RNG is used for creating encryption keys used in the AES hashing function implemented in a 2nd chip."
163	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Mark Hanson TEL: +1 651-628-1633 FAX: +1 651-628-2706 -Luis Chirinos TEL: +1 408-346-3784	**RSA Bsafe CryptoJ** **Version 4.1 (Firmware)**	Intel Xeon E5540 2.53GHz Quad Core; Intel Celeron E3400 2.60GHz Dual Core;	12/29/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1137)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#266) (SHS Val#1666) "McAfee Firewall Enterprise Control Center simplifies the management of multiple McAfee Firewall Enterprise appliances. Control Center enables centralized management and monitoring of the McAfee Firewall Enterprise solutions, allowing network administrators to centrally define firewall policy, deploy updates and inventory their firewall products."
162	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -Mark Hanson TEL: +1 651-628-1633 FAX: +1 651-628-2706 -Luis Chirinos TEL: +1 408-346-3784	**RSA Bsafe CryptoJ** **Version 4.1**	Intel Xeon w/ CGLinux	12/29/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1152)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#273) (SHS Val#1683) "McAfee Firewall Enterprise Control Center simplifies the management of multiple McAfee Firewall Enterprise appliances. Control Center enables centralized management and monitoring of the McAfee Firewall Enterprise solutions, allowing network administrators to centrally define firewall policy, deploy updates and inventory their firewall products."
161	Cummings Engineering Consultants Inc. 145 S. 79th St., Suite 26 Chandler, AZ 85226 USA -Darren Cummings TEL: 480-809-6024	**Cummings Engineering's Secure Mobility Suite B Crypto Module v1.0** **Version v1.0**	TI OMAP 3 w/ Linux 3.0.4; Intel Pentium T4200 w/ Android 2.2; Qualcomm QSD 8250 w/ Android 2.2; Intel Pentium T4200 w/ Ubuntu 10.04; Intel Celeron (64 bit mode) w/ Microsoft Windows 7; Intel Core i5 (with AES-NI) w/ Android 2.2; Intel Core i5 (with AES-NI) (64 bit mode) w/ Microsoft Windows 7; Intel Core i5 (with AES-NI) w/ Fedora 14	1/26/2012	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1692)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1151)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1927)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1927)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#276) (SHS Val#1692) "The cryptographic module used by the Cummings Engineering suite of products which allow for efficient and effective deployment of robust secure communications capability on commercial off the shelf (COTS) devices, such as Smartphones and Tablets, as well as speciality communications devices." *02/01/12: Added new tested information;*
160	RSA The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Damon Hopley TEL: 781-515-6355	**RSA BSAFE® Crypto-J JSAFE and JCE Software Module** **Version 6.0**	Intel T7300 Core 2 Duo w/ Android 2.2 ARM (32-bit) JRE 6.0; AMD Athlon 64 X2 Dual-Core Processor 3800+ w/ Microsoft Windows 7 (64-bit) with Sun JRE 6.0	12/29/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1148)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#271) (SHS Val#1678) "RSA BSAFE Crypto-J security software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. It supports a wide range of industry standard encryption algorithms offering Java developers the flexibility to choose the option most appropriate to meet their requirements."

					01/05/12: Updated implementation information;
159	Motorola Solutions Inc. 1301 East Algonquin Road Schaumburg, IL 60196 USA -Kirk Mathews TEL: 847-576-4101	**Motorola Solutions PIKE2 DRBG** **Version R02.01.00 (Firmware)** **Part # 51009397004**	Motorola PIKE2 51009397004	12/16/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#1901)] "The PIKE2 cryptographic processor is used in security modules embedded in Motorola Solutions security products." *12/23/11: Updated implementation information;*
158	Covia Labs 465 Fairchild Dr. Suite 130 Mountain View, CA 94043 USA -Bruce Bernstein TEL: 650-351-6444 FAX: 650-564-9740	**CCCM Library** **Version 2.0**	Intel Pentium 4 w/ Ubuntu Linux version 11; AMD E-350 w/ Red Hat Enterprise Linux version 5.8	12/13/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1136)] "The cccmLib is a dynamically linked library whose sole use is to serve as a cryptographic engine to the Covia Labs Connector application. In particular the cccmLib will provide the underlying functionality needed to implement secured communications and an encrypted file system." *08/21/12: Added new tested information;*
157	OpenSSL Software Foundation Inc. 1829 Mount Ephraim Road Adamstown, MD 27101 USA -Steve Marquess TEL: 877-673-6775	**OpenSSL FIPS Object Module** **Version 2.0**	Qualcomm QSD 8250 (HTC Desire; ARMv7) w/ Android 2.2; Qualcomm QSD 8250 (Dell Streak; ARMv7) w/ Android 2.2; Intel Itanium 2 (64 bit mode) w/ HP-UX 11i; Intel Itanium 2 (32 bit mode) w/ HP-UX 11i; Freescale PowerPC32-e300 w/ Linux 2.6.33; TI OMAP 3530 (ARMv7) w/ Android 2.2; Intel Pentium (R) T4200 w/ Ubuntu 10.04; ARM Limited ARM922T (ARMv4) w/ uCLinux 0.9.29; NVIDIA Tegra 250 T20 (Motorola Xoom, ARMv7) w/ Android 3.0; Intel Core i5 with AES-NI (64 bit mode) w/ Fedora 14; Intel Core i5 with AES-NI (32 bit mode) w/ Ubuntu 10.04; Intel Celeron (32 bit mode) w/ Microsoft Windows 7; TI TNETV1050 w/ VxWorks 6.8; PowerPC e300c3 w/ Linux 2.6.27; Intel Pentium T4200 (64 bit mode) w/ Cascade Server 6.10; Intel Pentium T4200 (32 bit mode) w/ Cascade Server 6.10; Intel Pentium 4 (64 bit mode) w/ Microsoft Windows 7; TI AM3703CBP w/ Linux 2.6.32; Broadcom BCM11107 (ARMv6) w/ Linux 2.6;TI TMS320DM6446 (ARMv7) w/ Linux 2.6; Intel Xeon 5675 (x86) with AES-NI (32 bit mode) w/ Oracle Solaris 11; Intel Xeon 5675 (x86) (64 bit mode) w/ Oracle Solaris 11; Intel Pentium T4200 (x86) (32 bit mode) w/ Ubuntu 10.04; Intel Xeon 5675 (x86) (32 bit mode) w/ Oracle Solaris 11; Intel Xeon 5675 (x86) with AES-NI (64 bit mode) w/ Oracle Solaris 11; Intel Pentium T4200 (x86) (64 bit mode) w/ Ubuntu 10.04; SPARC-T3 (SPARCv9) (32 bit mode) w/ Oracle Solaris 10; SPARC-T3 (SPARCv9) (64 bit mode) w/ Oracle Solaris 10; Intel Xeon 5675 (x86) (64 bit mode) w/ Oracle Linux 5; Intel Xeon 5675 with AES-NI (64 bit mode) w/ Oracle Linux 5; Intel Xeon 5675 (64-bit mode) w/ Oracle Linux 6; Intel Xeon 5675 with AES-NI (64-bit mode) w/ Oracle Linux 6; SPARC-T3 (SPARCv9) (32-bit mode) w/ Oracle Solaris 11; SPARC-T3 (SPARCv9) (64-bit mode) w/ Oracle Solaris 11; NVIDIA Tegra 250 T20 (ARMv7) w/ Android 4.0; Freescale PowerPC-e500 w/ Linux 2.6; TI C64x+ w/ DSP Media Framework 1.4; TI OMAP 3 (ARMv7) with NEON w/ Android 4.0	11/29/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1655)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1126)] **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1884)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1884)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Enabled and Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#264) (SHS Val#1655) "The OpenSSL FIPS Object Module is a full featured general purpose cryptographic library that is distributed in source code form under an open source license. It can be downloaded from www.openssl.org/source/." *12/14/11: Updated implementation information;* *12/21/11: Added new tested information;* *01/26/12: Added new tested information;* *01/30/12: Added new tested information;* *02/27/12: Added new tested information;* *03/20/12: Added new tested information;* *04/02/12: Updated implementation information;* *04/24/12: Updated implementation information;* *04/26/12: Added new tested information;* *05/31/12: Added new tested information;* *06/08/12: Updated implementation information;* *06/29/12: Updated implementation informaton;* *07/02/12: Added new tested information;*
156	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054 USA -David Gerendas TEL: 949-860-3369 FAX: 949-297-5575	**McAfee Endpoint Encryption Client Cryptographic Library** **Version 6.1.3**	Intel Core i3 w/ Windows XP 32-bit; Intel Core i7 with AES-NI w/ Windows Vista 64-bit; Intel Core i5 with AES-NI w/ Windows Vista 32-bit; Intel Core i7 with AES-NI w/ Windows 7 64-bit; Intel Core i3 w/ Windows 7 64-bit; Intel Core i5 with AES-NI w/ Windows 7 32-bit; Intel Core i7 with AES-NI w/ McAfee Endpoint Encryption Preboot OS; Intel Core i5 with AES-NI w/ McAfee Endpoint Encryption Preboot OS; Intel Core i3 w/ McAfee Endpoint Encryption Preboot OS	11/29/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (HMAC Val#1124)] "This Cryptographic algorithm module provides cryptographic functionality for McAfee's Endpoint Encryption product range."
155	Chunghwa Telecom Co. Ltd. Telecommunication Laboratories	**HiCOS PKI Native Smart Card v3.3** **Version 1.0 (Firmware)**	Renesas AE-5 Series Processor	11/22/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1649)]

	12, Lane 551, Min-Tsu Road SEC.5 Yang-Mei, Taoyuan, Taiwan 326 Taiwan, ROC -Yeou-Fuh Kuan TEL: +886-3-424-4333 FAX: +886-3-424-4129 -Char-Shin Miou TEL: +886-3-424-4381 FAX: +886-3-424-4129				"HiCOS PKI Native Smart Card supports SHA-1, SHA-256, SHA-384, SHA-512, Hash-DRBG, 3DES-3Key-MAC, 3DES-3Key encrypt/decrypt, RSA 1024/2048 encrypt/decrypt, RSA digital signature generation/verification and APDU command/response encryption and/or MAC."
154	Motorola Solutions Inc. 1301 East Algonquin Road Schaumburg, IL 60196 USA -Kirk Mathews TEL: 847-576-4101	**Motorola Solutions µMace DRBG** **Version R00.00.01_SP_800_90_DRBG (Firmware)** **Part # AT58Z04**	Motorola µMace AT58Z04	11/17/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#1876)] "The µMace cryptographic processor is used in security modules embedded in Motorola Solutions security products."
153	Blue Coat Systems Inc. 420 North Mary Avenue Sunnyvale, California 94085-4121 USA -Wendi Ittah TEL: (703) 399-0535 -Tammy Green TEL: (801) 999-2973	**SGOS 6.1 Cryptographic Library** **Version 2.1.1 (Firmware)**	AMD Opteron Shanghai Quad Core; Intel Xeon Lynnfield X3450 Quad Core; Intel Clarkdale i3-540 Dual Core; Intel Clarkdale G1101; Intel P4 Xeon; VIA Nano; Intel Celeron; AMD Opteron Istanbul 6 Core processor	11/17/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1648)] "The SGOS 6.1 is a proprietary operating system developed specifically for use on a series of hardware appliances that serve as an Internet proxy and Wide Area Network (WAN) optimizer. The series of appliances supported are 510 Series, 600 Series, 810 Series, 900 Series and 9000 Series." *01/30/12: Made correction to the implementation information;*
152	Imation Corp. Discovery Bldg. 1A-041 Oakdale, MN 55128 USA -Larry Hamid TEL: 408-737-4308	**Imation Crypto Library - P** **Version 1.0 (Firmware)** **Part # 294.010**	PS2251-85	11/17/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (HMAC Val#1119)] "The Imation Secure Flash Drive includes a high-speed hardware-based AES cryptography engine for encrypting and decrypting NAND flash and RAM buffers via USB. It also includes RSA, HMAC, SHA, and DRBG algorithms." *11/22/11: Updated vendor information;* *08/13/12: Updated vendor and implementation information;*
151	IBM Corporation 2455 South Road Poughkeepsie, New York 12601-5400 USA -William Penny TEL: 1-845-435-3010 -Jim Sweeny TEL: 1-845-435-7453	**IBM z/OS(r) Cryptographic Services ICSF PKCS #11** **Version OA36882** **Part # 5694-A01**	IBM zEnterprise 196 (z196) w/ IBM z/OS® V1.13	11/9/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1641)] "ICSF is a software element of z/OS that works with hardware cryptographic features and the Security Server (RACF) to provide secure, high-speed cryptographic services in the z/OS environment. ICSF, which runs as a started task, provides the application programming interfaces by which applications request the cryptographic services." *11/15/11: Update implementation information;* *01/27/12: Updated implementation information;*
150	Cubic Global Tracking Solutions 1919 Gallows Road, Suite 600 Vienna, VA 22182 USA -Paul Berenberg TEL: 650-887-0805 -Brenda Perrow TEL: 858-505-2355	**mist® DRBG** **Version 8013 (Firmware)** **Part # Texas Instruments CC2530**	Texas Instrument CC2530	11/9/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#1863)] "Universal DRBG implementation for mist™ mesh network" *11/15/11: Update implementation and vendor information;* *01/23/14: Updated vendor and implementation information;*
149	Centrify Corporation 785 N Mary Avenue Suite 200 Sunnyvale, CA 94085 USA -Keith Moreau TEL: 415 412 6482	**Centrify Cryptographic Module** **Version 1.0**	Intel Core i7 2GHz w/ Mac OS 10.7	10/31/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1861)] "The Centrify Cryptographic Module provides the cryptographic services for all of Centrify's products."
148	NetLogic Microsystems Inc. 3975 Freedom Circle Santa Clara, CA 95054 USA	**netl_random_drbg** **Version 1.0**	XLP A2 w/ Linux 2.6.x	10/18/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1842)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1842)]

