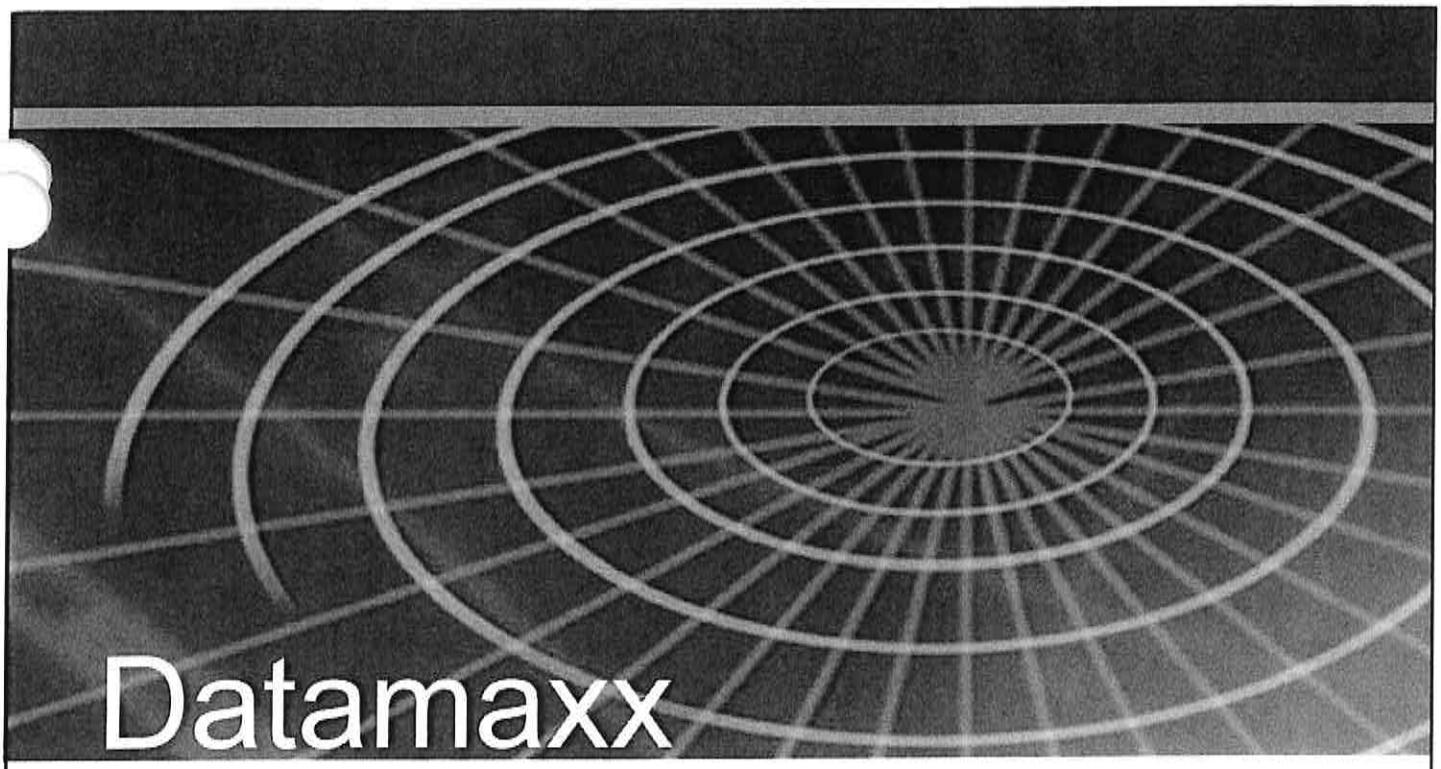


OMNIXX

Datamaxx's Support of the Current FBI CJIS Security Policy Encryption

www.Datamaxx.com

Datamaxx®
APPLIED TECHNOLOGIES

DATAMAXX'S SUPPORT OF THE CURRENT FBI CJIS SECURITY POLICY ENCRYPTION

The Omnixx Enterprise solution uses a variety of certified encryption modules to meet the FIPS 140-2 encryption requirement depending upon the client application. Certified encryption implementations include: RSA BSAFE (NIST Certificate #1047), Microsoft cryptographic libraries (NIST Certificate Numbers #1333, #1334, #1335, #1321, and #1337), BlackBerry Cryptographic Kernel (NIST Certificate #1083), and Network Security Services Cryptographic Module (NIST Certificate #1278). The certifications showing that these meet FIPS 140-2 compliancy are available from the NIST site at http://csrc.nist.gov/cryptval/140-1/140val-all.htm.

