Cryptographic Module Validation Program

Where security starts ….

5th Annual NIST IT Security Automation Conference

Randall J. Easter

Director, NIST CMVP

October 27, 2009

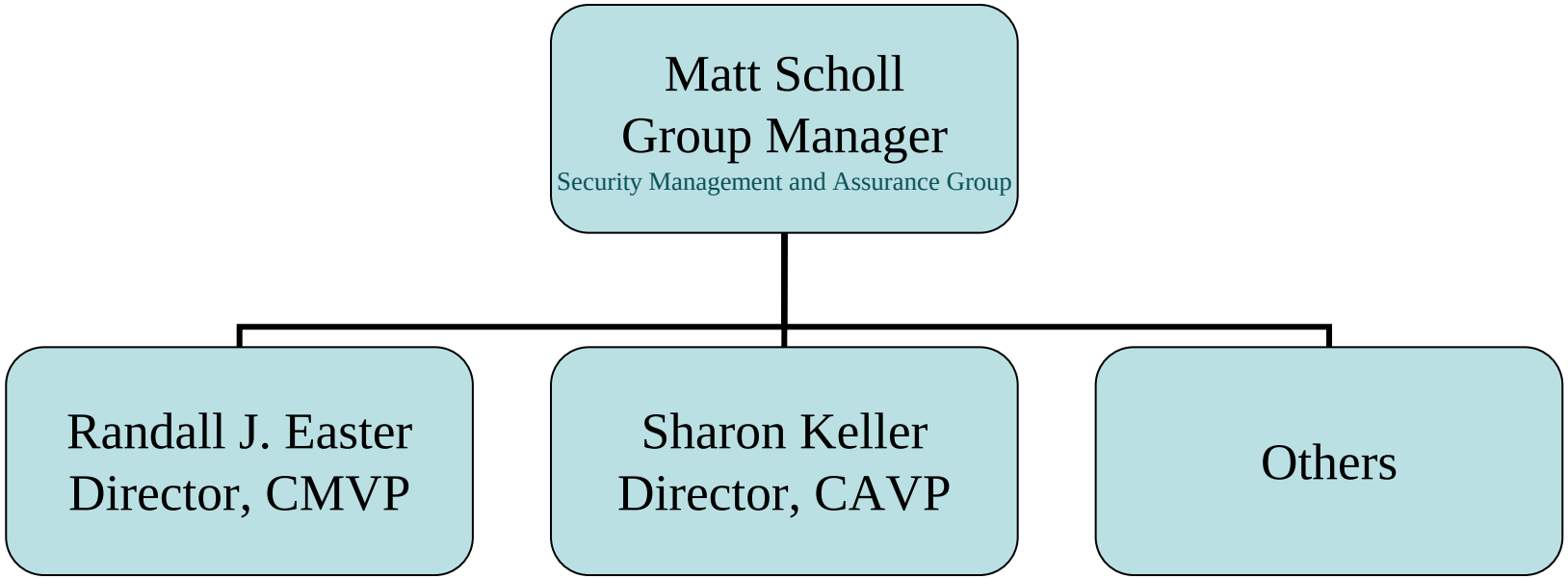
Agenda

- Organization
- CMVP
- Status
- FIPS 140-2
- Testing and Validation Process
- Maintaining validation

Security Management and Assurance

- **Cryptographic Module Validation Program (CMVP)**
  - Purpose: Independent 3rd party conformance testing to standards – FIPS 140-2
  - Established by NIST and the Communications Security Establishment Canada (CSEC) in 1995
  - Continued record growth in validations:
    - Over 1200 validated modules representing over 2500 modules
- **Cryptographic Algorithm Validation Program (CAVP)**
  - Purpose: to test and validate Approved algorithmic implementations

Security Management and Assurance Group
Computer Security Division
Information Technology Laboratory



Cryptographic Module Validation Program (CMVP)

- Purpose: to test and validate cryptographic modules to FIPS 140-2
- Established by NIST and the Communications Security Establishment Canada (CSEC) in 1995
- Original FIPS 140-1 requirements and updated FIPS 140-2 requirements developed with industry input