	-Mark Litvack TEL: 408-454-3296				"XLP multi-core processors offer full cache coherency and can deliver an unprecedented 160Gbps throughput and 240 million packets-per-second of application performance for next-generation 3G/4G mobile wireless infrastructure, enterprise, storage, security, metro Ethernet, edge and core infrastructure network applications."
147	Check Point Software Technologies Ltd. 9900 Belward Campus Dr. Suite 250 Rockville, MD 20850 USA -David Abrose TEL: +972 37534561 -Malcolm Levy TEL: +972 37534561	**VSX** **Version R67.10 with R7x hotfix (Firmware)**	Intel Xeon	10/18/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1617)] "Check Point VPN-1 Power VSX is a virtualized security gateway that allows virtualized enterprises and managed service providers to create up to 250 virtual systems (firewall, VPN, and intrusion prevention functionality within a virtual network environment) on a single, highly scalable hardware platform."
146	Check Point Software Technologies, Ltd. 9900 Belward Campus Dr. Suite 250 Rockville, MD 20850 USA -David Abrose TEL: +972 37534561 -Malcolm Levy TEL: +972 37534561	**Provider-1** **Version R71 with R7x hotfix (Firmware)**	Intel Xeon	10/18/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1616)] "Smart-1 50/150 Provider-1 Enterprise Edition brings a highly scalable multi-domain management solution to high-end enterprise customers. It includes a multi-domain management blade for management of up to 50 separate security domains, with separate management access rights while sharing global objects and policies."
145	Check Point Software Technologies Ltd. 9900 Belward Campus Dr. Suite 250 Rockville, MD 20850 USA -David Abrose TEL: +972 37534561 -Malcolm Levy TEL: +972 37534561	**Security Management** **Version R71 with R7x hotfix (Firmware)**	Intel Xeon	10/18/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1614)] "Smart-1 Security management appliances, delivers a unified solution for network, IPS and endpoint Policy Management with easy log access and performance capabilities for the most demanding environments."
144	Athena Smartcard Inc. 20380 Town Center Lane, Suite 240 Cupertino, CA 95014 USA -Ian Simmons TEL: (408) 865-0112 FAX: (408) 865-0333	**Athena OS755 DRBG Component** **Version S1.0 (Firmware)** **Part # STMicroelectronics ST23**	STMicroelectronics ST23	10/13/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1609)] "Athena OS755 is a GlobalPlatform Java Card smart card operating system implementing AES, TDES, DRBG, SHA-1/SHA-2, RSA, SP 800-56A KAS (ECC CDH Primitive only) and ECDSA2."
143	RSA RSA, The Security Division of EMC Suntec Tower 4 #31-01 Singapore, 038986 Singapore -Sandra Tong TEL: +852 9882 1502 -Young Son TEL: +82 10 6700 6735	**RSA BSAFE Crypto-C Micro Edition for VxWorks** **Version 3.0.0.1**	ARM9 w/ VxWorks built with Wind River Workbench 3.0	10/13/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#252) (SHS Val#1605) "Crypto-C ME is evaluated as a multi-chip, standalone module. The physical cryptographic boundary of the module is the case of the general-purpose computer or mobile device, which encloses the hardware running the module."
142	Inside Secure 41 Parc Club du Golf 13856, Aix-en-Provence France -David Cunningham TEL: +44 135 580 3554 FAX: +44 135 524 2743	**VaultIC460/440/420** **Version 1.2.1 (Firmware)** **Part # AT90SO128**	Inside Secure AT90SO128	10/13/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#1822)] "VaultIC^TM are security modules designed to secure applications such as anti-cloning, physical access control, personal access control for multimedia and web applications, hardware authentication, user strong authentication, SSL support, PKCS#11 to Microsoft (R) CSP applications, PKI, DRM, trusted computing and IP protection." *05/10/12: Updated implementation information;*
141	Utimaco Safeware AG Germanusstraße 4	**CryptoServer Se DRBG**	Texas Instruments TMS320C6416T	10/13/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1498

	Aachen, 52080 Germany -Dr. Gesa Ott TEL: ++49 241-1696-200 FAX: ++49 241-1696-190	**Version util3.0.1.2_smos3.1.1.0 (Firmware)**			)] "Safeguard® CryptoServer Se is an encapsulated, tamper-protected hardware security module which provides secure cryptographic services like encryption or decryption, hashing, signing and verification of data, random number generation, on-board secure key generation, key storage, and further key management functions."
140	Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 USA -Sonu Shankar TEL: 408-424-7279	**Cisco IOS** **Version 15.0(1)SY2(Firmware)**	Freescale MPC8572E	10/6/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1816)] "IOS Firmware cryptographic implementations used within Cisco devices to provide cryptographic functions." *04/10/12: Updated implementation information; 12/07/12: Updated implementation information;*
139	Voltage Security, Inc. 20400 Stevens Creek Blvd. Cupertino, CA 95014 USA -Luther Martin TEL: 650-543-1280 FAX: 650-543-1279 -Branislav Meandzija TEL: 408-886-3200 FAX: 408-886-3201	**Voltage IBE Cryptographic Module for z/OS** **Version 4.0**	IBM z10; 2097 / E26; X2 co-processor crypto-card w/ z/OS PUT1106 / RSU1108	10/6/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256 , SHA-512) (SHS Val#1590)] "Voltage IBE Cryptographic Module for z/OS implements the following algorithms: DSA; TDES; AES (ECB, CBC, CFB, OFB, FPE); DRNG; DRBG; SHA (1, 224, 256, 384, 512); HMAC; CMAC; RSA; DH; BF IBE; BB1 IBE; MD; DES"
138	Atos Worldline SA/NV Haachtsesteenweg 1142 Brussels, 1130 Belgium -Filip Demaertelaere TEL: +32 2 727 61 67 -Sam Yala TEL: +32 2 727 61 94	**ACC (Atos Worldline Cryptographic Core)** **Part # 1.0**	N/A	10/6/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1589)] "The ACC is the cryptographic engine of Atos Wordline Hardware Security Module. The ACC makes use of dedicated hardware accelerators."
137	RSA RSA, The Security Division of EMC Suntec Tower 4 #31-01 Singapore, 038986 Singapore -Sandra Tong TEL: +852 9882 1502 -Young Son TEL: +82 10 6700 6735	**RSA BSAFE Crypto-C Micro Edition for pSOS** **Version 3.0.0.1**	ARM9 w/ pSOS built with ARM SDT 2.51	9/30/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#249) (SHS Val#1587) "Crypto-C ME is evaluated as a multi-chip, standalone module. The physical cryptographic boundary of the module is the case of the general-purpose computer or mobile device, which encloses the hardware running the module."
136	ARX (Algorithmic Research) 10 Nevatim St Petah-Tikva, Israel 49561 Israel -Ezer Farhi TEL: +972-39279529 FAX: +972-39230864	**PrivateServer** **Version 4.8 (Firmware)**	Intel® Pentium Dual-Core	9/30/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#249) (SHS Val#1587) "PrivateServer performs sensitive cryptographic operations internally in a tamper-proof, high performance device. PrivateServer is configured as a network server or as a cryptographic backend to a host"
135	N/A	**N/A**	N/A	9/30/2011	N/A
134	N/A	**N/A**	N/A	9/30/2011	N/A
133	Research in Motion 295 Philip Street Waterloo, Ontario N2L 3W8 Canada -Security Certifications Team TEL: (519) 888-7465x72921 FAX: (519) 888-9852	**BlackBerry Cryptographic Kernel** **Version 3.8.7.1 (Firmware)**	Qualcomm MSM8655 Processor	9/30/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1800)] "The BlackBerry Cryptographic Library is the firmware module that provides the core cryptographic functionality to BlackBerry Smartphones."
132	Research in Motion	**BlackBerry Cryptographic Kernel**	Qualcomm MSM8655 Processor	9/30/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not

	295 Philip Street Waterloo, Ontario N2L 3W8 Canada -Security Certifications Team TEL: (519) 888-7465x72921 FAX: (519) 888-9852	**Version 3.8.7.0 (Firmware)**			Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1798)] "The BlackBerry Cryptographic Kernel is the firmware module that provides the core cryptographic functionality to BlackBerry Smartphones."
131	Ciena Corporation 1201 Winterson Road Linthicum, MD 21090 USA -Patrick Scully TEL: 613-670-3207	**565/5100/5200 QOTR/E Cryptography Engine** **Version 1.0 (Firmware)**	MPC8314e	9/20/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1682)] BlockCipher_No_df: (, AES-256) (AES Val#1682)] "The 565/5100/5200 Advanced Services Platform offers an integrated transport encryption solution providing an ultra-low latency and protocol-agnostic wirespeed encryption service for use in small to large enterprises or datacenters and also offered through service providers as a differentiated managed service."
130	Ciena Corporation 1201 Winterson Road Linthicum, MD 21090 USA -Patrick Scully TEL: 613-670-3207	**565/5100/5200 SP Cryptography Engine** **Version 1.0 (Firmware)**	MPC8270	9/20/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1682)] BlockCipher_No_df: (, AES-256) (AES Val#1682)] "The 565/5100/5200 Advanced Services Platform offers an integrated transport encryption solution providing an ultra-low latency and protocol-agnostic wirespeed encryption service for use in small to large enterprises or datacenters and also offered through service providers as a differentiated managed service."
129	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -M.K Whitlock TEL: 919-392-9396	**IOS** **Version 15.1(3)T2 (Firmware)**	Freescale MPC8358E	9/20/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1793)] "The Cisco 800 Series of integrated Services Routers intelligently embed data and security into a single, resilient system for fast, scalable delivery of mission-critical business applications from small offices to demanding enterprise environments."
128	Thales e-Security Inc. 2200 North Commerce Parkway Suite 200 Weston, Florida 33326 USA -Robert Burns TEL: +19548886215 -Alan Brown TEL: +14084577706	**Thales e-Security keyAuthority® - Random bit generator library** **Version 3.12.6**	Intel Xeon Dual Core w/ Linux - CentOS 5.2	9/20/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1573)] "An implementation of the SP800-90 random bit generator for providing cryptographically secure random numbers to all libraries in the Thales e-Security keyAuthority®." *10/06/11: Update implementation information; 10/18/11: Update implementation information; 12/07/11: Updated implementation information;*
127	Certicom Corp. 4701 Tahoe Blvd. Building A Mississauga, ON L4W 0B5 Canada -Certicom Sales TEL: 905-507-4220 FAX: 905.507.4230 -Kris Orr TEL: 289.261.4104 FAX: 905.507.4230	**Security Builder FIPS Core** **Version 6.0**	64-bit Intel Core i5-2300 w/ RedHat Linux 5.6; 32-bit Intel Core i7 w/ RedHat Linux 5.6; 32-bit Intel Pentium III w/ QNX 6.5; ARM Cortex A9 MPCore w/ QNX 6.6; Intel Core 2 Duo w/ Mac OS X 10.5; 32-bit Intel Core i5-2300 w/ Windows 7	9/20/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1571)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1054)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1789)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-256) (P-384: , SHA-384) (P-521: , SHA-512) (ECDSA Val#242) (SHS Val#1571) "Security Builder FIPS Core provides application developers with cryptographics tools to easily integrate encryption, digital signatures and other security mechanisms into C-based apps for FIPS 140-2 and Suite B security. It can also be used with Certicom's PKI, IPSec SSL and DRM modules." *10/01/11: Update implementation information; 01/19/12: Added new tested information;*
126	Hughes Network Systems LLC. 11717 Exploration Lane Germantown, MD 20876 USA -Tim Young TEL: 301-428-1632	**Hughes SPACEWAY Crypto Kernel** **Version 1.0 (Firmware)**	AMCC PowerPC (32-bit); Intel Pentium 4 (32-bit); Intel dual-core Xeon (32-bit);	9/20/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (HMAC Val#)] "The HSCK v1.0 is a firmware library that provides cryptographic functionality for securing communications over the Hughes SPACEWAY Satellite communication systems. SPACEWAY enables a full-mesh digital network that