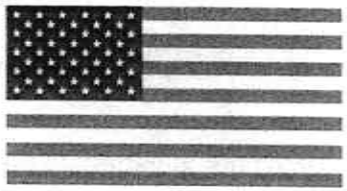
Certificates #1047, #1083, #1278, #1321, #1333, #1334, #1335 and #1337 are provided in **Appendix A**.

DATAMAXX'S SUPPORT OF THE CURRENT FBI CJIS SECURITY POLICY ADDITIONAL AREAS

Additionally, Datamaxx products are fully compliant with other areas of the FBI CJIS Security policy as they pertain to:

- Password Management
- Password Strength
- Identity Management
- Advanced Authentication

FIPS 140-2 Validation Certificate



The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. 1337

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

Windows Server 2008 R2 Enhanced Cryptographic Provider (RSAENH) *by* Microsoft Corporation

(When operated in FIPS mode with Windows Server 2008 R2 Code Integrity (ci.dll) validated to FIPS 140-2 under Cert. #1334 operating in FIPS mode and Microsoft Windows Server 2008 R2 Kernel Mode Cryptographic Primitives Library (cng.sys) validated to FIPS 140-2 under Cert. #1335 operating in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

Windows Server 2008 R2 Enhanced Cryptographic Provider (RSAENH) *by* Microsoft Corporation
(*Software Version: 6.1.7600.16385;* Software)

---

and tested by the Cryptographic Module Testing accredited laboratory: *SAIC CSTL, NVLAP Lab Code 200492-0*
CRYPTIK Version 7.0
is as follows:

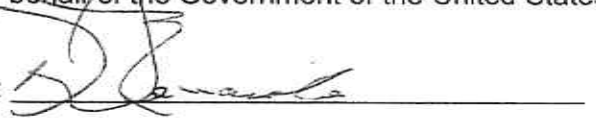
Cryptographic Module Specification:	Level 1	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: *(Multi-Chip Standalone)*	Level N/A	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 1	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level 1	*tested in the following configuration(s):*	Microsoft Windows Server 2008 R2 (x64 Version); Microsoft Windows Server 2008 R2 (IA64 version) (single-user mode)

The following FIPS approved Cryptographic Algorithms are used: **AES (Cert. #1168); DRBG (Cert. #23); HMAC (Cert. #687); SHS (Cert. #1081); RSA (Certs. #559 and #568); Triple-DES (Cert. #846)**

The cryptographic module also contains the following non-FIPS approved algorithms: **DES; MD2; MD4; MD5; RC2; RC4; RSA (key wrapping; key establishment methodology provides between 80 and 256-bits of encryption strength)**

Overall Level Achieved: 1

Signed on behalf of the Government of the United States

Signature: 

Dated: 19 Aug 2010

Chief, Computer Security Division
National Institute of Standards and Technology

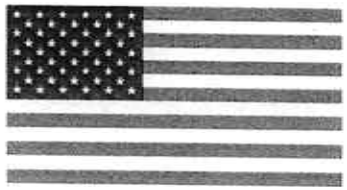
Signed on behalf of the Government of Canada

Signature: 

Dated: August 13, 2010

Director, Industry Program Group
Communications Security Establishment Canada

FIPS 140-2 Validation Certificate



The National Institute of Standards and Technology of the United States of America

TM

The Communications Security Establishment of the Government of Canada

Certificate No. 1335

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

Microsoft Windows Server 2008 R2 Kernel Mode Cryptographic Primitives Library (cng.sys) *by* Microsoft Corporation

(When operated in FIPS mode with Windows Server 2008 R2 Winload OS Loader (winload.exe) validated to FIPS 140-2 under Cert. #1333 operating in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

Microsoft Windows Server 2008 R2 Kernel Mode Cryptographic Primitives Library (cng.sys) *by* Microsoft Corporation
(*Software Version: 6.1.7600.16385;* Software)

and tested by the Cryptographic Module Testing accredited laboratory: *SAIC CSTL, NVLAP Lab Code 200492-0*
CRYPTIK Version 7.0
is as follows:

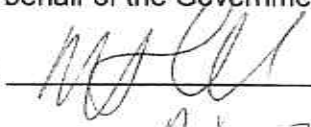
Cryptographic Module Specification:	Level 1	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: *(Multi-Chip Standalone)*	Level N/A	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 1	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level 1	*tested in the following configuration(s):*	Microsoft Windows Server 2008 R2 (x64 Version); Microsoft Windows Server 2008 R2 (IA64 version) (in single-user mode)

