Cryptographic Module Validation Program (CMVP)

FIPS VALIDATED 140-2 ™

http://csrc.nist.gov/groups/STM/cmvp/index.html

Randall J. Easter, Director	reaster@nist.gov	301.975.4641
Beverly Trapnell, Deputy Director	trapnell@nist.gov	301.975.6745
Jim Fox	jfox@nist.gov	301.975.3642
Caroline Scace	cscace@nist.gov	301.975.8908
Kim Schaffer	kimsch@nist.gov	301.975.8375

Cryptographic Module Validation Program (CMVP)

- Purpose: to test and validate cryptographic modules to

  FIPS 140-2, *Security Requirements for Cryptographic Modules*

  - 11 Security Sections
  - 4 Security Assurance Levels

- Established by NIST and the Communications Security Establishment Canada (CSEC) in 1995

- Independent 3rd party conformance testing

- With the passage of the Federal Information Security Management Act of 2002, there is no longer a statutory provision to allow for agencies to waive mandatory Federal Information Processing Standards

- Therefore All cryptographic modules used by US Federal Government to protect non-classified sensitive information go through CMVP validation program

Cryptographic Module Validation Program (CMVP)

- International Standards Organization
  - ISO/IEC 19790 Security Requirements for Cryptographic Modules
    - Published March 2006
  - ISO/IEC 24759 Test requirements for cryptographic modules
    - Published July 2008

  Randall Easter (NIST CMVP) was the editor for both international standards

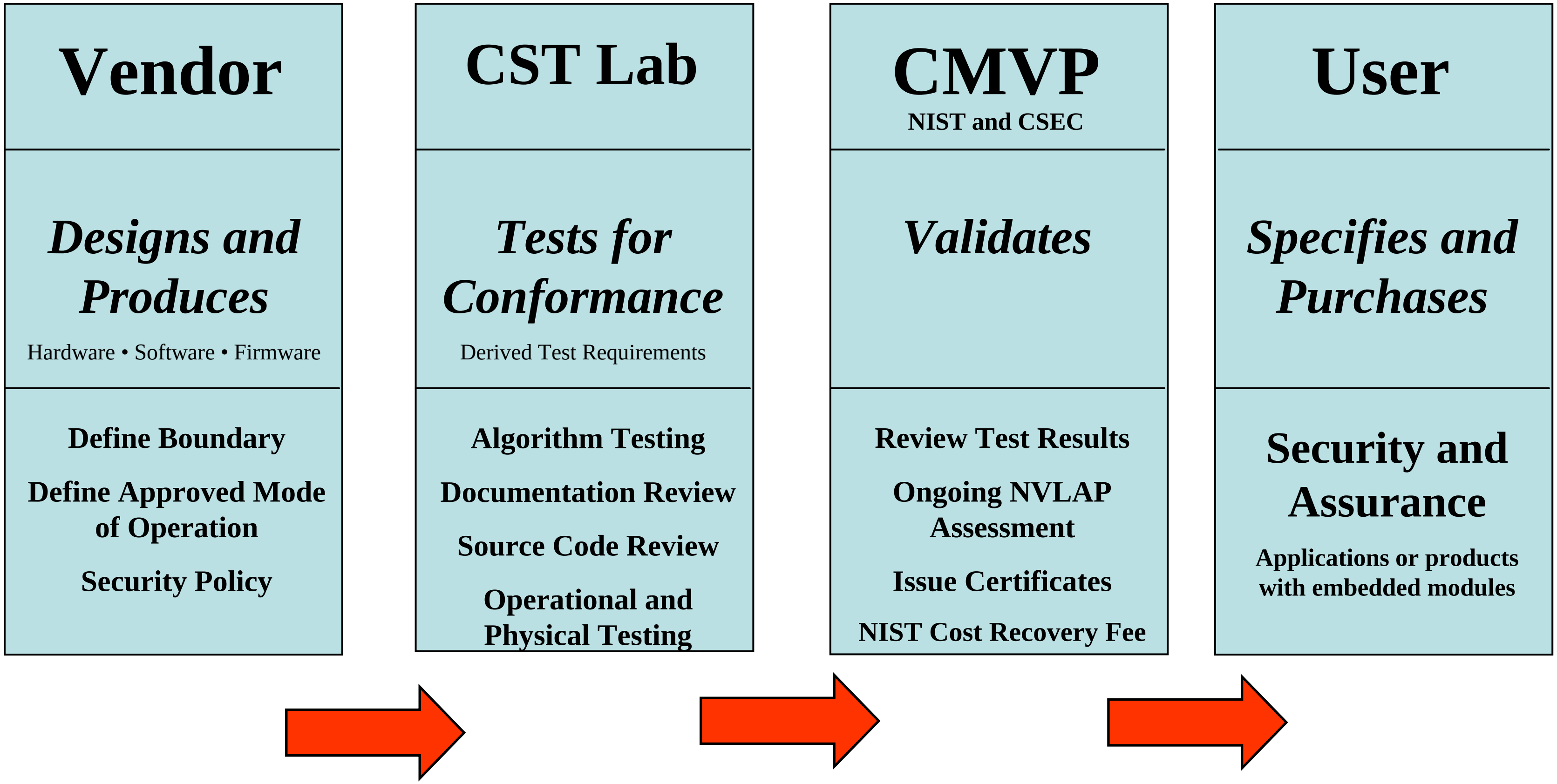
- Japanese Government Relationship (October 11, 2006)
  - Japan Cryptographic Module Validation Program (JCMVP)
    - Managed by the Information-Technology Promotion Agency (IPA), Japan
    - Support Japanese Laboratories to become accredited by NVLAP
    - Assist JCMVP regarding CMVP requirements and technical guidance