					interconnects with a wide range of end-user equipment and systems."
125	Hitachi Solutions, Ltd. 4-12-7,Higashishinagawa Shinagawa-ku, Tokyo 140-0002 Japan -Applied Security Development Department TEL: +81-3-5780-2111	**HIBUN Cryptographic Module for User-Mode** **Version 1.0 Rev. 2**	Intel(R) Core(TM) i5-650 w/ Windows XP Professional; Intel(R) Core(TM) i5-650 w/ Windows Vista Ultimate; Intel(R) Core(TM) i5-650 w/ Windows 7 Ultimate; Intel(R) Core(TM) i5-650 w/ Windows 7 Ultimate 64bit; Intel(R) Core(TM) i5-650 w/ Linux Kernel 2.6 (Fedora 12)	8/30/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#1045)] "HIBUN Cryptographic Module for User-Mode is the cryptographic library module which operates on the Windows User-Mode and Linux User-Mode."
124	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -Vincent Moscaritolo TEL: 650-527-8000	**PGP Software Developer's Kit (SDK) Cryptographic Module** **Version 4.2.0**	Apple iPad w/ iOS 5; Dell PowerEdge 860 Dual Core Xeon 3060 processor, 1GB RAM, DVD_ROM, 80 GB SATA hard disk drive w/ Windows XP Professional SP3; Dell Power Edge 860 Dual Core Xeon 3060 processor, 1 GB RAM, DVD-ROM, 80 GB SATA hard drive w/ Linux, 32-bit CentOS 5.5; Apple MacBook Pro 13" w/ Mac OS X 10.7	8/30/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#1777)] "The PGP SDK Cryptographic Module is a FIPS 140-2 validated software only cryptographic module. The module implements the cryptographic functions for PGP products including: PGP Whole Disk Encryption, PGP NetShare, PGP Command Line, PGP Universal, and PGP Desktop. It includes a wide range of field-tested and standards-based encryption, digital sign." *09/13/11: Update implementation information; 01/18/12: Update implementation information;*
123	Motorola Solutions Inc. Unit A1, Linhay Business Park Ashburton, Devon TQ13 7UP UK -Richard Carter TEL: +44 (0) 1364 655504 FAX: +44 (0) 1364 654625	**PTP800 DRBG Library** **Version PTP800 DRBG-04-00 (Firmware)**	TI TMS320C6421	8/30/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#1776)] "DTP800 Crypto Libraries: used in the PTP800 product. Operating in the 6 to 38 GHz RF bands at up to 368 Mbps throughput (full duplex) and with user-configured channel bandwidths from 7 to 56 MHz, the Motorola Point-to-Point 800 Series of Licensed Ethernet Microwave solutions offer operators a highly reliable licensed band wireless solution." *09/08/11: Update implementation information;*
122	RSA, The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Damon Hopley TEL: 781-515-6355	**RSA BSAFE Crypto-C Micro Edition (ME)** **Version 3.0.0.14**	Freescale MPC8536DS w/ TimeSys Linux 2.6.26.8	8/30/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#239) (SHS Val#1555) "RSA BSAFE® Crypto-C ME software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. The software supports a wide range of industry standard encryption algorithms offering developers the flexibility to choose the appropriate option to meet their requirements."
121	LSI Corporation 1501 McCarthy Boulevard Milpitas, CA 95035 USA -Lav Ivanovic TEL: 408-433-7248 FAX: 408-954-4430	**LSI-CS** **Version 1.0 (Firmware)**	Synopsys VCS simulation environment	8/30/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#617)] "Optimized hardware cryptographic module used in custom silicon implementations which need to support security applications." *04/24/12: Added new tested information;*
120	Thales E-Security Ltd Jupiter House Station Road Cambridge, CB5 8JJ UK -Marcus Streets TEL: +44 1223 723600 FAX: +44 1223 723601 -Mark Wooding TEL: +44 1223 723600 FAX: +44 1223 723601	**MiniHSM Algorithm Library** **Version 2.50.17 (Firmware)**	Freescale DragonBall MXL	8/30/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1770)] "The MiniHSM Algorithm Library provides cryptographic functionality for the MiniHSM series of Thales hardware security modules."
119	Marvell Semiconductor, Inc. 5488 Marvell Lane Santa Clara, CA 95054 USA	**Monet2.0-FW-DRBG_SP800-90_Crypto-Lib** **Version 1.0 (Firmware)**	88SS9187	8/18/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-128 , AES-256) (AES Val#1679)]

	-Lei Poo TEL: (408) 222-5000 -Yoko Enokida TEL: (408) 222-5000				"Marvell's Monet 2.0 SoC is a highly integrated System-On-Chip (SoC) controller solution customized for NAND Flash drives. It feaures a NAND Flash interface controller with a highly efficient architecture, and advanced correction capabilities. It integrates an AES-256 HW engine to support Full Drive Encryption (FDE), as well as a single-chip securit."
118	Thales e-Security Meadow View House, Crendon Industrial Estate, Long Crendon Aylesbury, Buckinghamshire HP18 9EQ UK -Tim Fox TEL: +44 (0) 1844 201800 FAX: +44 (0) 1844 208550	**TSPP-DRBG** **Version 1.1 (Firmware)**	Freescale MPC8548	8/16/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1323)] "Thales e-Security implements this algorithm for applications running on its Thales Secure Processing Platform (TSPP) providing secure cryptographic resources to products in the Thales e-Security portfolio, inlcuding the payShield 9000 HSM family."
117	RSA, The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Damon Hopley TEL: 781-515-6355	**RSA BSAFE® Crypto-J JSAFE and JCE Software Module** **Version 5.0.1**	Intel Core i7-2620M w/ Microsoft Windows XP SP3 (32-bit) with Sun JRE5.0; Intel Core i7-2620M w/ Microsoft Windows XP SP3 (32-bit) with Sun JRE6.0	8/16/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#236) (SHS Val#1549) "RSA BSAFE Crypto-J security software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. It supports a wide range of industry standard encryption algorithms offering Java developers the flexibility to choose the option most appropriate to meet their requirements."
116	Giesecke & Devrient 45925 Horseshoe Drive Dulles, VA 20166 USA -Thomas Palsherm TEL: +49 89 4119 2384 FAX: +49 89 4119 9093 -Jatin Deshpande TEL: +1 408 573 6352	**Sm@rtCafé Expert 6.0** **Version Sm@rtCafé Expert 6.0 (Firmware)**	NXP Secure_MX51	8/3/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: [3KeyTDES (TDES Val#1136))] "The firmware is a Classic Edition Java Card 3 Platform that implements the GlobalPlatform (GP) Card Specification Version 2.1.1 and the Secure Channel Protocol 03."
115	Voltage Security, Inc. 20400 Stevens Creek Blvd. Cupertino, CA 95014 USA -Luther Martin TEL: 650--543-1280 FAX: 650--543-1279 -Branislav Meandzija TEL: 408-886-3200 FAX: 408-886-3201	**Voltage IBE Encryption toolkit SDK 4.0** **Version 4.0**	Intel Xenon 2.80 GHz w/ Red Hat Enterprise Linux Server 5.3, 32-bit; Intel x64 1000 MHz w/ Windows 7 Professional SP1, 32-bit	8/3/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256 , SHA-512) (SHS Val#1539)] "Voltage IBE Cryptographic Module implements the following algorithms: DSA; TDES; AES (ECB, CBC, CFB, OFB, FPE); DRNG; DRBG; SHS; HMAC; CMAC; RSA; DH; BF IBE; BB1 IBE; MD; DES" *09/13/11: Update implementation information; 02/06/12: Updated implementation information; 02/09/12: Updated implementation information;*
114	SafeNet, Inc. 4690 Millennium Drive Belcamp, MD 21017 USA -Jim Dickens TEL: 443 327 1389 FAX: 410 931 7524 -Chris Brych TEL: 613.221.5081 FAX: 613.723.5079	**SAFEXCEL 3120 CHIP** **Part # SF914-35005-002A**	N/A	8/3/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#1743)] "The SafeNet SafeXcel-3120 is a highly integrated device designed for modest performance and high security, where power and cost-sensitivity are a priority at the network edge. The embedded ARM processor, via a digital signature, will allow customer-specific application code to execute, enabling the device to implement a complete product solution."
113	Kingston Technology Company, Inc. 17600 Newhope Street Fountain Valley, CA 92708 USA -Joel Tang TEL: 714-435-2604	**Kingston DT4000** **Version 3.03 (Firmware)** **Part # DT4000 v1.0**	DT4000 v1.0	8/3/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (HMAC Val#1020)] "Kingston's DataTraveler DT4000 Series USB Flash Drive is assembled in the US for organizations that require a secure way to store and transfer portable data. The stored data is secured by hardware-based AES-256 encryption to guard sensitive information in case the drive is lost or stolen." *02/07/13: Updated impelementation information;*

112	Beijing Huada Infosec Technology Co. Ltd 4F,Tower B,Yandong Building,No.2 Wanhong West Street,Chaoyang District Beijing, Beijing 100015 P.R.China -Hao Zhang -Hong Chi	**XA_RNGC V1.0** **Version V1.0 (Firmware)**	IS8U192A with 8-bit HC8051 embedded	8/3/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1527)] "XA_RNGC V1.0 Hardware Cryptographic Library provides core cryptographic functionality for Beijing Huada Infosec's security IC providing a capability to develop complex and flexible security applications."
111	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Sunil Chitnis TEL: 408-333-2444 FAX: 408-333-4887 -Bob Colvin TEL: 408-333-4839	**FIPS 140-2 for Brocade ServerIron 1000, 4000, and 10000 series** **Version 12.3.02 (Firmware)**	Freescale MPC8572E	7/14/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1520)] "Our Goal is to receive FIPS 140-2 SL2 certification (hardware category- tamper detection tape) on the above platforms. For this, we have identified the cryptographic boundary to be the management module (with access to E2PROM on backplane). The software is to be updated to use NSS/NSPR as the cryptographic engine."
110	Cavium, Inc. 2315 N. First Street San Jose, CA 95131 USA -Mike Scruggs TEL: 858-271-4516 FAX: 858-271-4516	**NITROX Px DRBG** **Version 1.1 (Firmware)** **Part # Nitrox Px series v1.2**	Nitrox Px Series	7/11/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1379)] "NITROX Px is a programmable IC. Microcode is loaded on the IC by its driver. The DRBG implementation combines SHA512 HW and a DRBG microcode function. The DRBG function is version-controlled separately from the overall microcode version. Thus many microcode binary file versions may contain the certified DRBG function version."
109	N/A	**N/A**	N/A	7/5/2011	N/A
108	Protected Mobility 6259 Executive Blvd Rockville, MD 20852 USA -Paul Benware TEL: 585-582-5601	**PM Cryptographic Library** **Version 1.0**	ARM Cortex-A9 w/ Android 3.0; ARM Cortex-A8 w/ Andriod 2.2; ARM Cortex-A9 w/ Android 2.3; ARM 6 w/ iOS 4.2; ARM 7 w/ iOS 4.2; ARM 7 w/ iOS 4.3	7/11/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1716)] "Cryptographic library running on Android and IOS for for encryption, decryption, hashing and random number generation."
107	Utimaco Safeware AG Germanusstraße 4 Aachen, 52080 Germany -Dr. Gesa Ott TEL: ++49 241-1696-200 FAX: ++49 241-1696-190	**CryptoServer Se DRBG** **Version util3.0.1.2_smos3.1.0.6 (Firmware)**	Texas Instruments TMS320C6416T	7/11/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1498)] "Safeguard® CryptoServer Se is an encapsulated, tamper-protected hardware security module which provides secure cryptographic services like encryption or decryption, hashing, signing and verification of data, random number generation, on-board secure key generation, key storage, and further key management functions."
106	Chunghwa Telecom Co. Ltd. Telecommunication Laboratories 12, Lane 551 Min-Tsu Road SEC.5 Yang-Mei, Taoyuan 326 Taiwan, ROC -Yeou-Fuh Kuan TEL: +886-3-424-4333 FAX: +886-3-424-4129 -Char-Shin Miou TEL: +886-3-424-4381 FAX: +886-3-424-4129	**HiKey Cryptographic Library** **Version 2.0 (Firmware)**	Java Card Runtime Environment v2.2.2 with Global Platform v2.1.1 on Renesas AE-5 Series Processor	6/29/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1493)] "HiKey Cryptographic Library supports AES, Triple-DES, HMAC, SHS, RSA and a NIST 800-90 Hash DRBG Implementations for the HiKey PKI token and HiKey flash products." *07/13/11: Update implementation information;*
105	Micron Technology 3060 N. First Street San Jose, CA 95134 USA -Mehdi Asnaashari TEL: (408) 834-1737 FAX: (408) 834-1711	**Micron 400 DRBG Module** **Version 5967 (Firmware)** **Part # 88SS9174**	Marvell Van Gogh Controller Embedded ARM Processor	6/22/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1704)] "Solid State hard drive"
104	SPYRUS Inc. 1860 Hartog Drive San Jose, CA 95131-2203 USA -Jack Young TEL: 408-392-0319 FAX: 408-392-9131	**SPYRUS FIPS Sector-based Encryption Module** **Version 03.00.0C (Firmware)** **Part # 8800740013F**	NXP LPC3131	6/16/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1483)] "The Spyrus FIPS Sector-based Encryption Module is a multifunctional USB security device combining security token and portable secure storage drive features with the strongest hardware-based