FIPS 140-2 and Applicability

- FIPS 140-2 specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information.
  - The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4.
  - The security requirements cover areas which include cryptographic module specification, cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.
- U.S. Federal organizations must use validated cryptographic modules
- 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.
  - Also includes enforcement mechanisms

International Recognition

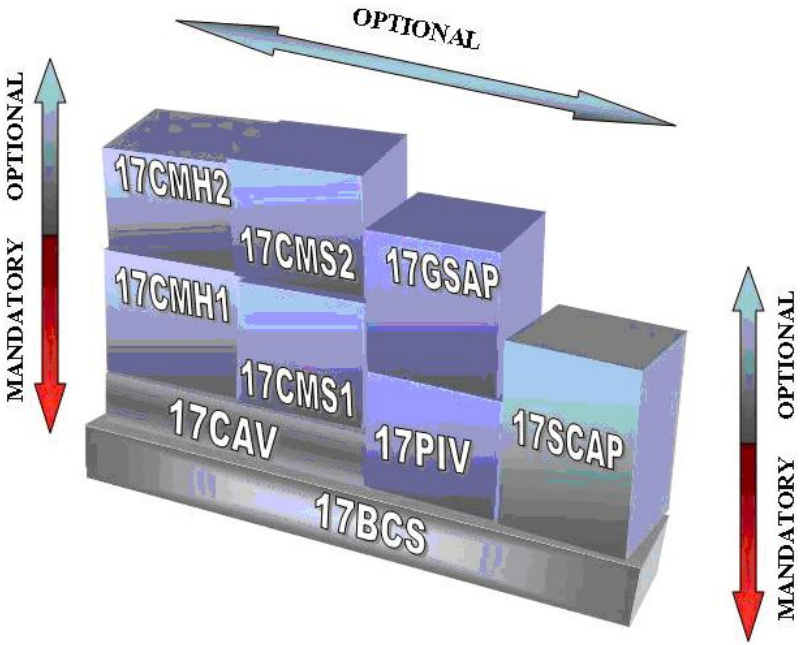
- **International Standards Organization**
  - ISO/IEC 19790 *Security Requirements for Cryptographic Modules*
    - *Published March 2006*
  - ISO/IEC 24759 *Test requirements for cryptographic modules*
    - *Published July 2008*
- **Japanese Government Relationship (October 11, 2006)**
  - Japan Cryptographic 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