The following FIPS approved Cryptographic Algorithms are used: **AES (Certs. #1168 and #1187); AES GCM (Cert. #1168, vendor-affirmed); AES GMAC (Cert. #1168, vendor-affirmed); DRBG (Certs. #23 and #27); ECDSA (Cert. #142); HMAC (Cert. #686); KAS (SP 800-56A, vendor affirmed, key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength); RNG (Cert. #649); RSA (Certs. #559 and #567); SHS (Cert. #1081); Triple-DES (Cert. #846)**

The cryptographic module also contains the following non-FIPS approved algorithms: **AES (Cert. #1168, key wrapping; key establishment methodology provides between 128 and 256 bits of encryption strength); DES; Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 150 bits of encryption strength; non-compliant less than 80 bits of encryption strength); MD2; MD4; MD5; HMAC MD5; RC2; RC4**

Overall Level Achieved: 1

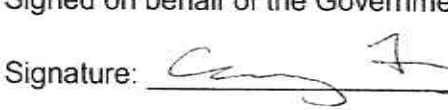
Signed on behalf of the Government of the United States

Signature: 

Dated: Aug 12, 2010

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: 

Dated: August 10, 2010

Director, Industry Program Group
Communications Security Establishment Canada

FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

TM

The Communications Security Establishment of the Government of Canada

Certificate No. 1334

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

Windows Server 2008 R2 Code Integrity (ci.dll) *by* Microsoft Corporation

(When operated in FIPS mode with Windows Server 2008 R2 Winload OS Loader (winload.exe) validated to FIPS 140-2 under Cert. #1333 operating in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

Windows Server 2008 R2 Code Integrity (ci.dll) *by* Microsoft Corporation
(*Software Version: 6.1.7600.16385;* Software)

---

and tested by the Cryptographic Module Testing accredited laboratory: ***SAIC CSTL, NVLAP Lab Code 200492-0***
CRYPTIK Version 7.0

is as follows:

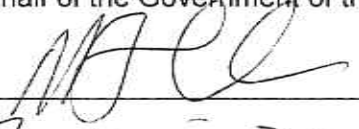
Cryptographic Module Specification:	Level 1	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: (Multi-Chip Standalone)	Level N/A	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 1	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level 1	*tested in the following configuration(s):* Microsoft Windows Server 2008 R2 (x64 Version); Microsoft Windows Server 2008 R2 (IA64 version) (single-user mode)	

The following FIPS approved Cryptographic Algorithms are used: RSA (Cert. #568); SHS (Cert. #1081)

The cryptographic module also contains the following non-FIPS approved algorithms: MD5

Overall Level Achieved: 1

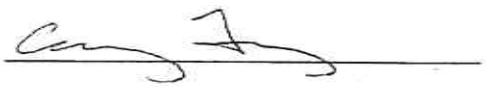
Signed on behalf of the Government of the United States

Signature: 

Dated: JUNE 15, 2010

Chief, Computer Security Division
National Institute of Standards and Technology

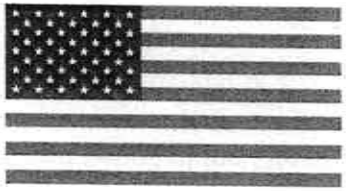
Signed on behalf of the Government of Canada

Signature: 

Dated: June 10, 2010

Director, Industry Program Group
Communications Security Establishment Canada

FIPS 140-2 Validation Certificate



The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. 1333

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

Windows Server 2008 R2 Winload OS Loader (winload.exe) *by* Microsoft Corporation

(When operated in FIPS mode with Windows Server 2008 R2 Boot Manager (bootmgr) validated to FIPS 140-2 under Cert. #1321 operating in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

Windows Server 2008 R2 Winload OS Loader (winload.exe) *by* Microsoft Corporation
(*Software Version: 6.1.7600.16385;* Software)

---

and tested by the Cryptographic Module Testing accredited laboratory: ***SAIC CSTL, NVLAP Lab Code 200492-0***
CRYPTIK Version 7.0
is as follows:

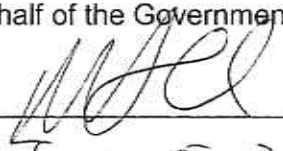
Cryptographic Module Specification:	Level 1	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: *(Multi-Chip Standalone)*	Level N/A	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 1	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level 1	*tested in the following configuration(s):*	Microsoft Windows Server 2008 R2 (x64 Version); Microsoft Windows Server 2008 R2 (IA64 version) (single-user mode)

The following FIPS approved Cryptographic Algorithms are used: AES (Certs. #1168 and #1177); RSA (Cert. #568); SHS (Cert. #1081)

The cryptographic module also contains the following non-FIPS approved algorithms: MD5

Overall Level Achieved: 1

Signed on behalf of the Government of the United States

Signature: 

Dated: June 15, 2010

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: 

Dated: June 10, 2010

Director, Industry Program Group
Communications Security Establishment Canada

FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. 1321

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

Windows Server 2008 R2 Boot Manager (bootmgr) *by* Microsoft Corporation

(When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

Windows Server 2008 R2 Boot Manager (bootmgr) *by* Microsoft Corporation
(*Software Version: 6.1.7600.16385;* Software)

---

and tested by the Cryptographic Module Testing accredited laboratory: ***SAIC CSTL, NVLAP Lab Code 200492-0***
CRYPTIK Version 7.0
is as follows:

Cryptographic Module Specification:	Level 1	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: *(Multi-Chip Standalone)*	Level N/A	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 1	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level 1	*tested in the following configuration(s):*	Microsoft Windows Server 2008 R2 (x64 Version); Microsoft Windows Server 2008 R2 (IA64 version) (single-user mode)

The following FIPS approved Cryptographic Algorithms are used: **AES (Certs. #1168 and #1177); HMAC (Cert.#675); RSA (Cert. #568); SHS (Cert. #1081)**

The cryptographic module also contains the following non-FIPS approved algorithms: **MD5**

Overall Level Achieved: 1

Signed on behalf of the Government of the United States

Signature: Tomas F. Bodson

Dated: June 22, 2010

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: June 15, 2010

Director, Industry Program Group
Communications Security Establishment Canada

FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

TM

The Communications Security Establishment of the Government of Canada

Certificate No. 1278

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

Network Security Services (NSS) Cryptographic Module (Basic ECC)
***by* Sun Microsystems, Inc., Red Hat, Inc. *and* Mozilla Foundation, Inc.**
(When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

Network Security Services (NSS) Cryptographic Module (Basic ECC)
***by* Sun Microsystems, Inc., Red Hat, Inc. *and* Mozilla Foundation, Inc.**
***(Software Version: 3.12.4;* Software)**

and tested by the Cryptographic Module Testing accredited laboratory:
is as follows:

Atlan Laboratories, NVLAP Lab Code 200492-0
CRYPTIK Version 7.0

Cryptographic Module Specification:	Level 1	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: *(Multi-Chip Standalone)*	Level N/A	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 1	*Mitigation of Other Attacks:*	Level 1
Operational Environment:	Level 1	*tested in the following configuration(s):*	Microsoft Windows XP with SP3; Apple Mac OS X 10.5 (single-user mode)

The following FIPS approved Cryptographic Algorithms are used: **AES (Cert. #1128); DSA (Cert. #368); DRBG (Cert. #18); ECDSA (Cert. #133); HMAC (Cert. #638); RSA (Cert. #535); SHS (Cert. #1050); Triple-DES (Cert. #823)**

The cryptographic module also contains the following non-FIPS approved algorithms: **Camelia; DES; Diffie-Hellman; EC Diffie-Hellman; MD2; MD5; RC2; RC4; SEED**

Overall Level Achieved: 1

Signed on behalf of the Government of the United States

Signature: Donna F. Dodson

Dated: March 29, 2010

Chief, Computer Security Division
National Institute of Standards and Technology

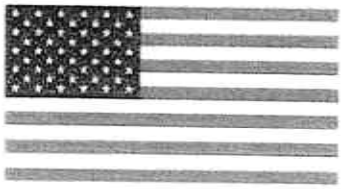
Signed on behalf of the Government of Canada

Signature:

Dated: March 23, 2010

Director, Industry Program Group
Communications Security Establishment Canada

FIPS 140-2 Validation Certificate



The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. 1083

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

BlackBerry Cryptographic Kernel *by* Research In Motion Ltd.