					encryption technology commercially available for protection of user data files." *06/27/11: Update implementation information;*
103	SPYRUS Inc. 1860 Hartog Drive San Jose, CA 95131-2203 USA -Jack Young TEL: 408-392-0319 FAX: 408-392-9131	**SPYRUS FIPS Sector-based Encryption Module** **Version 03.00.0C (Firmware)** **Part # 8800740012F**	NXP LPC3131	6/16/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1482)] "The Spyrus FIPS Sector-based Encryption Module is a multifunctional USB security device combining security token and portable secure storage drive features with the strongest hardware-based encryption technology commercially available for protection of user data files." *06/27/11: Update implementation information;*
102	SPYRUS, Inc. 1860 Hartog Drive San Jose, CA 95131-2203 USA -Jack Young TEL: 408-392-0319 FAX: 408-392-9131	**SPYRUS FIPS Sector-based Encryption Module** **Version 03.00.0C (Firmware)** **Part # 8800740010F**	NXP LPC3131	6/16/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1481)] "The Spyrus FIPS Sector-based Encryption Module is a multifunctional USB security device combining security token and portable secure storage drive features with the strongest hardware-based encryption technology commercially available for protection of user data files." *06/27/11: Update implementation information;*
101	SPYRUS Inc. 1860 Hartog Drive San Jose, CA 95131-2203 USA -Jack Young TEL: 408-392-0319 FAX: 408-392-9131	**SPYRUS FIPS Sector-based Encryption Module** **Version 03.00.0C (Firmware)** **Part # 880074009F**	NXP LPC3131	6/16/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1474)] "The Spyrus FIPS Sector-based Encryption Module is a multifunctional USB security device combining security token and portable secure storage drive features with the strongest hardware-based encryption technology commercially available for protection of user data files." *06/27/11: Update implementation information;*
100	SPYRUS Inc. 1860 Hartog Drive San Jose, CA 95131-2203 USA -Jack Young TEL: 408-392-0319 FAX: 408-392-9131	**SPYRUS FIPS Sector-based Encryption Module** **Version 03.00.0C (Firmware)** **Part # 880074007F**	NXP LPC3131	6/16/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1471)] "The Spyrus FIPS Sector-based Encryption Module is a multifunctional USB security device combining security token and portable secure storage drive features with the strongest hardware-based encryption technology commercially available for protection of user data files." *06/27/11: Update implementation information;*
99	SPYRUS Inc. 1860 Hartog Drive San Jose, CA 95131-2203 USA -Jack Young TEL: 408-392-0319 FAX: 408-392-9131	**SPYRUS FIPS Sector-based Encryption Module** **Version 03.00.0C (Firmware)** **Part # 880074006F**	NXP LPC3131	6/16/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1468)] "The Spyrus FIPS Sector-based Encryption Module is a multifunctional USB security device combining security token and portable secure storage drive features with the strongest hardware-based encryption technology commercially available for protection of user data files." *06/27/11: Update implementation information;*
98	Athena Smartcard Inc. 20380 Town Center Lane, Suite 240 Cupertino, CA 95014 USA -Ian Simmons TEL: (408) 865-0112 FAX: (408) 865-0333	**Athena OS755 DRBG Component** **Version A1.0 (Firmware)** **Part # Inside Secure AT90SC**	Inside Secure AT90SC w/ OS755	6/16/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1465)] "Athena OS755 is a GlobalPlatform Java Card smart card operating system implementing AES, TDES, DRBG, SHA-1/SHA-2, RSA, SP 800-56A, KAS (ECC CDH Primitive only) and ECDSA2." *06/22/11: Update implementation information;*
97	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA -James Murphy	**Apple CommonCrypto on iPhone4** **Version 2.0**	iPhone4 - Apple A4 w/ iOS 5	6/7/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#1677)] "Apple iOS CommonCrypto Module v2.0 cryptographic library offering various cryptographic mechanisms to apps."
96	Apple Inc. 1 Infinite Loop Cupertino, CA 95014 USA	**Apple CommonCrypto on iPad2** **Version 2.0**	iPad2 - Apple A5 w/ iOS 5	6/7/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#1675)]

	-James Murphy				"Apple iOS CommonCrypto Module v2.0 cryptographic library offering various cryptographic mechanisms to apps."
95	Watchdata Technologies Pte Ltd Admirax 8 Admiralty Street #2-07/08 Singapore, Singapore 757438 Singapore -Jing Bai TEL: 65 67793050 FAX: 65 67792460 -Haitao Cao TEL: 65 67793050 FAX: 65 67792460	**Watchdata-FIPS-S192-TimeCOS Hardware Cryptographic Library** **Version 1.0.0.1 (Firmware)**	CIU96S192UFB	6/7/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1461)] "Watchdata-FIPS-S192-TimeCOS Hardware Cryptographic Library provides core cryptographic functionality for Watchdata's security products providing a capability to develop complex and flexible security applications."
94	Freescale Semiconductor Inc. 7700 West Parmer Lane Austin, TX 78729 USA -Geoffrey Waters TEL: 512-996-5815 FAX: 512-996-7866	**RNG4 4.0** **Version i.MX61 (Firmware)**	Chronologic VCS simulator, vcs D-2010.06-04	6/7/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1455)] "Freescale's RNG4 4.0 is included in i.MX media processors, including: iMX61. It is planned for inclusion in multiple additional i.MX processors and in the QorIQ integrated Communications Processor family."
93	N/A	**N/A**	N/A	5/25/2011	N/A
92	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Sunil Chitnis TEL: 408-333-2444 FAX: 408-333-4887 -Bob Colvin TEL: 408-333-4839 FAX: 408-333-4887	**FIPS 140-2 for Brocade IP Products** **Version FastIron 7.2.1 (Firmware)**	Freescale MPC8248; Freescale MPC8544E; Freescale MPC8245	5/24/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1449)] "Our Goal is to receive FIPS 140-2 SL2 certification on the above platforms. For this, we have identified the cryptographic boundary to be the management module (with access to E2PROM on backplane). The software is to be updated to use NSS/NSPR as the cryptographic engine."
91	Micron Technology 3060 N. First Street San Jose, CA 95134 USA -Mehdi Asnaashari TEL: (408) 834-1737 FAX: (408) 834-1711	**Micron DRBG Module** **Version 2266 (Firmware)** **Part # 88SS9174B1-BLD2C000-P154**	Marvell Van Gogh Controller Embedded ARM processor	5/24/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1646)] "Solid State hard drive"
90	Uplogix Inc. 7600 B North Capital of Texas Highway Suite 220 Austin, TX 78731 USA -Martta Howard TEL: 512-857-7043	**Uplogix NSS** **Version 3.12.6 (Firmware)**	Intel Celeron; AMD Geode	5/24/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1445)] "Uplogix remote management appliance utilizes Mozilla's Network Security Services for general purpose cryptographic functionality. NSS provides the algorithms necessary to secure Uplogix' SSH and TLS implementations. See http://www.uplogix.com"
89	Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Jennifer Gilbert TEL: 703-484-0168	**Software crypto implementation for Cisco 5940** **Version 15.2(3)GC (Firmware)**	Freescale MPC8548E	5/24/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1643)] "Cisco 5940 ESR Air-Cooled Card, Cisco 5940 ESR Conduction-Cooled Card" *07/02/12: Updated implementation information;* *02/01/13: Updated implementation information;* *02/01/13: Updated implementation information;*
88	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Ashit Vora TEL: 703-484-5118	**IOS Firmware** **Version 15.1(3)S5 (Firmware)**	MIPS R7000/SR71000	5/12/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1634)] "IOS Firmware cryptographic implementations used within Cisco devices to provide cryptographic functions" *01/06/12: Updated implementation information;* *06/15/12: Updated implementation information;* *08/06/13: Updated implementation information;*
87	Hewlett-Packard TippingPoint 7501 N. Capital of Texas Highway Austin, TX 78737 USA	**HP TippingPoint SMS (NSS JCE Provider)** **Version 3.12.6 (Firmware)**	Intel Xeon	5/5/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1436)] "The TippingPoint SMS is a centeralized management solution for managing and

	-Dinesh Vakharia TEL: 512-681-8271 -Freddie Jimenez Jr. TEL: 512-681-8305				monitoring a deployment of TippingPoint security devices. The SMS provides cryptographic services for communicating with the security devices and user interfaces. This implementation focuses on the NSS cryptographic library which is used to implement a SUN JCE Provider."
86	Kanguru Solutions 1360 Main Street Millis, MA 02054 USA -Nate Cote TEL: 508-376-4245 FAX: 508-376-4462	**Kanguru Defender 2000** **Version 1.0 (Firmware)** **Part # KN3000/3001**	Kanguru KN3000/3001	4/20/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (HMAC Val#954)] "The Kanguru Defender 2000 is a hardware encrypted USB security device designed for secure data storage. It is also used as a platform to run secure virtual operating systems and applications." *02/16/12: Updated implementation information;*
85	Watchdata Technologies Pte Ltd Admirax 8 Admiralty Street #2-07/08 Singapore, Singapore 757438 Singapore -Jing Bai TEL: 65 67793050 FAX: 65 67792460 -Haitao Cao TEL: 65 67793050 FAX: 65 67792460	**Watchdata-FIPS-TimeCOS Hardware Cryptographic Library** **Version 1.0.0.1 (Firmware)**	Z32L256D32U	4/20/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1425)] "Watchdata-FIPS-TimeCOS Hardware Cryptographic Library provides core cryptographic functionality for Watchdata's security products providing a capability to develop complex and flexible security applications." *04/27/11: Update vendor information;*
84	Brocade Communications Systems Inc. 130 Holger Way San Jose, CA 95134 USA -Sunil Chitnis TEL: 408-333-2444 FAX: 408-333-4887 -Bob Colvin TEL: 408-333-4839 FAX: 408-333-4887	**FIPS for Brocade IP Products** **Version NetIron 5.1.1a (Firmware)**	Freescale MPC8544E; Freescale MPC7447A	4/20/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1424)] "Our Goal is to receive FIPS 140-2 SL2 certification (hardware category- tamper detection tape) on the above platforms. For this, we have identified the cryptographic boundary to be the management module (with access to E2PROM on backplane). The software is to be updated to use NSS/NSPR as the cryptographic engine."
83	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -John Bordwine TEL: (703) 885-3854 FAX: (703) 668-8953	**Symantec Cross-Platform Cipher Engine** **Version 1.0**	Intel Pentium w/ Windows 2003 Server 32-bit; Sun UltraSPARC III w/ Solaris 10; Intel Xeon w/ RHEL 5 32-bit	4/20/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1423)] "The Symantec Cross-Platform Cipher Engine is designed to provide FIPS140-2 algorithm support for the Symantec Cross-Platform Cryptographic Module. This module supports Symantec Applications by providing validated Cryptographic Services. The incorporation of these algorithms make these products ideal for enterprise and government applications."
82	Certicom Corp. 5520 Explorer Drive., 4th Floor Mississauga, Ontario L4W 5L1 Canada -Atsushi Yamada TEL: 905-501-3884 FAX: 905-508-4230 -Kris Orr TEL: 605-501-3804 FAX: 908-507-4230	**Security Builder® FIPS Core** **Version 5.6**	ARMv7 w/ QNX Neutrino 6.6 ; Intel Celeron N2820 w/ QNX Neutrino 6.6; Freescale P1010 w/ QNX Neutrino 6.5	4/8/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1422)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384) (HMAC Val#945)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1609)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-256) (P-384: , SHA-384) (P-521: , SHA-512) (ECDSA Val#200) (SHS Val#1422) "Security Builder® FIPS Core provides application developpers with cryptographics tools to easily integrate encryption, digital signatures and other security mechanisms into C-based apps for FIPS 140-2 and Suite B security. It can also be used with Certicom's PKI, IPSec SSL and DRM modules." *02/25/15: Added new tested information;*
81	Research in Motion 295 Phillip Street Waterloo, Ontario N2L 3W8 Canada -Security Certifications Team TEL: 519-888-7465 X72921 FAX: 519-888-9852	**BlackBerry Tablet Cryptographic Library** **Version 5.6**	ARMv7 w/ BlackBerry Tablet OS	4/8/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1421)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#944)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-