NVLAP

National Voluntary Laboratory Accreditation Program

Accredits laboratories in 23 technologies

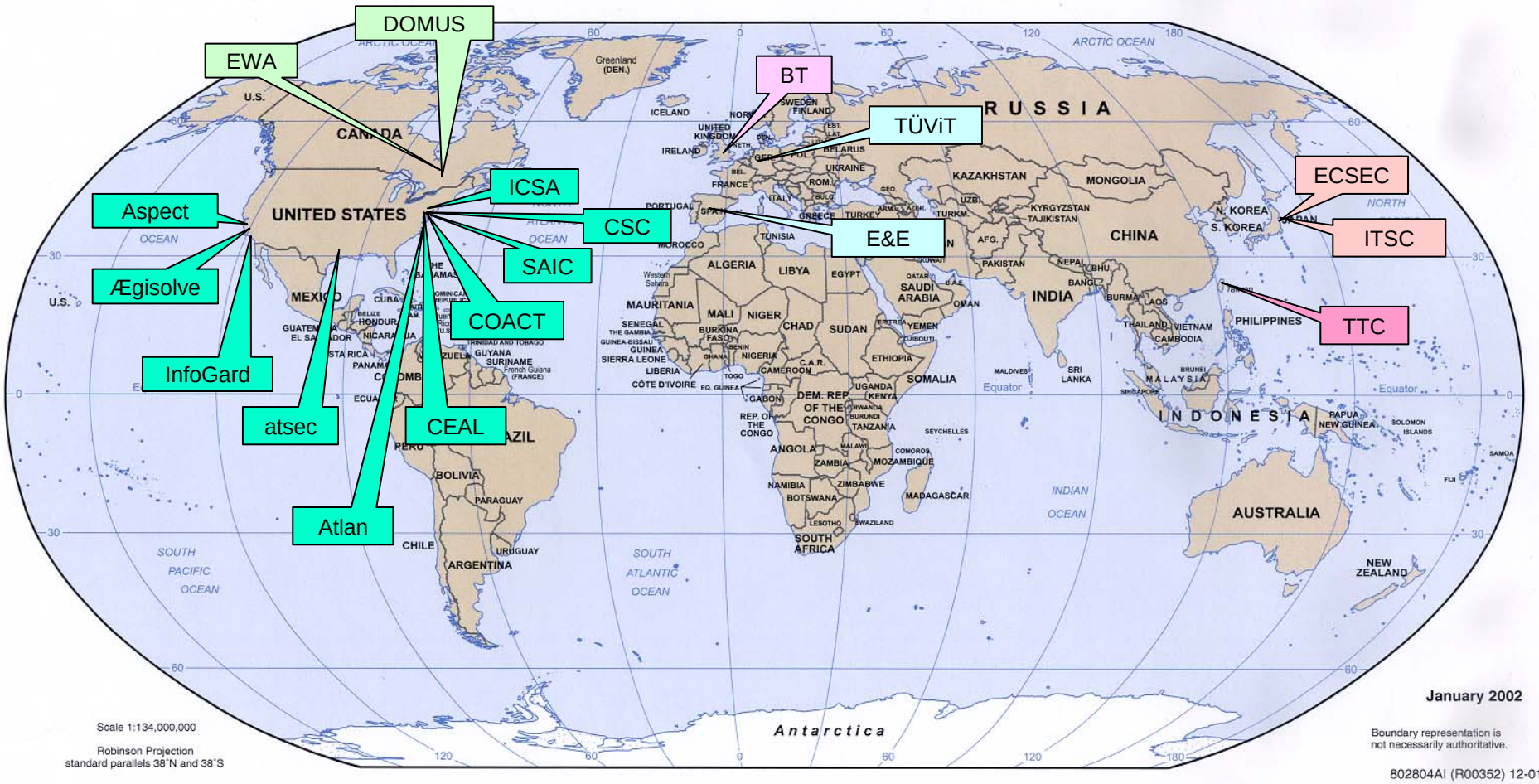
- Handbook 150-17:
  Cryptographic and Security Testing
  - Conformance Test Methods
    - FIPS 140-1 and FIPS 140-2 Levels 1, 2 and 3 testing
    - FIPS 140-1 and FIPS 140-2 Level 4 testing
    - FIPS 201 PIV card application testing
    - FIPS 201 PIV middleware testing
    - FIPS 201 Evaluation Program
    - SCAP



Cryptographic and Security Testing (CST) Laboratories

- Eighteen NVLAP-accredited testing laboratories
  - True independent 3rd party accredited testing laboratories
  - Cannot test and provide design assistance
  - US, Canada, UK, Germany, Spain, Japan and Taiwan
    - Additional domestic and international labs in FY10