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

BlackBerry Cryptographic Kernel by Research In Motion Ltd.
(Firmware Versions: 3.8.5.42 and 3.8.5.48; Firmware)

and tested by the Cryptographic Module Testing accredited laboratory: *DOMUS IT Security Laboratory, NVLAP Lab Code 200017-0*
CRYPTIK Version 7.0
is as follows:

Cryptographic Module Specification:	Level 1	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: (Multi-Chip Standalone)	Level 1	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 3	*Mitigation of Other Attacks:*	Level 1
Operational Environment:	Level N/A	*tested in the following configuration(s):*	BlackBerry 9000 with BlackBerry OS Version 4.6

The following FIPS approved Cryptographic Algorithms are used: Triple-DES (Certs. #717 and #718); AES (Certs. #873, #874, #875 and #876); SHS (Certs. #867 and #868); HMAC (Certs. #489 and #490); RSA (Certs. #422 and #423); RNG (Certs. #501 and #502); ECDSA (Certs. #108 and #109)

The cryptographic module also contains the following non-FIPS approved algorithms: EC Diffie-Hellman (key agreement; key establishment methodology provides 256 bits of encryption strength); ECMQV (key agreement; key establishment methodology provides 256 bits of encryption strength)

Overall Level Achieved: 1

Signed on behalf of the Government of the United States

Signature: 

Dated: January 22, 2009

Chief, Computer Security Division
National Institute of Standards and Technology

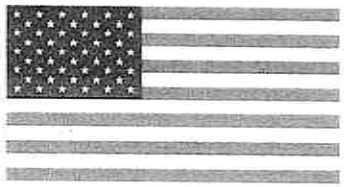
Signed on behalf of the Government of Canada

Signature: 

Dated: January 15, 2009

Director, Industry Program Group
Communications Security Establishment Canada

FIPS 140-2 Validation Certificate



The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. **1047**

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

RSA BSAFE® Crypto-J Software Module *by* RSA Security, Inc.

(When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

RSA BSAFE® Crypto-J Software Module *by* RSA Security, Inc.
(Software Version: 4.0; Software*)*

---

and tested by the Cryptographic Module Testing accredited laboratory: *Atlan Laboratories, NVLAP Lab Code 200492-0*
CRYPTIK Version 7.0
is as follows:

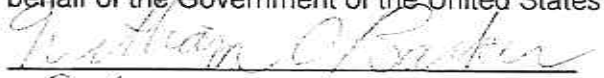
Cryptographic Module Specification:	Level 1	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: (Multi-Chip Standalone)	Level N/A	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 1	*Mitigation of Other Attacks:*	Level 1
Operational Environment:	Level 1	*tested in the following configuration(s):* 32-bit x86 Intel Pentium M w/ Windows XP SP2 Professional with Sun JRE 1.4.2; 32-bit x86 Intel Pentium M w/ Windows XP SP2 Professional with Sun JRE 1.5; 32-bit x86 Intel Pentium M w/ Windows XP SP2 Professional with Sun JRE 1.6 (single-user mode)	

The following FIPS approved Cryptographic Algorithms are used: **AES (Cert. #670); DSA (Cert. #252); ECDSA (Cert. #73); HMAC (Cert. #354); RNG (Cert. #390 and vendor affirmed: SP 800-90); RSA (Cert. #312); SHS (Cert. #703); Triple-DES (Cert. #615)**

The cryptographic module also contains the following non-FIPS approved algorithms: **AES-GCM (non-compliant); DES; Diffie-Hellman; DESX; ECAES; EC Diffie-Hellman; ECDHC; ECIES; MD2; MD5; PBE (SHA-1 and Triple-DES); RIPEMD 160; RNG (X9.31 non-compliant, MD5 and SHA-1); RC2; RC4; RC5; RSA OAEP (for key transport); Raw RSA; RSA Keypair Generation MultiPrime; RSA (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength; non-compliant less than 80 bits of encryption strength); HMAC-MD5**

Overall Level Achieved: 1

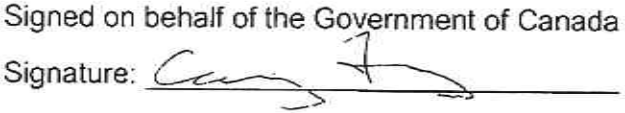
Signed on behalf of the Government of the United States

Signature: 

Dated: October 27, 2008

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: 

Dated: October 20, 2008

Director, Industry Program Group
Communications Security Establishment Canada

FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0003

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority, and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority, hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover several areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested and identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a unique assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions. Overall Level, Individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the ICs created Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: _____