					192 , AES-256) (AES Val#1608)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-256) (P-384: , SHA-384) (P-521: , SHA-512) (ECDSA Val#199) (SHS Val#1421) "The BlackBerry Tablet Cryptographic Library is the software module that provides advanced cryptographic functionality to BlackBerry Tablets."
80	Avaya Inc. 211 Mt. Airy Road Basking Ridge, NJ 07920 USA -Dragan Grebovich TEL: (978) 671-3476 -Rob Tashjian TEL: (408) 496-3447	**Secure Router 2330 FW Cryptographic Library** **Version 1.0 (Firmware)**	Freescale MPC8347A	3/31/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1419)] "Avaya's Secure Router 2330 FW Cryptographic Library provides the cryptographic functionality needed to securely connect to, manage, and maintain the router device."
79	Avaya Inc. 211 Mt. Airy Road Basking Ridge, NJ 07920 USA -Dragan Grebovich TEL: (978) 671-3476 -Rob Tashjian TEL: (480) 496-3447	**Secure Router 4134 FW Cryptographic Library** **Version 1.0 (Firmware)**	Freescale MPC8541	3/31/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1418)] "Avaya's Secure Router 4134 FW Cryptographic Library provides the cryptographic functionality needed to securely connect to, manage, and maintain the router device."
78	BAE Systems 2525 Network Place Herndon, VA 20171 USA -John Ata TEL: 703-736-4384 FAX: 703-736-4348	**Stop 7 Kernel Cryptographic Module** **Version 1.1**	Intel Pentium D w/ Stop 7.3 Beta 1	3/31/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#1603)] "The Stop 7 Kernel Cryptographic Module provides cryptographic services that the Stop 7 kernel uses to implement random number generation and file system encryption."
77	RSA The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Damon Hopley TEL: 781-515-6355	**RSA BSAFE® CNG Cryptographic Primitives Library** **Version 1.0**	Intel Pentium M Processor w/ Microsoft Windows 7 (32-bit); AMD Athlon 64 X2 Dual Core Processor w/ Microsoft Windows 7 (64-bit)	3/8/2011	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-256 , SHA-512256) (HMAC Val#935)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-256) (P-384: , SHA-256) (P-521: SHA-256) (ECDSA Val#196) (SHS Val#1410) "The RSA BSAFE CNG Cryptographic Primitives Library is a drop-in replacement for the Microsoft user-mode CNG provider. It can be dynamically linked into applications by software developers to permit the use of general purpose cryptography."
76	ZTE NO. 55, Hi-tech Road South ShenZhen, Guangdong 518057 P.R.China -Royce Wang TEL: 0086-755-2677 0345 FAX: 0086-755-2677 0347	**Unified Platform Cryptographic Library for Intel** **Version 1.1**	Intel(R) Xeon(TM) w/ EMBSYS (TM) Carrier Grade Embedded Linux V3	2/24/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1405)] "UPCL (Unified Platform Cryptographic Library) on intel platform provides the cryptographic API to Net elements' applications running on series of intel multi-core processors."
75	ZTE NO. 55, Hi-tech Road South ShenZhen, Guangdong 518057 P.R.China -Royce Wang TEL: 0086-755-2677 0345 FAX: 0086-755-2677 0347	**Unified Platform Cryptographic Library for AMD** **Version 1.1**	AMD Opteron(R) w/ EMBSYS(TM) Carrier Grade Embedded Linux V3	2/24/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1404)] "UPCL(Unified Platform Cryptographic Library) on AMD platform provides the cryptographic API to Net elements' applications running on series of AMD multi-core processors."
74	ZTE NO. 55, Hi-tech Road South ShenZhen, Guangdong 518057 P.R.China -Royce Wang TEL: 0086-755-2677 0345 FAX: 0086-755-2677 0347	**UEP Cryptographic Module for Intel** **Version 4.11.10**	NewStart CGS Linux V3.02 with Sun JDK/JRE 1.6.0_11	2/24/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1403)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#930)] "UEPCM (Unified Element Management Platform Cryptographic Module) on Intel platform provides the cryptographic API to Net Management applications running on the series of Intel multi-core processors." *07/07/11: Update implementation information;*
73	ZTE NO. 55, Hi-tech Road South	**UEP Cryptographic Module for AMD** **Version 4.11.10**	NewStart CGS Linux V3.02 with Sun JDK/JRE 1.6.0_11	2/24/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1402)]

	ShenZhen, Guangdong 518057 P.R.China -Royce Wang TEL: 0086-755-2677 0345 FAX: 0086-755-2677 0347				**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#929)] "UEPCM (Unified Element Platform Cryptographic Module) on AMD platform provides the cryptographic API to Net Management applications running on series of AMD multi-core processors." *07/07/11: Update implementation information;*
72	Thales E-Security Ltd Jupiter House Station Road Cambridge, CB5 8JJ UK -Marcus Streets TEL: +44 1223 723600 FAX: +44 1223 723601 -Mark Wooding TEL: +44 1223 723600 FAX: +44 1223 723601	**nShield Algorithm Library** **Version 2.50.16 (Firmware)**	Motorola PowerPC	2/24/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1579)] "The nShield algorithm library provides cryptographic functionality for Thales's nShield Hardware Security Modules."
71	Oracle Corporation 500 Eldorado Blvd., Bldg 5 Broomfield, CO 80021 USA -David Hostetter TEL: 303-272-7126	**T10000C CTR DRBG** **Version 2.0 (Firmware)**	ARM 926EJS	2/3/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1566)] "Oracle StorageTek T10000C Tape Drive."
70	Hewlett-Packard TippingPoint 7501 N. Capital of Texas Highway Austin, TX 78737 USA -Dinesh Vakharia TEL: 512-681-8271 -Freddie Jimenez Jr. TEL: 512-681-8305	**TippingPoint Security Management System (NSS JCE Provider)** **Version 3.2 (Firmware)**	Intel Xeon E5520 2.27GHz	1/26/2011	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1386)] "The TippingPoint SMS is a centeralized management solution for managing and monitoring a deployment of TippingPoint security devices. The SMS provides cryptographic services for communicating with the security devices and user interfaces."
69	Centrify Corporation 785 N Mary Avenue Suite 200 Sunnyvale, CA 94085 USA -Keith Moreau TEL: 415 412 6482	**Centrify Cryptographic Module** **Version 1.0**	Intel Core 2 Duo, 1.83 GHZ w/ Mac OS X 10.6.4; Intel I7-870 w/ Red Hat Enterprise Linux ES release 4; Intel I7-870 w/ Red Hat Enterprise Linux ES v5; Intel Core 2 Duo, 1.83 GHZ w/ Mac OS X 10.6.5	1/13/2011	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1554)] "The Centrify Cryptographic Module provides the cryptographic services for all of Centrify's products." *02/10/11: Add new tested information;*
68	Acme Packet Inc. 100 Crosby Drive Bedford, MA 01730 USA -Prashant Kumar TEL: 781-328-4450	**Acme Packet Net-Net 4500** **Version C6.3 (Firmware)**	Intel Core Duo T2500	12/27/2010	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1) (SHS Val#1373)] "Acme Packet's FIPS-validated Session Border Controller provides critical control functions to deliver trusted, first-class interactive communications-: voice, video and multimedia sessions -across IP network borders."
67	Acme Packet Inc. 100 Crosby Drive Bedford, MA 01730 USA -Prashant Kumar TEL: 781-328-4450	**Acme Packet Net-Net 3820** **Version C6.3 (Firmware)**	Intel Celeron M 440	12/27/2010	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1) (SHS Val#1372)] "Acme Packet's FIPS-validated Session Border Controller provides critical control functions to deliver trusted, first-class interactive communications-: voice, video and multimedia sessions -across IP network borders."
66	General Dynamics C4 Systems 77 A Street Needham, MA 02494 USA -David Aylesworth TEL: 781-400-6527	**Fortress Cryptographic Implementation** **Version 2.0 (Firmware)**	RMI Alchemy MIPS Processor; Broadcom XLS Processor	12/6/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#889)] "The Fortress Cryptographic Implementation suite works in unison to provide security to your wireless and wired networks." *11/06/14: Updated vendor and implemenation information;*
65	General Dynamics C4 Systems 77 A Street Needham, MA 02494 USA -David Aylesworth TEL: 784-400-6527	**Fortress Cryptographic Implementation - SSL** **Version 2.0 (Firmware)**	RMI Alchemy MIPS Processor; Broadcom XLS Processor	11/23/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#887)] "The Fortress Cryptographic Implementation suite works in unison to provide security to your wireless and wired networks."

					11/05/2014: Updated vendor and implementation information;
64	Mocana Corporation 710 Sansome Street San Francisco, CA 94104 USA -James Blaisdell TEL: 415-617-0055 FAX: 415-617-0056	**Mocana Cryptographic Library** **Version 5.4f**	Intel Core2 Duo w/ VxWorks 6.7; ARM v7 w/ Android 2.2; PowerQuicc III w/ VxWorks 5.5; Freescale e600 w/ VxWorks 5.5; PowerQuicc II Pro w/ VxWorks 6.2; PowerQuicc III w/ VxWorks 6.4; PowerQuicc II w/ VxWorks 6.4; Intel XScale PXA w/ VxWorks 6.4; Freescale e500 w/ Wind River 4.0 using Linux 2.6.34	11/16/2010	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1505)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1505)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (SHS Val#1353) "NanoCrypto is the engine of Mocana's Device Security Framework - a software framework that secures all aspects of a system. The Device Security Framework helps applications and device designers reduce development costs and dramatically enhance cryptographic performance. For details see www.mocana.com." *05/26/11: Add new tested information;* *06/13/11: Update implementation information;* *06/21/11: Add new tested information;* *06/30/11: Add new tested information;* *09/21/11: Add new tested information;* *10/05/11: Add new tested information;* *10/12/11: Update implementation information;*
63	Pierson Capital Technology LLC and Pierson Capital Technology (Beijing) LTD (Beijing) LTD Centerville Road, Suite 400 Wilmington, Delaware 19808 USA Level 18, Suite 9, Oriental Plaza 1, East Chang An Avenue, Dong Cheng District, Beijing 100738 P.R. China -Frank Psaila TEL: 86-10-65215700-5735 -Frank Psaila TEL: 86-13501108625	**MIIKOO Device** **Version MIIKOO Device Algorithm Library V2.1 (Firmware)**	Synochip AS602	11/16/2010	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1351)] "MIIKOO device combines fingerprint recognition and additional cryptography capabilities to generate Dynamic PINs. It is compatible with any type of smart card, magnetic stripe or contact-less cards by seamlessly providing the added biometrical triggering of dynamic PIN security over the existing financial transaction network."
62	Seagate Technology LLC. 389 Disc Drive Longmont, CO 80503 USA -Monty Forehand TEL: 720-684-2835 FAX: 720-684-2733	**800-90 DRBG** **Version 1.0 (Firmware)**	ARM Cortex-R Family	11/16/2010	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1225)] "SP 800-90 based DRBG." *02/28/14: Updated implementation information;*
61	Francotyp-Postalia GmbH Triftweg 21-26 Birkenwerder, 16547 Germany -Dirk Rosenau TEL: +49/3303/525/616 FAX: +49/3303/525/07/616 -Hasbi Kabacaoglu TEL: +49/3303/525/656 FAX: +49/3303/525/07/656	**FP mCryptoLibrary - CTR-DRBG** **Version 1.1 (Firmware)**	Maxim IC0400	10/26/2010	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#1493)] "The firmware implementation of the FP mCryptoLibrary, which runs on an embedded hardware module, with a Maxim IC0400 processor. The cryptographic algorithm implementation is used in the context of security critical services."
60	Kingston Technology Company, Inc. 17600 Newhope Street Fountain Valley, CA 92708 USA -Joel Tang TEL: 714 435 2604	**Kingston DT4000** **Version 03.01.10 (Firmware)** **Part # DT4000 v1.0**	DT4000 v1.0	10/4/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (HMAC Val#872)] "Kingston's DataTraveler DT4000 Series USB Flash Drive is assembled in the US for organizations that require a secure way to store and transfer portable data. The stored data is secured by hardware-based AES-256 encryption to guard sensitive information in case the drive is lost or stolen."
59	Cisco Systems Inc. 175 W Tasman Drive San Jose, CA 95134 USA -Jennifer Gilbert TEL: 703-484-0168	**Network Security Services (NSS)** **Version 3.12.5 and 3.12.5.1**	Intel Core 2 Duo w/ Cisco CARS 1.2.0.182	9/27/2010	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1334)] "General purpose cryptographic library" *03/25/13: Update implementation information;*
58	Feitian Technologies Co. Ltd.	**Feitian-FIPS-COS Hardware**	ST Visual Develop BR6	9/27/2010	**CTR_DRBG**: [Prediction Resistance Tested: Not