CST Accredited Laboratories



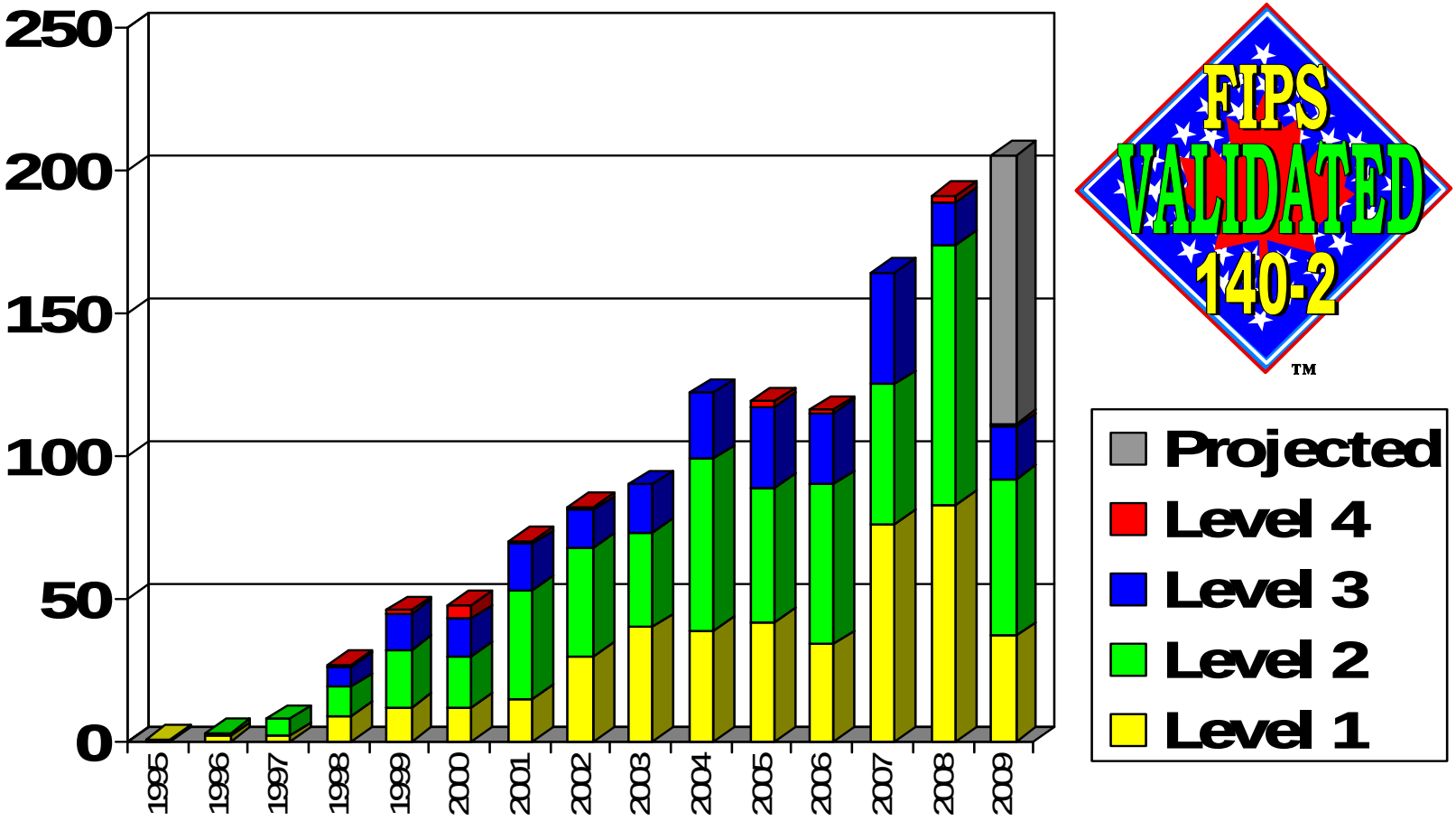
Seventh added in 2002
Eighth added in 2003
Ninth added in 2004
Tenth, Eleventh and Twelfth added in 2005
Thirteenth added in 2006
Fourteenth and Fifteenth added and lost one in 2007
Added in Japan and Taiwan in 2008
Added Spain, Japan and US in 2009

CMVP Status

- Continued record growth in the number of cryptographic modules validated
  - 1114 Validations representing over 2250 modules
- All four security levels of FIPS 140-2 represented on the Validated Modules List
- Over 285 participating vendors