Dated: _____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: _____

Director, Industry Program Group
Communications Security Establishment Canada

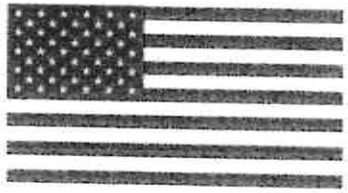
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1491	01/28/2011	HX280 Broadband Satellite Router	Hughes Network Systems, LLC	Hardware Version: Rev C.; Firmware Version: 6.8.0.3
1492	02/04/2011	IBM® z/OS® Version 1 Release 11 System SSL Cryptographic Module	IBM® Corporation	Hardware Version: FC3863 w/System Driver Level 77, CEX3A and CEX3C [CEX3A and CEX3C are separately configured versions of 4765-001 (P/N 45D6048)]; Software Version: System SSL level HCPT3B0/JCPT3B1 with APAR OA31595, RACF level HRF7760 with APAR OA30951 and ICSF level HCR7770 with APAR OA32012; Firmware Version: 4765-001 (e1ced7a0)
1496	02/10/2011	Cisco Secure Access Control Server (ACS) FIPS module (cryptolib)	Cisco Systems, Inc.	Software Version: 1.1
1497	02/10/2011	Cisco Secure Access Control Server (ACS) FIPS module (NSS)	Cisco Systems, Inc.	Software Version: 3.12.5
1498	02/10/2011	PA-500, PA-2000 Series and PA-4000 Series Firewalls	Palo Alto Networks	Hardware Version: HW P/N 910-000006-00D Rev. D with FIPS Kit P/N 920-000005-001 Rev. 1 (PA-500), HW P/N 910-000004-00K Rev. K with FIPS Kit P/N 920-000004-001 Rev. 1 (PA-2020), HW P/N 910-000003-00K Rev. K with FIPS Kit P/N 920-000004-001 Rev. 1 (PA-2050), HW P/N 910-000002-00Q Rev. Q with FIPS Kit P/N 920-000003-001 Rev. 1 (PA-4020), HW P/N 910-000001-00P Rev. P with FIPS Kit P/N 920-000003-001 Rev. 1 (PA-4050) and HW P/N 910-000005-00G Rev. G with FIPS Kit P/N 920-000003-001 Rev. 1 (PA-4060); Firmware Version: 3.1.2
1500	02/10/2011	Pragma Systems Cryptographic Module	Pragma Systems, Inc.	Software Version: 1.0.0.12

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1501	02/24/2011	Cryptographic Module for F5 and CS	ActivIdentity, Inc.	Software Version: 1.7.0.4
1502	02/24/2011	RSA BSAFE® Crypto-J JSAFE and JCE Software Module	RSA, The Security Division of EMC	Software Version: 5.0
1503	02/24/2011	RSA BSAFE® Crypto-J JSAFE and JCE Software Module	RSA, The Security Division of EMC	Software Version: 5.0
1504	02/24/2011	Data Locker Enterprise, V2.0	Data Locker Inc.	Hardware Versions: P/Ns DL500E2 and DL1000E2; Firmware Version: 2.30
1505	02/24/2011	IBM 4765 Cryptographic Coprocessor Security Module	IBM® Corporation	Hardware Version: P/N 45D6048 Version 1.0; Firmware Version: e1ced7a0

FIPS 140-2 Validation Certificate



The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. 1436

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580-20 *and* 5580-40 Security Appliances *by* Cisco Systems, Inc.

(When operated in FIPS mode and with the tamper evident seals installed as indicated in the Security Policy)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FI -2 provides four increasing, qualitative levels of security , Level 2, Level 3, and Level 4. These levels are intenc over the range and potential applications and environments in whic cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580-20 and 5580-40 Security Appliances by Cisco Systems, Inc. (*Hardware Versions: 5505 [1,2], 5510 [1], 5520 [1], 5540 [1], 5550 [1], 5580-20 [3], 5580-40 [3], [FIPS Kit (Cisco-FIPSKIT=): Revision -B0] [1], [ASA 5505 FIPS Kit (ASA5505-FIPS-KIT=): Revision -A0] [2] and [ASA 5580 FIPS Kit (ASA5580-FIPS-KIT=)] [3]; Firmware Version: 8.3.2;* Hardware)

and tested by the Cryptographic Module Testing accredited laboratory: *SAIC CSTL, NVLAP Lab Code 200492-0*
CRYPTIK Version 7.0
is as follows:

Cryptographic Module Specification:	Level 2	*Cryptographic Module Ports and Interfaces:*	Level 2
Roles, Services, and Authentication:	Level 3	*Finite State Model:*	Level 2
Physical Security: *(Multi-Chip Standalone)*	Level 2	*Cryptographic Key Management:*	Level 2
EMI/EMC:	Level 2	*Self-Tests:*	Level 2
Design Assurance:	Level 3	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level N/A	*tested in the following configuration(s):*	N/A

The following FIPS approved Cryptographic Algorithms are used: AES (Certs. #105, #564, #1394 and #1407); HMAC (Certs. #125, #301, #818 and #828); RNG (Certs. #144, #329, #763 and #772); RSA (Certs. #106, #261, #680 and #684); SHS (Certs. #196, #630, #1265 and #1277); Triple-DES (Certs. #217, #559, #954 and #960)

The cryptographic module also contains the following non-FIPS approved algorithms: Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 112 bits of encryption strength; non-compliant less than 80 bits of encryption strength); MD5; DES; RC4; HMAC MD5; RSA (key wrapping; key establishment methodology provides 80 bits or 112 bits of encryption strength; non-compliant less than 80 bits of encryption strength)

Overall Level Achieved: 2

Signed on behalf of the Government of the United States

Signature: _____

Dated: November 3, 2010

Chief, Computer Security Division
National Institute of Standards and Technology

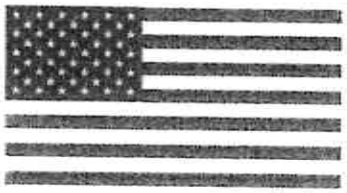
Signed on behalf of the Government of Canada

Signature: _____

Dated: October 29, 2010

Director, Industry Program Group
Communications Security Establishment Canada

FIPS 140-2 Validation Certificate



The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. 1337

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

Windows Server 2008 R2 Enhanced Cryptographic Provider (RSAENH) *by* Microsoft Corporation

(When operated in FIPS mode with Windows Server 2008 R2 Code Integrity (ci.dll) validated to FIPS 140-2 under Cert. #1334 operating in FIPS mode and Microsoft Windows Server 2008 R2 Kernel Mode Cryptographic Primitives Library (cng.sys) validated to FIPS 140-2 under Cert. #1335 operating in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

Windows Server 2008 R2 Enhanced Cryptographic Provider (RSAENH) *by* Microsoft Corporation
***(Software Version: 6.1.7600.16385;* Software)**

and tested by the Cryptographic Module Testing accredited laboratory: *SAIC CSTL, NVLAP Lab Code 200492-0*
CRYPTIK Version 7.0
is as follows:

Cryptographic Module Specification:	Level 1	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: (Multi-Chip Standalone)	Level N/A	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 1	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level 1	*tested in the following configuration(s):*	Microsoft Windows Server 2008 R2 (x64 Version); Microsoft Windows Server 2008 R2 (IA64 version) (single-user mode)

The following FIPS approved Cryptographic Algorithms are used: **AES (Cert. #1168); DRBG (Cert. #23); HMAC (Cert. #687); SHS (Cert. #1081); RSA (Certs. #559 and #568); Triple-DES (Cert. #846)**

The cryptographic module also contains the following non-FIPS approved algorithms: **DES; MD2; MD4; MD5; RC2; RC4; RSA (key wrapping; key establishment methodology provides between 80 and 256-bits of encryption strength)**

Overall Level Achieved: 1

Signed on behalf of the Government of the United States

Signature: _____

Dated: 12 Aug 2010

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: August 13 2010

Director, Industry Program Group
Communications Security Establishment Canada

FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0004

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its lifecycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a unique, assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions. Overall Level, Individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: _____