	5th Floor Building 7A No. 40 Xueyuan Road Haidan District Beijing, Beijing 100191 China -Tibi Zhang TEL: 86-010-62304466 x821 FAX: 86-010-62304416 -Xiaozhi Zheng TEL: 86-010-62304466 x531 FAX: 86-010-62304416	**Cryptographic Library** **Version 0.0.5.6 (Firmware)**			Enabled; BlockCipher_No_df: [3KeyTDES (TDES Val#991))] "The Feitian-FIPS-COS Hardware Cryptographic Library provides cryptographic algorithm support to the Feitian-FIPS-COS cryptographic module."
57	RSA The Security Division of EMC 2831 Mission College Blvd. Santa Clara, CA 95054 USA -Kathy Kriese TEL: 408-326-4552	**RSA BSAFE(R) Crypto-J Software Module** **Version 5.0**	AMD Athlon(TM) 64 X2 Dual Core Processor w/ Microsoft Windows XP Professional SP3, Sun JRE 6.0; AMD Athlon(TM) 64 X2 Dual Core w/ Microsoft Windows XP Professional SP3, Sun JRE 5.0	9/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#863)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#182) (SHS Val#1328) "RSA BSAFE Crypto-J security software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. It supports a wide range of industry standard encryption algorithms offering Java developers the flexibility to choose the option most appropriate to meet their requirements"
56	Thales e-Security Meadow View House, Crendon Industrial Estate, Long Crendon Aylesbury, Buckinghamshire HP18 9EQ UK -Tim Fox TEL: +44 (0) 1844 201800 FAX: +44 (0) 1844 208550	**TSPP-DRBG** **Version 1.0 (Firmware)**	Freescale MPC8548 Family	9/9/2010	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1323)] "Thales e-Security implements this algorithm for applications running on its Thales Secure Processing Platform (TSPP) providing secure cryptographic resources to products in the Thales e-Security portfolio, including the payShield 9000 HSM family."
55	Code Corporation 14940 S Pony Express Rd Ste 500 Bluffdale, UT 84065 USA -Tim Jackson TEL: 801-984-7865 FAX: 801-495-0280	**Traffic Encryption Key Generation** **Version 7541 (Firmware)**	AMD Alchemy Au1100-400MBD	8/30/2010	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1457)] "FIPS approved DRBG using AES-256 used to generate session based keys for encrypting data sent from a Code Reader 2500 FIPS or Code Reader 3500 FIPS module to a CodeXML FIPS Bluetooth Modem module."
54	Hangzhou Synochip Technologies Co. Ltd. 2F, Building 17, No. 176 Tianmushan Road Hangzhou, Zhejiang 310012 China -Windy Ye TEL: (86)571 8827 1908 FAX: (86)571 8827 1901 -Howard He TEL: (86)571 8827 1908 FAX: (86)571 8827 1901	**"Cordis5+" 32-bit RISC core platform** **Version 1.0**	Cordis 5+ is a core with best-in-class speed, die area and power characteristics. w/ Fingerprint processing accelerator, algorithm firmware	6/30/2010	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-256) (SHS Val#1222)] "1) Security Applications,such as Digital Certification, USB Keys,2) Fingerprint Identification, 3)Embedded Applications"
53	Exar Corporation 48720 Kato Road Fremont, CA 94538 USA -Zack Mihalis TEL: 408-399-3637 FAX: 408-458-1924 -Jeffrey Chan TEL: 408-399-3606 FAX: +86-571-8815-6615	**Panther-I 820x Series Die** **Part # 820x-01**	N/A	6/30/2010	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1284)] "Exar 820x is an application services processor family designed for storage capacity optimization and network security. 820x accelerates algorithms such as LZS compression, AES encryption, SHA hash and PK operations for deduplication and security. It has a throughput up to 6Gbps doing compress, encrypt and hash in a single pass."
52	Certicom Corp. 5520 Explorer Drive., 4th Floor Mississauga, Ontario L4W 5L1 Canada -Rob Williams TEL: 289-261-4187 FAX: 905-507-4230	**Security Builder GSE-J Crypto Core** **Version 2.8**	Intel Pentium D w/ Red Hat Enterprise Linux AS 5.5 with SUN JRE 1.5.0; Intel Pentium D w/ Red Hat Enterprise Linux AS 5.5 with SUN JRE 1.6.0; Intel Xeon w/ Red Hat Enterprise Linux AS 5.5 x64 with SUN JRE 1.5.0; Intel Xeon w/ Red Hat Enterprise Linux AS 5.5 x64 with SUN JRE 1.6.0; SPARC v9 w/ Sun Solaris 10 (32-bit) with SUN JRE 1.5.0; SPARC v9 w/ Sun Solaris 10 (32-bit) with SUN JRE	6/30/2010	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#1281)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#832)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1411)]

	-Atsushi Yamada TEL: 289-261-4184 FAX: 905-507-4230		1.6.0; SPARC v9 w/ Sun Solaris 10 (64-bit) with SUN JRE 1.5.0; SPARC v9 w/ Sun Solaris 10 (64-bit) with SUN JRE 1.6.0; Intel Xeon w/ MS-Windows Vista SP2 (32-bit) with SUN JRE 1.5.0; Intel Xeon w/ MS-Windows Vista SP2 (32-bit) with SUN JRE 1.6.0; Intel Xeon w/ MS-Windows Vista SP2 (64-bit) with SUN JRE 1.5.0; Intel Xeon w/ MS-Windows Vista SP2 (64-bit) with SUN JRE 1.6.0; Intel Xeon w/ MS-Windows 2008 Server SP2 (64-bit) with JRE 1.5.0; Intel Xeon w/ MS-Windows 2008 Server SP2 (64-bit) with JRE 1.6.0		**Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#179) (SHS Val#1281) "Java cryptographic toolkit." *10/12/10: Update vendor information; 08/30/11: Update implementation information;*
51	N/A	**N/A**	N/A	1/19/2011	N/A
50	Verdasys Inc. 404 Wyman Street Suite 320 Waltham, MA 02541 USA -Scott Shou TEL: 917-371-3386 -Josh McCally TEL: 703-267-6050 x111 FAX: 703-267-6810	**FIPS Kernel Mode Cryptographic Module (VSEC.SYS)** **Version 1.0**	Intel Core 2 Quad w/ Microsoft Windows XP (64-bit); Intel Core 2 Quad w/ Microsoft Windows XP (32-bit)	6/10/2010	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1261)] "Previously called: Digital Guardian Security Kernel v1.0. VSEC.SYS is a Windows kernel mode export driver that provides FIPS Approved cryptographic services to Verdasys applications such as Digital Guardian."
49	Wind River Systems, Inc. 500 Wind River Way Alameda, CA 94501 USA -Janet Davis TEL: 613-270-5770	**Network Security Services Library** **Version 3.12.4**	x86_64 Nehalem Xeon 5500 w/ Wind River Linux Secure 1.0; ppc_32 mpc8572 w/ Wind River Linux Secure 1.0; x86_64 Pentium core2 duo w/ Wind River Linux Secure 1.0; ARM TI OMAP3530 w/ Wind River Linux Secure 1.0	6/3/2010	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1256)] "Wind River Linux Secure uses Network Security Services (NSS) to provide a set of libraries designed to support cross-platform development of security-enabled client and server applications. Applications built with WRLS can support SSL v2 and v3, TLS, PKCS #5, PKCS #7, PKCS #11, PKCS #12, S/MIME, X.509 v3 certificates, and other security standards."
48	Thales e-Security Inc. 2200 North Commerce Parkway Suite 200 Weston, Florida 33326 USA -Marcus Streets TEL: +44 1223 723613 FAX: +44 1223 723601 -James Huang TEL: +1 408 457 7714 FAX: +1 408 457 7681	**TEMS - Random bit generator library (NSS)** **Version NSS 3.12.4 (Firmware)**	Intel Xeon Dual Core	5/10/2010	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1231)] "An implementation of the SP800-90 random bit generator used to provide cryptographically secure random numbers for all libraries in the TEMS appliance."
47	IBM Corporation IBM/Tivoli P.O. Box 3499 Australia Fair Southport, Queensland 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420 -Alex Hennekam TEL: +61 7 5552 4045 FAX: +61 7 5571 0420	**ICC Algorithmic Core on AIX PowerPC-64 for 64 bits** **Version 8.0.0**	IBM PowerPC 5 64-bit w/ IBM AIX 6.1	4/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256) (HMAC Val#779)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1331)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1331)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
46	IBM Corporation IBM/Tivoli P.O. Box 3499 Australia Fair Southport, Queensland 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420 -Alex Hennekam TEL: +61 7 5552 4045 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Windows 64-bit x86-64 for 32 bits** **Version 8.0.0**	AMD Opteron X86_64 w/ Microsoft Windows Servers 2008 32-bit	4/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256) (HMAC Val#778)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1330)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1330)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
45	IBM Corporation IBM/Tivoli P.O. Box 3499 Australia Fair Southport, Queensland 4215 Australia	**ICC Algorithmic Core on Windows 64-bit x86-64 for 64 bits** **Version 8.0.0**	AMD Opteron X86_64 w/ Microsoft Windows Server 2008 64-bit	4/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256) (HMAC Val#777)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-

	-Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420 -Alex Hennekam TEL: +61 7 5552 4045 FAX: +61 7 5571 0420				192 , AES-256) (AES Val#1329)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1329)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
44	IBM Corporation IBM/Tivoli P.O. Box 3499 Australia Fair Southport, Queensland 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420 -Alex Hennekam TEL: +61 7 5552 4045 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Solaris UltraSparc-64 for 64 bits** **Version 8.0.0**	Sun UltraSPARC T1000 64-bit w/ Sun Solaris 10	4/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256) (HMAC Val#776)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1328)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1328)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
43	IBM Corporation IBM/Tivoli P.O. Box 3499 Australia Fair Southport, Queensland 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420 -Alex Hennekam TEL: +61 7 5552 4045 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Solaris UltraSparc-64 for 32 bits** **Version 8.0.0**	Sun UltraSPARC T1000 64-bit w/ Sun Solaris 10	4/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256) (HMAC Val#775)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1327)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1327)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
42	IBM Corporation IBM/Tivoli P.O. Box 3499 Australia Fair Southport, Queensland 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420 -Alex Hennekam TEL: +61 7 5552 4045 FAX: +61 7 5571 0420	**ICC Algorithmic Core on AIX PowerPC-64 for 32 bits** **Version 8.0.0**	IBM PowerPC 5 64-bit w/ IBM AIX 6.1	4/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256) (HMAC Val#774)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1326)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1326)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
41	IBM Corporation IBM/Tivoli P.O. Box 3499 Australia Fair Southport, Queensland 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420 -Alex Hennekam TEL: +61 7 5552 4045 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL zSeries-64 for 64 bits** **Version 8.0.0**	IBM zSeries z10 64-bit w/ Red Hat Enterprise Linux Server 5	4/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256) (HMAC Val#773)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1325)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1325)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
40	IBM Corporation IBM/Tivoli P.O. Box 3499 Australia Fair Southport, Queensland 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420 -Alex Hennekam TEL: +61 7 5552 4045 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL zSeries-64 for 32 bits** **Version 8.0.0**	IBM zSeries z10 64-bit w/ Red Hat Enterprise Linux Server 5	4/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256) (HMAC Val#772)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1324)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1324)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
39	IBM Corporation IBM/Tivoli P.O. Box 3499	**ICC Algorithmic Core on RHEL x86-64 for 64 bits**	AMD Opteron X86_64 w/ Red Hat Enterprise Linux Server 5	4/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256