- Cryptographic and Security Testing Laboratories (CSTL) are accredited by the National Voluntary Laboratory Accreditation Program (NIST NVLAP)
  - Perform the 3rd party independent conformance testing
  - CMVP provides the technical assessors for laboratory accreditation

- Works jointly with the NIST Cryptographic Algorithm Validation Program (CAVP)
  - CAVP algorithmic validation is a prerequisite for CMVP module validation

- List of validated implementations posted publicly on CMVP website
  - http://csrc.nist.gov/groups/STM/cmvp/validation.html

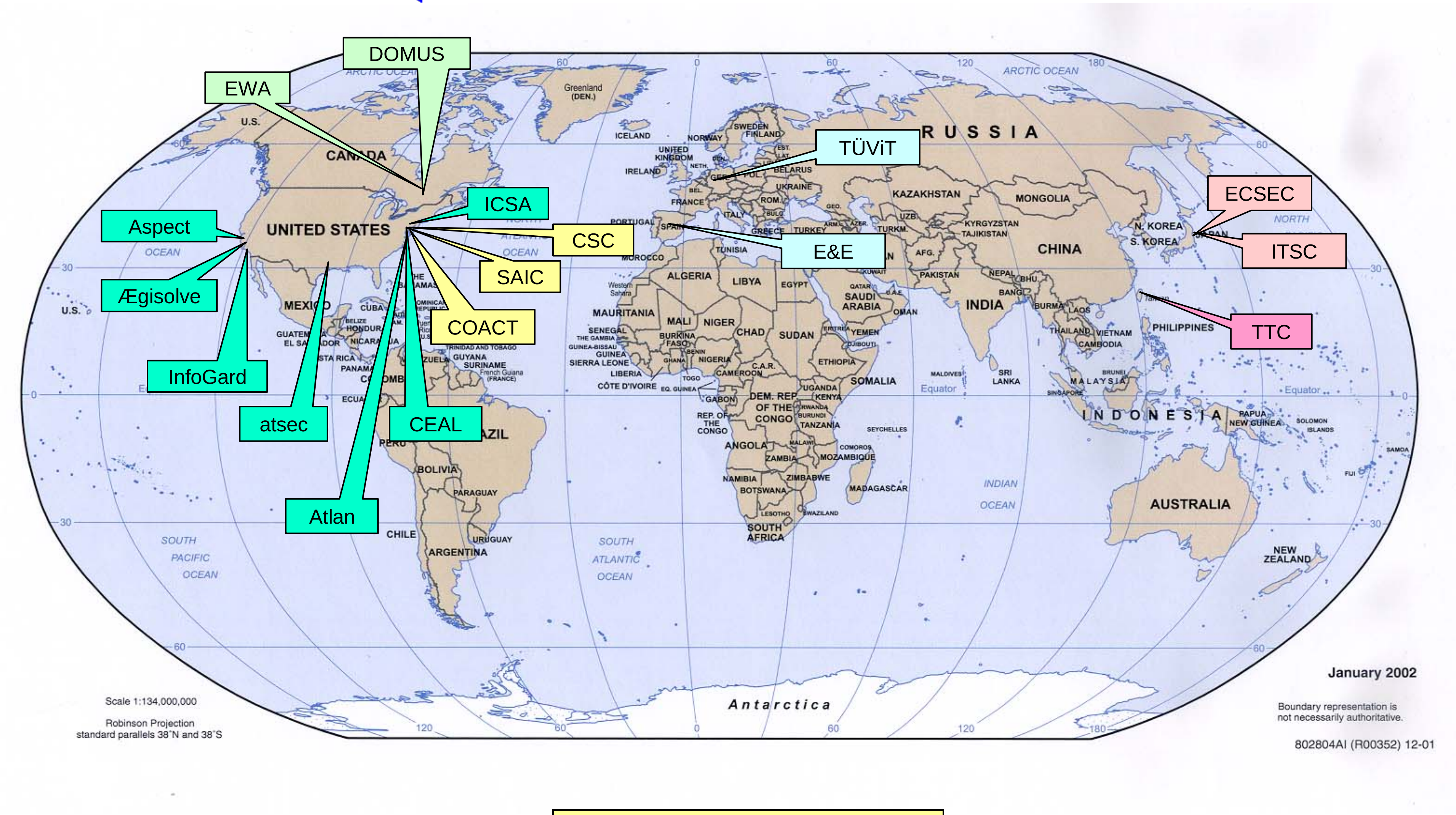
CMVP Testing and Validation Process for Cryptographic Module Implementations