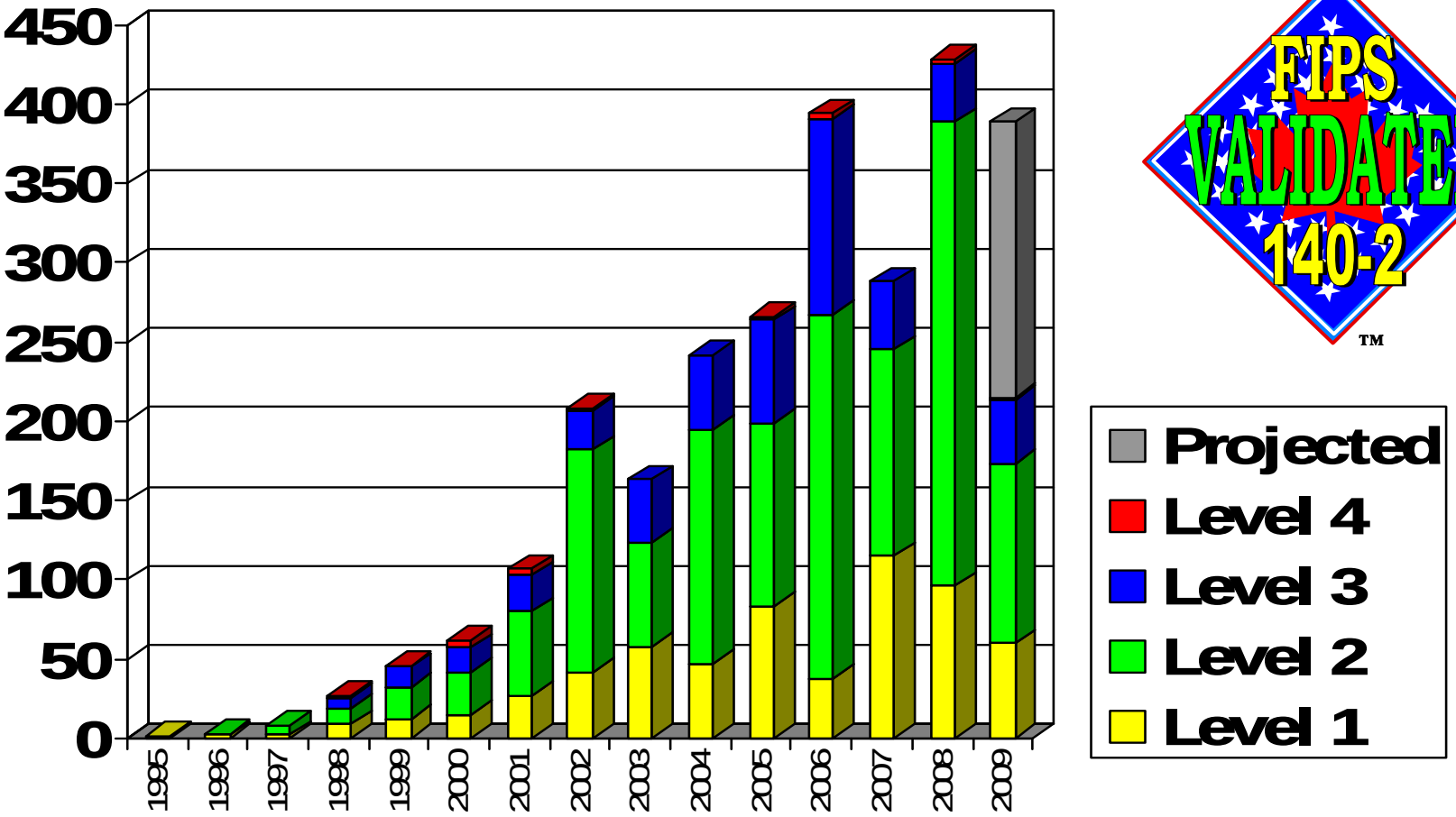
FIPS 140-2 Validation Certificates by Year and Level

(September 30, 2009)