	Australia Fair Southport, Queensland 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420 -Alex Hennekam TEL: +61 7 5552 4045 FAX: +61 7 5571 0420	**Version 8.0.0**			) (HMAC Val#771)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1323)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1323)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
38	IBM Corporation IBM/Tivoli P.O. Box 3499 Australia Fair Southport, Queensland 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420 -Alex Hennekam TEL: +61 7 5552 4045 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL x86-64 for 32 bits** **Version 8.0.0**	AMD Opteron X86_64 w/ Red Hat Enterprise Linux Server 5	4/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256) (HMAC Val#770)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1322)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1322)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
37	IBM Corporation IBM/Tivoli P.O. Box 3499 Australia Fair Southport, Queensland 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420 -Alex Hennekam TEL: +61 7 5552 4045 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL 32-bit x86-64 for 32 bits** **Version 8.0.0**	AMD Opteron X86_64 w/ Red Hat Enterprise Linux Server 5	4/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256) (HMAC Val#769)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1321)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1321)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library used by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
36	IBM Corporation IBM/Tivoli P.O. Box 3499 Australia Fair Southport, Queensland 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420 -Alex Hennekam TEL: +61 7 5552 4045 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL PPC64 for 64 bits** **Version 8.0.0**	IBM PowerPC 5 64-bit w/ Red Hat Enterprise Linux Server 5	4/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256) (HMAC Val#768)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1320)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1320)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
35	IBM Corporation IBM/Tivoli P.O. Box 3499 Australia Fair Southport, Queensland 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420 -Alex Hennekam TEL: +61 7 5552 4045 FAX: +61 7 5571 0420	**ICC Algorithmic Core on RHEL PPC64 for 32 bits** **Version 8.0.0**	IBM PowerPC 5 64-bit w/ Red Hat Enterprise Linux Server 5	4/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256) (HMAC Val#767)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1319)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1319)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library that uses the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."
34	IBM Corporation IBM/Tivoli P.O. Box 3499 Australia Fair Southport, Queensland 4215 Australia -Peter Waltenberg TEL: +61 7 5552 4016 FAX: +61 7 5571 0420 -Alex Hennekam TEL: +61 7 5552 4045 FAX: +61 7 5571 0420	**ICC Algorithmic Core on Windows 32-bit x86-64 for 32 bits** **Version 8.0.0**	AMD Opteron X86_64 w/ Microsoft Windows Server 2008 32-bit	4/21/2010	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256) (HMAC Val#766)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1318)] BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#1318)] "ICC is a C language implementation of cryptographic functions based on the cryptographic library provided by the OpenSSL project. This enables IBM products to use an open source solution for cryptography and a FIPS 140-2 certified cryptographic provider."

33	Toshiba Corporation 1-1, Shibaura 1-chome Minato-ku, Tokyo 105-8001 Japan -Yichang Chan TEL: 408-324-5812 FAX: 408-324-5903	**Hash DRBG** **Version 1.4 (Firmware)**	Toshiba SoC	2/16/2010	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1181)] "Toshiba Secure Cryptographic Suite (TSCS) is a library of unique hardware and software cipher solutions which are standard encryption algorithm-based to provide Toshiba products and the systems using them a robust and secure data storage environment."
32	Cavium Networks 805 E Middlefield Road Mountain View, CA 94109 USA -TA Ramanujam TEL: 650-623-7039 FAX: 650-625-9751	**NITROX XL CN16XX-NFBE** **Version 1.0 (Firmware)**	Cavium Networks OCTEON CN52XX Processor with NITROX CN16XX Security Processor	1/7/2010	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1265)] "NITROX XL CN16XX-NFBE HSM (Hardware Security Module) Adapter family."
31	SPYRUS Inc. 1860 Hartog Drive San Jose, CA 95131-2203 USA -Tom Dickens TEL: 408-392-9131 FAX: 408-392-0319	**Hydra PC Locksmith (Board 3 / Level 3)** **Part # 880074004F, v03.00.0C**	N/A	12/30/2009	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1157)] "The Hydra PC Locksmith is a multifunctional USB security device combining security token and portable secure storage drive features with the strongest hardware-based encryption technology commercially available for protection of user data files."
30	SPYRUS Inc. 1860 Hartog Drive San Jose, CA 95131-2203 USA -Tom Dickens TEL: 408-392-9131 FAX: 408-392-0319	**Hydra PC Locksmith (Board 3 / Level 3)** **Part # 880074003F, v03.00.0C**	N/A	12/30/2009	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1156)] "The Hydra PC Locksmith is a multifunctional USB security device combining security token and portable secure storage drive features with the strongest hardware-based encryption technology commercially available for protection of user data files."
29	SPYRUS Inc. 1860 Hartog Drive San Jose, CA 95131-2203 USA -Tom Dickens TEL: 408-392-9131 FAX: 408-392-0319	**Hydra PC Locksmith (Board 3/Level 3)** **Part # 880074002F, v03.00.0C**	N/A	12/30/2009	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1155)] "The Hydra PC Locksmith is a multifunctional USB security device combining security token and portable secure storage drive features with the strongest hardware-based encryption technology commercially available for protection of user data files."
28	RSA Security, Inc. 177 Bovet Road, Suite 200 San Mateo, CA 94402 USA -Kathy Kriese TEL: 650-931-9781	**RSA BSAFE® TLS-J Micro Edition** **Version 1.1**	Intel Pentium D w/ Windows XP SP3 Pro w/ JME SDK 3.0 CDC Runtime Env	12/30/2009	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-256) (HMAC Val#727)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-256 , SHA-384) (ECDSA Val#146) (SHS Val#1143) "RSA BSAFE TLS-J ME security software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. It supports a wide range of industry standard encryption algorithms offering Java developers the flexibility to choose the option most appropriate to meet their requirements"
27	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA -Tim Myers TEL: 1-800-MICROSOFT	**Windows Server 2008 R2 CNG algorithms** **Version 1.0**	Intel Itanium 2 w/ Windows Server 2008 R2 (IA64); Intel Core 2 Duo w/ Windows Server 2008 R2 (x64); Intel Core 2 Duo w/ Windows Server 2008 R2 SP1 (x64); Intel Itanium2 w/ Windows Server 2008 R2 SP1 (IA64)	9/30/2009	**Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-256) (ECDSA Val#142) (SHS Val#1081) "The Microsoft Windows Cryptographic Primitives Library is a general purpose, software-based, cryptographic module which can be dynamically linked into applications by developers to permit the use of FIPS 140-2 Level 1 compliant cryptography." *05/12/11: Add new tested inforamtion and update vendor information;* *06/08/11: Add new tested information;*
26	Motorola Unit A1 Linhay Business Park Ashburton, Devon TQ13 7UP UK -Richard Carter TEL: 01364 655504	**PTP500-DRNG** **Version PTP500-DRNG-00-01 (Firmware)**	TI C6412 DSP	9/30/2009	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#1179)] "The Motorola family of PTP Wireless Ethernet Bridges offers a solution to the challenge of establishing a reliable, secure, point-to-point network connection. Whether operating in a Non-

	FAX: 01364 654525				Line-of-Sight (NLoS), adverse or marginally adverse environment." *10/07/09: Update Processor;*
25	Motorola Unit A1 Linhay Business Park Ashburton, Devon TQ13 7UP UK -Richard Carter TEL: 01364 655504 FAX: 01364 654525	**PTP300-DRNG** **Version PTP300-DRNG-00-01 (Firmware)**	TI C6412 DSP	9/30/2009	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#1179)] "The Motorola family of PTP Wireless Ethernet Bridges offers a solution to the challenge of establishing a reliable, secure, point-to-point network connection. Whether operating in a Non-Line-of-Sight (NLoS), adverse or marginally adverse environment." *01/07/09: Update Processor;*
24	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA -Tim Myers TEL: 1-800-MICROSOFT	**Windows 7 CNG algorithms** **Version 1.0**	Intel Core 2 Duo w/ Windows 7 Ultimate (x86); Intel Core 2 Duo w/ Windows 7 Ultimate (x64); Intel Core 2 Duo w/ Windows 7 Ultimate SP1 (x64); Intel Core 2 Duo w/ Windows 7 Ultimate SP1 (x86)	9/30/2009	**Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-256) (SHS Val#1081) "The Microsoft Windows Cryptographic Primitives Library is a general purpose, software-based, cryptographic module which can be dynamically linked into applications by developers to permit the use of FIPS 140-2 Level 1 compliant cryptography." *05/12/11: Add new tested information and update vendor information;*
23	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA -Tim Myers TEL: 1-800-MICROSOFT	**Windows 7 and Server 2008 R2 RNG Library** **Version 1.0**	Intel Core 2 Duo w/ Windows 7 Ultimate (x64); Intel Core 2 Duo w/ Windows 7 Ultimate (x86); Intel Core 2 Duo w/ Windows Server 2008 R2 (x64); Intel Itanium2 w/ Windows Server 2008 R2 (IA64); Intel Core 2 Duo w/ Windows Server 2008 R2 SP1 (x64); Intel Core 2 Duo w/ Windows 7 Ultimate SP1 (x64); Intel Core 2 Duo w/ Windows 7 Ultimate SP1 (x86); Intel Itanium2 w/ Windows Server 2008 R2 SP1 (IA64)	9/21/2009	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_No_df: (AES-256) (AES Val#1168)] "Provides random number generation algorithms for use by Microsoft cryptographic libraries." *09/29/09: Add new tested OES';* *05/04/11: Add new tests and vendor information;* *06/08/11: Add new tested information;*
22	FalconStor Software, Inc. 2 Huntington Quadrangle Melville, NY 11747 USA -Yeggy Javadi TEL: 631-773-6745 FAX: 631-777-6882 -Wai Lam TEL: 631-962-1116 FAX: 631-501-7633	**FalconStor Cryptographic Module** **Version 3.12.4**	Intel Pentium D w/ Oracle Enterprise Linux 5.3 (64-bit)	9/15/2009	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1085)] "Cryptographic Library for Authentication and Encryption Implementations for All FalconStor Software Products."
21	Motorola Solutions Inc. Unit A1, Linhay Business Park Ashburton, Devon TQ13 7UP UK -Richard Carter TEL: 01364 655504 FAX: 01364 654525	**PTP600-DRNG** **Version PTP600-DRNG-00-01 (Firmware)**	TI C6414 DSP	8/17/2009	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128) (AES Val#1144)] "The Motorola family of PTP Wireless Ethernet Bridges offers a solution to the challenge of establishing a reliable, secure, point-to-point network connection. Whether operating in a Non-Line-of-Sight (NLoS), adverse or marginally adverse environment."
20	Pitney Bowes, Inc. 35 Waterview Drive Shelton, CT 06484-8000 USA -Robert Sisson TEL: 203-924-3061 FAX: 203-924-3518	**appPRNG** **Version 01.00.0003 (Firmware)**	Sigma ASIC	8/17/2009	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#650)] "The Pitney Bowes Cygnus X-3 Postal Security Device (PSD) is designed in compliance with FIPS 140-2 and IPMAR standards to support the USPS IBIP and international digital indicia standards globally. The PSD employs strong cryptographic and physical security techniques for the protection of customer funds in Pitney Bowes Postage Metering products."
19	Silex Technology 157 West 7065 South Salt Lake City, UT 84047 USA -ksugawara@silexamerica.com TEL: 801-748-1199 FAX: 714-258-0730	**SX-500 HASH-DRNG** **Version sx500_crvpto_VI (Firmware)** **Part # CN210**	eCos on Cavium CN210 processor	8/10/2009	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1) (SHS Val#1059)] "Deterministic random number generator for creation of authentication nonces and other random values."
18	Red Hat, Inc. and Sun Microsystems, Inc. 4150 Network Circle	**Network Security Services (NSS) Cryptographic Module (Basic ECC)** **Version 3.12.4**	Intel Core 2 Duo w/ Mac OS X 10.5 (32-bit); Intel Core 2 Duo w/ Mac OS X 10.5 (64-bit); AMD Opteron w/ Windows XP Professional SP3 (32-bit)	7/10/2009	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1050)]