Vendor	CST Lab	CMVP NIST and CSEC	User
Designs and Produces Hardware • Software • Firmware	*Tests for Conformance* Derived Test Requirements	*Validates*	*Specifies and Purchases*
Define Boundary **Define Approved Mode of Operation** **Security Policy**	**Algorithm Testing** **Documentation Review** **Source Code Review** **Operational and Physical Testing**	**Review Test Results** **Ongoing NVLAP Assessment** **Issue Certificates** **NIST Cost Recovery Fee**	**Security and Assurance** **Applications or products with embedded modules**

3 of the 10 US CST Labs reside in Maryland

NVLAP® Accredited CST Laboratories



January 2002

Scale 1:134,000,000

Robinson Projection
standard parallels 38°N and 38°S

Boundary representation is
not necessarily authoritative.

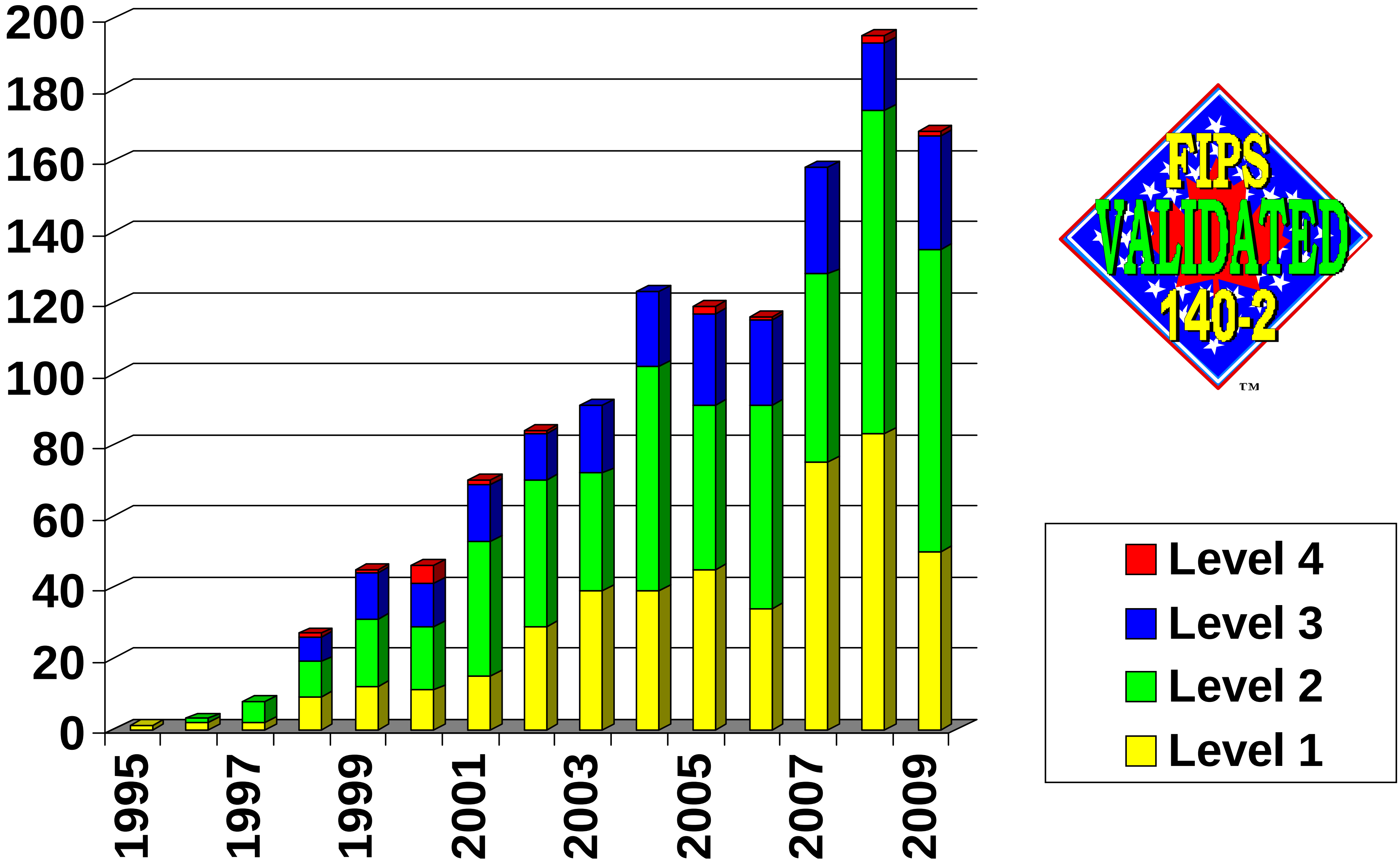
802804AI (R00352) 12-01

Maryland CST Labs

New domestic and international laboratory initial accreditation currently in process.

FIPS 140-1 and FIPS 140-2 Validation Certificates by Year and Level

(January 5 2010)



FIPS 140-2 Validation Certificate

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

FIPS VALIDATED 140-2 TM

The Communications Security Establishment of the Government of Canada

Certificate No. **1250**

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:

CipherOptics ESG100 *and* CipherOptics ESG1002 *by* CipherOptics, 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.

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments.

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:

CipherOptics ESG100 *and* CipherOptics ESG1002 *by* CipherOptics, Inc.
(Hardware Version: ESG100, A and ESG1002, A; Firmware Version: 2.3;* Hardware*)

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 2	*Cryptographic Module Ports and Interfaces:*	Level 2