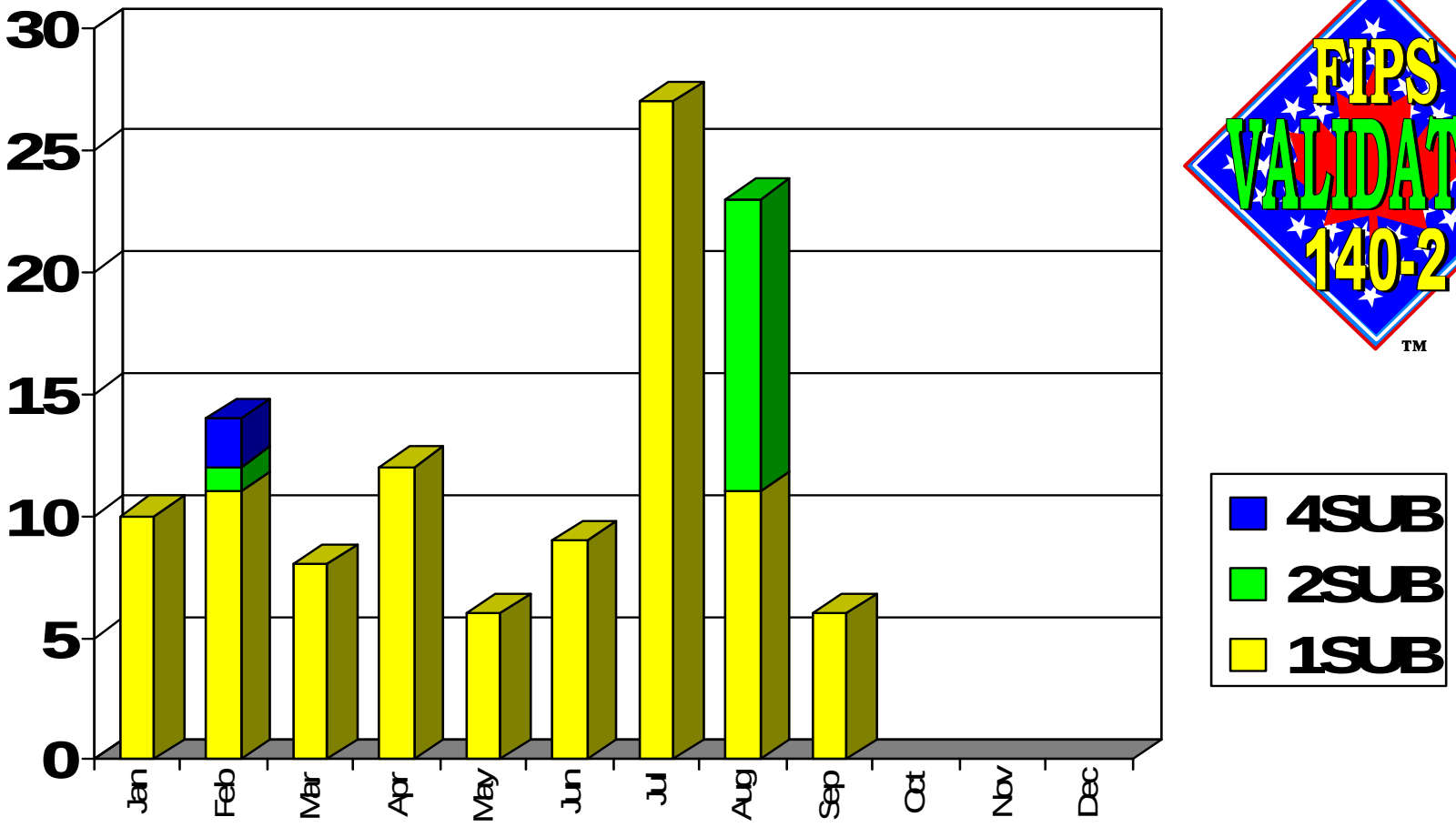
FIPS 140-2 Validated Modules by Year and Level

(September 30, 2009)



FIPS 140-2 Validation 1SUB/2SUB/4SUB Change Requests by Month

(September 30, 2009)



Modules In Process Listing

- Posted each Friday afternoon - http://csrc.nist.gov/groups/STM/cmvp/inprocess.html
- Describes five stages that a module report is progressing:
  - **Implementation Under Test**
  - **Review Pending**
  - **In Review**
  - **Coordination**
  - **Finalization**