	Santa Clara, CA 95054 USA -Glen Beasley TEL: 800-555-9SUN -Robert Relyea TEL: 650-254-4236				"Network Security Services (NSS) is a set of open source C libraries designed to support cross-platform development of security-enabled applications. NSS implements major Internet security standards. NSS is available free of charge under a variety of open source compatible licenses. See http://www.mozilla.org/projects/security/pki/nss/."
17	Red Hat Inc. and Sun Microsystems Inc. 4150 Network Circle Santa Clara, CA 95054 USA -Glen Beasley TEL: 800-555-9SUN -Robert Relyea TEL: 650-254-4236	**Network Security Services (NSS) Cryptographic Module (Extend ECC)** **Version 3.12.4**	Sun UltraSPARC III Cu w/ Sun Solaris 10 5/08 (32-bit); Sun UltraSPARC III Cu w/ Sun Solaris 10 5/08 (64-bit); AMD Opteron w/ Sun Solaris 10 5/08 (32-bit); AMD Opteron w/ Sun Solaris 10 5/08 (64-bit)	7/10/2009	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1049)] "Network Security Services (NSS) is a set of open source C libraries designed to support cross-platform development of security-enabled applications. NSS implements major Internet security standards. NSS is available free of charge under a variety of open source compatible licenses. See http://www.mozilla.org/projects/security/pki/nss/."
16	Red Hat Inc. and Sun Microsystems Inc. 4150 Network Circle Santa Clara, CA 95054 USA -Glen Beasley TEL: 800-555-9SUN -Robert Relyea TEL: 650-254-4236	**Network Security Services (NSS) Cryptographic Module** **Version 3.12.4**	AMD Opteron w/ Red Hat Enterprise Linux v5 (32-bit); Intel Xeon w/ Red Hat Enterprise Linux v5 (64-bit)	7/10/2009	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#1048)] "Network Security Services (NSS) is a set of open source C libraries designed to support cross-platform development of security-enabled applications. NSS implements major Internet security standards. NSS is available free of charge under a variety of open source compatible licenses. See http://www.mozilla.org/projects/security/pki/nss/." *10/07/09: Update OES;*
15	RSA Security Inc. 177 Bovet Road, Suite 200 San Mateo, CA 94402 USA -Kathy Kriese TEL: 650-931-9781	**RSA BSAFE® Crypto-J Software Module** **Version 4.1**	Intel Pentium D w/ Windows XP Professional SP2, Sun JRE 5.0; Intel Pentium D w/ Windows XP Professional SP2, Sun JRE 6.0	6/26/2009	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#621)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#130) (SHS Val#1032) "RSA BSAFE Crypto-J security software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. It supports a wide range of industry standard encryption algorithms offering Java developers the flexibility to choose the option most appropriate to meet their requirements."
14	SPYRUS, Inc. 1860 Hartog Drive San Jose, CA 95131-2203 USA -Tom Dickens TEL: 408-392-4324 FAX: 408-392-0319	**Hydra PC Locksmith Board 3 Level 2 (ARM)** **Part # 880074001F, v03.00.04**	N/A	6/17/2009	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#1027)] "The Hydra PC Data Traveler is a multifunctional USB security device combining security token and portable secure storage drive features with the strongest hardware-based encryption technology commercially available for protection of user data files. The Hydra PC Locksmith is a multifunctional USB security device combining security token and portable secure storage drive features with the strongest hardware-based encryption technology commercially available for protection of user data files." *07/07/09: Update implementation description;*
13	Pitney Bowes Inc. 35 Waterview Drive Shelton, CT 06484-8000 USA -Robert Sisson TEL: 203-924-3061 FAX: 203-924-3518	**Sigma ASIC - DRBG/RNG** **Version 01.00.0002 (Firmware)**	ARM7-TDMI	5/7/2009	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#650)] "The Pitney Bowes Cygnus X-3 Postal Security Device (PSD) is designed in compliance with FIPS 140-2 and IPMAR standards to support the USPS IBIP and international digital indicia standards globally. The PSD employs strong cryptographic and physical security techniques for the protection of customer funds in Pitney Bowes Postage Metering products." *Prediction resistance not supported;*
12	DeltaCrypt Technologies Inc. 261A, chemin des Epinettes Piedmont, Quebec J0R 1K0 Canada	**DeltaCrypt Cryptographic Library** **Version 1.0.0.0**	Intel Celeron w/ Microsoft Windows Server 2003; Intel Pentium 4 w/ Microsoft Windows 2000; Intel Pentium 4 w/ Microsoft Windows Vista; Intel Pentium 4 w/ Microsoft Windows XP	4/30/2009	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#1065)]

	-Ann Marie Colizza TEL: 450-744-0137 FAX: 450-227-9043 -Olivier Fournier TEL: 450-227-6622 FAX: 450-227-9043				"DeltaCrypt Cryptographic Library implements the cryptographic functionalities for DeltaCrypt Encryption applications. DeltaCrypt provides sensitive data protections for computers, laptops, USB mass storage devices as well as CDs/DVDs."
11	Oracle Corporation 500 Eldorado Blvd., Bldg 5 Broomfield, CO 80021 USA -David Hostetter TEL: 303-272-7126	**T9840D DRBG nist_CTR_DRBG** **Version 1.0 (Firmware)**	ARM ARM7TDMI	4/30/2009	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#1061)] "This algorithm is used by the Sun StorageTek T9840D Tape Drive." *04/24/09: Update implementation information;*
10	SPYRUS Inc. 1860 Hartog Drive San Jose, CA 95131-2203 USA -Tom Dickens TEL: 408-392-9131 FAX: 408-392-0319	**Hydra PC Locksmith (ARM)** **Part # 88007021F, v03.00.04**	N/A	3/12/2009	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#972)] "The Hydra PC Locksmith is a multifunctional USB security device combining security token and portable secure storage drive features with the strongest hardware-based encryption technology commercially available for protection of user data files."
9	Redline Communications Inc. 302 Town Centre Blvd., 4th Floor Markham, Ontario L3R OE8 Canada -Leigh Chang TEL: 905-479-8344 x2507 -Lee Lipes TEL: 905-479-8344 x2480	**Redline Broadband Wireless Infrastructure Radio Cryptographic Library** **Version 1.0 (Firmware)**	Intel IXP420 w WindRiver VxWorks 6.5	2/19/2009	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-256) (SHS Val#962)] "This is a firmware library that provides the cryptographic functions used on Redline's industry leading reliable, secure and high performance broadband wireless products." *03/12/09: Update implementation information;*
8	Harris Corporation (RF Communications Division) 1680 University Avenue Rochester, New York 14610 USA -Elias Theodorou TEL: 585-720-8790 FAX: 585-241-8459	**Harris Broadband Ethernet Radio Cryptographic Library** **Version 1.0 (Firmware)**	Intel IXP420 w/ WindRiver VxWorks 6.5	2/19/2009	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-256) (SHS Val#961)] "This is a firmware library that provides the cryptographic functions used on Harris' industry leading reliable, secure and high performance broadband Ethernet radio products." *03/12/09: Update implementation information;*
7	Midland Radio Corporation 5900 Parretta Drive Kansas City, Missouri 64120 United States -Dave Berneking TEL: 816-462-0421	**Midland Radio Base Station Implementation** **Version 1.0 (Firmware)**	TI TMS320VC5509A DSP	2/5/2009	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (HMAC Val#548)] "Implemented on a TI TMS320VC5509A DSP in firmware under the control of a Hitachi H8 Host Processor. No Operating System is used. The Algorithms are used on Midland BTIII Base Stations provide encrypted and clear voice, data and Short Message Service communications in accordance with the Project 25 standard."
6	Oracle Corporation 500 Eldorado Blvd., Bldg 5 Broomfield, CO 80021 USA -David Hostetter TEL: 303-272-7126	**SP 800-90 Firmware-based CTR RBG** **Version 1.0 (Firmware)**	ARM926EJ	11/26/2008	**CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#942)] "The Sun T10000A and T10000B tape drives produce cryptographically secure random numbers by using an internal source with high entropy, coupled with an SP 800-90 CTR DRBG based on AES-256."
5	Midland Radio Corporation 5900 Parretta Drive Kansas City, Missouri 64120 United States -David Kingsolver TEL: 816-462-0421	**Midland Radio Cryptographic Module** **Version 1.0 (Firmware)**	Texas Instruments C54 DSP Processor	11/26/2008	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-256) (HMAC Val#521)] "Implemented on a TI C54 DSP in firmware under the control of a Renesas M16C62 Host Processor. No Operating System is used. The algorithms are used on Midland Mobile, Trunk, Portable and Desk mount radio products to provide encrypted voice, data and short message services compatible with the P25 Standard."
4	RSA The Security Division of EMC 177 Bovet Road, Suite 200 San Mateo, CA 94402 USA -Kathy Kriese TEL: 650-931-9781	**RSA BSAFE Crypto-C Micro Edition (ME)** **Version 3.0.0.1**	Intel Celeron w/ Microsoft Windows XP Professional SP2; AMD Athlon X2 w/ Microsoft Windows Vista Ultimate; Intel Celeron w/ Red Hat Enterprise Linux AS 4.0 w/ LSB 3.0.3	9/11/2008	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#477)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-

					384 , SHA-512) (ECDSA Val#98) (SHS Val#855) "RSA BSAFE® Crypto-C ME software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. The software supports a wide range of industry standard encryption algorithms offering developers the flexibility to choose the appropriate option to meet their requirements."
3	SPYRUS Inc. 1860 Hartog Drive San Jose, CA 95131-2203 USA -Tom Dickens TEL: 408-392-5124 FAX: 408-392-0319	**Hydra PC Series II Oki** **Version P/N 730070001, v01.02.12 (Firmware)**	ARM 9 TDMI 32-bit Processor	9/11/2008	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-512) (SHS Val#852)] "The Hydra Privacy Card (Hydra PC) Series II, Personal Encryption Device and Enterprise Edition, is a multifunctional USB security device combining security token and portable secure storage drive features with the strongest hardware-based encryption technology commercially available for protection of user data files."
2	RSA Security Inc. 177 Bovet Road, Suite 200 San Mateo, CA 94402 USA -Kathy Kriese TEL: 650-931-9781	**RSA BSAFE Crypto-C Micro Edition (ME)** **Version 3.0**	IBM Power3 w/ AIX 5L 5.3 (32-bit); IBM Power3 w/ AIX 5L 5.3 (64-bit); PA-RISC 2.0 w/ HP-UX 11i v1 (32-bit); PA-RISC 2.0W w/HP-UX 11i v2 (64-bit); Intel Itanium2 w/ HP-UX 11i v3 (32-bit); Intel Itanium2 w/ HP-UX 11i v3 (64-bit); Intel Celeron w/ Red Hat Enterprise Linux AS 4.0 (32-bit w/ LSB 3.0.3); Intel AMD Athlon X2 w/ Red Hat Enterprise Linux AS 5.0 (64-bit w/ LSB 3.0.3); SPARC V8 w/ Solaris 10 (32-bit); SPARC V8+ w/ Solaris 10 (32-bit); SPARC V9 w/ Solaris 10 (64-bit); AMD Opteron w/ Solaris 10 (64-bit); PowerPC 603 w/ VxWorks 5.5; PowerPC 604 w/ VxWorks 5.5; PowerPC 604 w/ VxWorks 6.0; Intel PXA250 w/ Windows Mobile 2003; Intel PXA270 w/ Windows Mobile 5; Intel PXA270 w/ Windows Mobile 6.0; AMD Athlon X2 w/ Windows Server 2003 SP2 (64-bit w/ MT Static Wrap); Intel Itanium2 w/ Windows Server 2003 SP2 (64-bit w/ MT Static Wrap); Intel Itanium2 w/ Windows Server 2003 SP2 (w/ MD Dynamic Wrap); Intel Pentium M w/ Windows XP Professional SP2 (w/ MT Static Wrap); AMD Athlon X2 w/ Windows Vista Ultimate (32-bit w/ MD Dynamic Wrap); Intel Pentium D w/ Windows Vista Ultimate (64-bit w/ MD Dynamic Wrap)	7/3/2008	**HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#449)] **Dual_EC_DRBG**:[Prediction Resistance Tested: Not Enabled (P-256: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-384: SHA-224 , SHA-256 , SHA-384 , SHA-512) (P-521: SHA-256 , SHA-384 , SHA-512) (ECDSA Val#92) (SHS Val#807) "RSA BSAFE® Crypto-C ME software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. The software supports a wide range of industry standard encryption algorithms offering developers the flexibility to choose the appropriate option to meet their requirements."
1	Certicom Corp. 5520 Explorer Drive., 4th Floor Mississauga, Ontario L4W 5L1 Canada -Atsushi Yamada TEL: 905-501-3884 FAX: 905-507-4230 -Rob Williams TEL: 905-501-3887 FAX: 905-507-4230	**Security Builder GSE-J Crypto Core** **Version 2.2**	Intel Core 2 Duo w/ Windows 2008 Server 64-bit w/ JRE 1.6.0; Intel Pentium III w/ Linux Redhat AS5 32 Bit w/ JRE 1.6.0; Intel Pentium D w/ Redhat Linux AS5 64 bit w/ JRE 1.6.0; Sun UltraSPARC III w/ Solaris 10 32 Bit w/ JRE 1.6.0; Sun UltraSPARC III w/ Solaris 10 64 bit w/ JRE 1.6.0; Intel Pentium D w/ Windows Vista 32 bit w/ JRE 1.6.0; Intel Core 2 Duo w/ Windows Vista 64 bit w/JRE 1.6.0; Intel Celeron w/ NetBSD v2.0.3 w/ CDC 1.1; PMC-SierraRM7035C-533L w/ NetBSD v2.0.3 w/ CDC 1.1	6/13/2008	**Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#802)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512256) (HMAC Val#444)] **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#804)] "Security Builder GSE-J is a standards-based cryptographic toolkit written in Java. It supports optimized Elliptic Curve Cryptography and provides application developers with sophisticated tools to flexibly integrate encryption, digital signatures and other security mechanisms into Java-based applications." *11/19/09: Add new tested OES';* *11/23/09: Update implementation information;*