Roles, Services, and Authentication:	Level 2	*Finite State Model:*	Level 2
Physical Security: *(Multi-Chip Standalone)*	Level 2	*Cryptographic Key Management:*	Level 2
EMI/EMC:	Level 3	*Self-Tests:*	Level 2
Design Assurance:	Level 2	*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: **Triple-DES (Cert. #258); AES (Cert. #156); SHS (Cert. #117); HMAC (Cert. #34); RSA (Cert. #209); RNG (Cert. #274)**

The cryptographic module also contains the following non-FIPS approved algorithms: **Diffie-Hellman (key agreement; key establishment methodology provides 90 bits of encryption strength); MD5; HMAC MD5; DES; NDRNG**

Overall Level Achieved: 2

Signed on behalf of the Government of the United States

Signature: For

Dated: December 29, 2009

Chief, Computer Security Division
National Institute of Standards and Technology

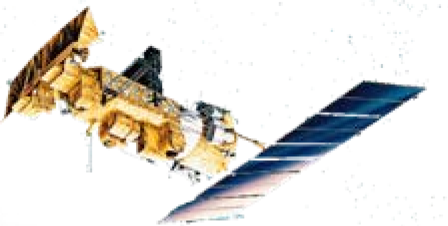
Signed on behalf of the Government of Canada

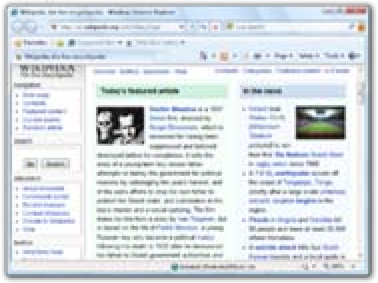
Signature:

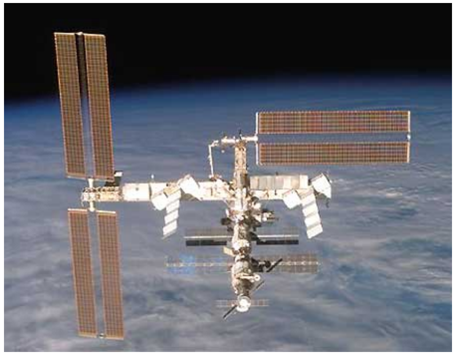
Dated: December 16, 2009

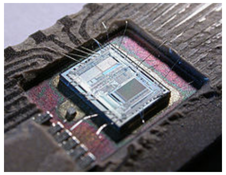
Director, Industry Program Group
Communications Security Establishment Canada

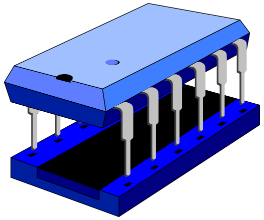
Examples of Cryptographic Modules or Products with embedded Cryptographic Modules











CMVP

Conformance Through Testing

FIPS VALIDATED 140-2 ™

Impact! … *Making a Difference*

- Cryptographic Modules Surveyed (during testing)
  - Percentage of modules that contained *at least* one security relevant non-conformance error
    - **59%** Level 1 and Level 2 Modules
    - **65%** Level 3 and Level 4 Modules
  - In addition
    - **96.3%** FIPS Interpretation and Documentation Errors
    - **~10%** Algorithm Implementation Errors
- ***Corrected** during testing and prior to CMVP validation*