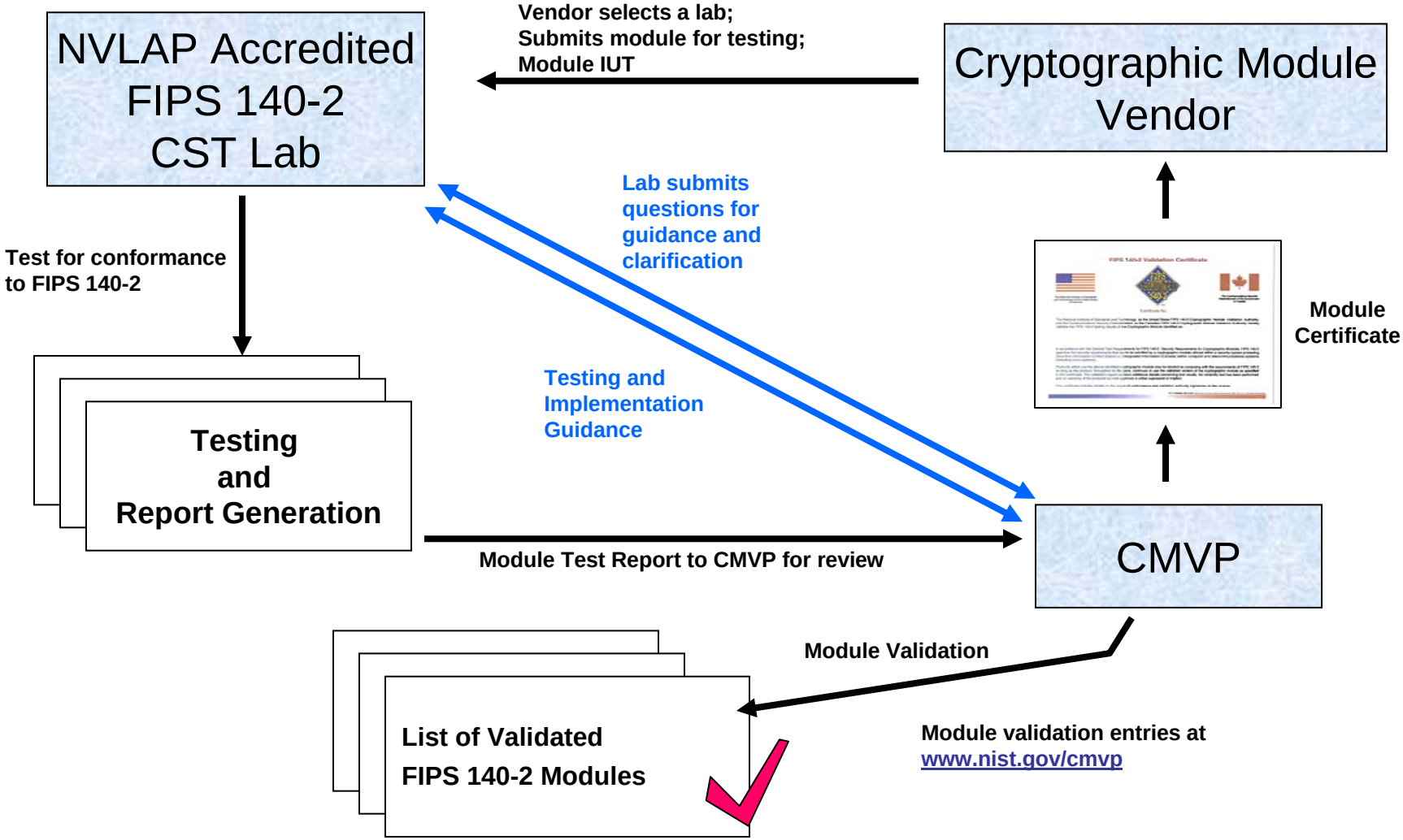
DISCLAIMER: The Cryptographic Module Validation Program (CMVP) FIPS 140-1 and FIPS 140-2 Modules In Process List is provided for information purposes only. Participation on the list is voluntary and is a joint decision by the vendor and Cryptographic and Security Testing (CST) laboratory. Modules are listed alphabetically by name. Blank entries indicate modules in process but joint decision made not to post. Posting on the list does not imply guarantee of final FIPS 140-1 or FIPS 140-2 validation.

Benefits! … Making a Difference

- **Cryptographic Modules Surveyed (during testing)**
  - **Contained at least one non-conformance**
    - 59% Level 1 and Level 2 Modules
    - 65% Level 3 and Level 4 Modules
  - 96.3% FIPS Interpretation and Documentation Errors
- **Areas of Greatest Difficulty**
  - Physical Security
  - Self Tests
  - Random Number Generation
  - Key Management

CMVP Testing and Validation Flow

Vendor	CMT Lab	CMVP NIST and CSE	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**


NVLAP Accredited FIPS 140-2 CST Lab
Vendor selects a lab;
Submits module for testing;
Module IUT
Cryptographic Module Vendor
Lab submits questions for guidance and clarification
Test for conformance to FIPS 140-2
Module Certificate
Testing and Implementation Guidance
Testing and Report Generation
Module Test Report to CMVP for review
CMVP
Module Validation
List of Validated FIPS 140-2 Modules
Module validation entries at www.nist.gov/cmvp