Dated: April 6, 2011

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: March 31, 2011

Director, Industry Program Group
Communications Security Establishment Canada

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1493	03/21/2011	Sony Security Module	Sony Corporation	Hardware Version: 1.1.0; Firmware Version: 1.1.0
1494	03/21/2011	Sony Security Module	Sony Corporation	Hardware Version: 1.0.1; Firmware Version: 1.0.1
1495	02/28/2011			
1506	02/28/2011			
1507	03/02/2011	F-Secure Kernel Mode Cryptographic Driver	F-Secure Corporation	Software Version: 2.3.9
1509	03/02/2011	CodeXML® FIPS Bluetooth® Modem	Code Corporation	Hardware Version: P/N BTHDFIPS-M2_01; Firmware Version: 0187
1510	03/02/2011	F-Secure Kernel Mode Cryptographic Driver for Linux	F-Secure Corporation	Software Version: 2.3.9
1511	03/04/2011	NITROX XL 1600-NFBE HSM Family	Cavium Networks	Hardware Versions: P/Ns CN1620-NFBE1NIC-2.0-G, CN1620-NFBE2NIC-2.0-G, CN1620-NFBE3NIC-2.0-G, CN1610-NFBE1NIC-2.0-G, CN1620-NFBE1-2.0-G, CN1620-NFBE2-2.0-G, CN1620-NFBE3-2.0-G and CN1610-NFBE1-2.0-G, Version: 2.0; Firmware Version: 2.0
1512	03/04/2011	SafeNet Encryptor, Model 650	SafeNet, Inc.	Hardware Versions: 904-53260-007, 904-53261-007, 904-53361-20p, 943-53270-007, 943-53271-007 and 943-53371-20p; Firmware Version: 4.0.2
1513	03/04/2011	SafeNet Encryptor, Model 600	SafeNet, Inc.	Hardware Versions: 904-10001-00x, 904-10002-00x, 904-10003-00x, 904-10014-00x, 904-10112-00x, 904-10113-00x, 904-20001-00x, 904-20002-00x, 904-20003-00x, 904-25005-00x, 904-30013-00x, 904-511I0-00p, 904-511I1-00p, 943-511I0-00p and 943-511I1-00p; Firmware Version: 4.0.2

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1514	03/09/2011	Apple FIPS Cryptographic Module	Apple Inc.	Software Version: 1.0
1515	03/09/2011	Motorola PTP 600 Series	Motorola, Inc.	Hardware Versions: P/Ns BP5830BHC, BP5830BHC15, BP5530BHC, BP5530BHC15, WB2781, WB3039, WB3037, WB3092, WB3094, WB3387, WB3389, WB3222, BP5830BH, BP5830BH15, BP5530BH, BP5530BH15, WB2780, WB3036, WB3038, WB3091, WB3093, WB3386, WB3388 and WB3221; P/N WB3593 (HW Security Upgrade Kit); Firmware Version: PTP600 08-50
1516	03/11/2011	HP Enterprise Secure Key Manager	Hewlett-Packard Company	Hardware Version: P/N AJ575A, Version 2.1; Firmware Version: 4.8.9

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1517	03/11/2011	Aruba 3000 and 6000/M3 Mobility Controllers with ArubaOS Firmware	Aruba Networks, Inc.	Hardware Versions: 3200: 3200-8-AOS-STD-FIPS-US; 3400: 3400-32-AOS-STD-FIPS-US; 3600: 3600-64-AOS-STD-FIPS-US; 6000: (6000-BASE-2PSU-200-FIPS or 6000-BASE-2PSU-400-FIPS) with [(minimum one: LC-2G-1, LC-2G24F-1 or LC-2G24FP-1) and (one or two: M3mk1-G10X-10G2X)] (no more than four total); 3200 Revision C4: 3200-8-AOS-STD-FIPS-US Revision C4; 3400 Revision C4: 3400-32-AOS-STD-FIPS-US Revision C4; 3600 Revision C4: 3600-64-AOS-STD-FIPS-US Revision C4; 6000 Revision C4: (6000-BASE-2PSU-200-FIPS or 6000-BASE-2PSU-400-FIPS) with [(minimum one: LC-2G-1, LC-2G24F-1 or LC-2G24FP-1) and (one or two: M3mk1-G10X-10G2X Revision C4)] (no more than four total); Firmware Versions: 3200, 3400 and 3600: A3000_3.3.2.0-FIPS, A3000_3.3.2.11-FIPS, A3000_3.3.2.14-FIPS, A3000_3.3.2.18-FIPS, A3000_3.3.2.19-FIPS, A3000_3.3.2.20-FIPS or A3000_3.4.2.3-FIPS; 6000: ArubaOS_MMC_3.3.2.0-FIPS, ArubaOS_MMC_3.3.2.11-FIPS, ArubaOS_MMC_3.3.2.14-FIPS, ArubaOS_MMC_3.3.2.18-FIPS, ArubaOS_MMC_3.3.2.19-FIPS, ArubaOS_MMC_3.3.2.20-FIPS or ArubaOS_MMC_3.4.2.3-FIPS
1518	03/11/2011	IMB	GDC Technology (USA), LLC	Hardware Version: GDC-IMB-v1; Firmware Version: 1.1