CMVP Testing: Process

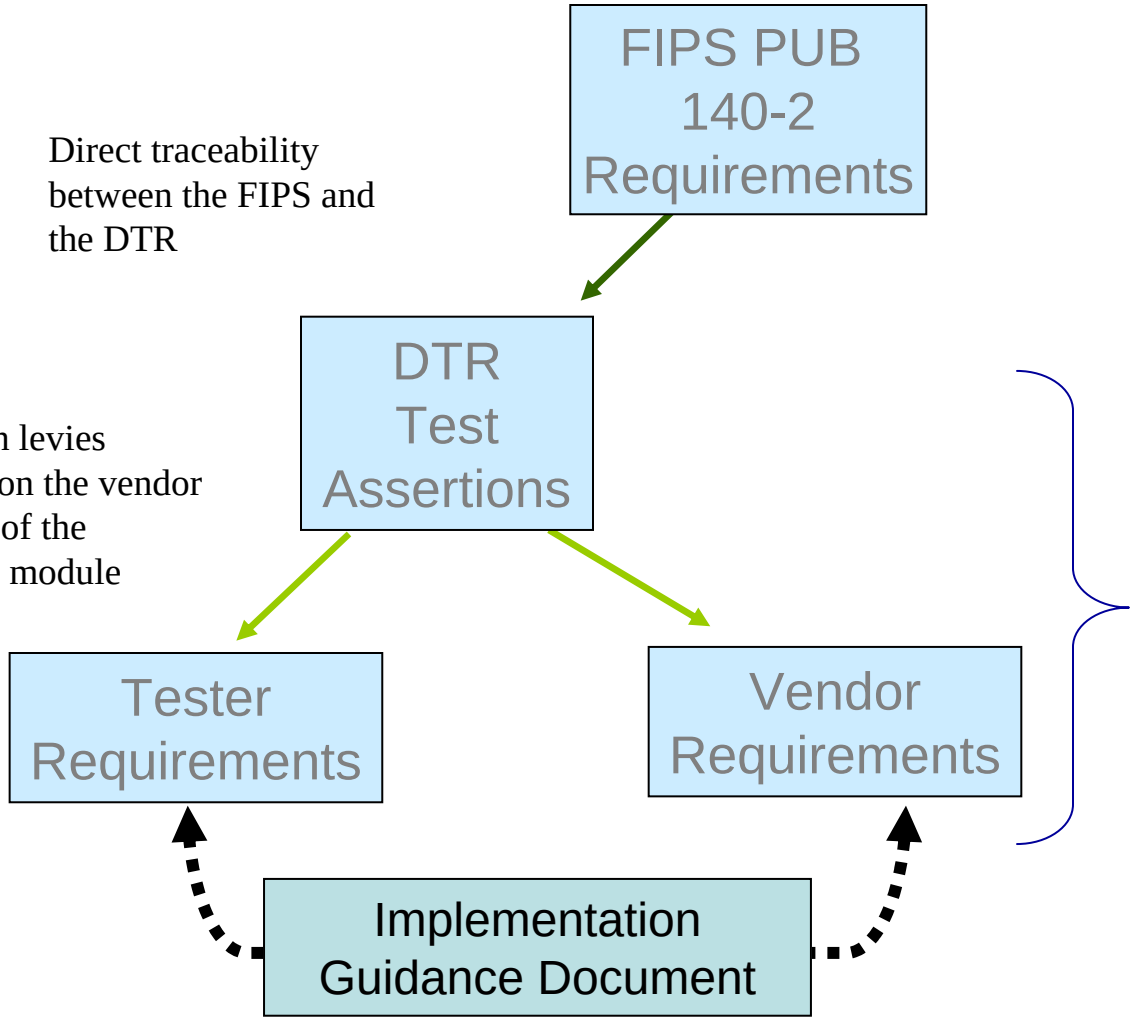
- CMVP
  - Conformance testing of cryptographic modules using the Derived Test Requirements (DTR)
  - Not evaluation of cryptographic modules. Not required are:
    - Vulnerability assessment
    - Design analysis, etc.
- Laboratories
  - Test submitted cryptographic modules
- NIST/CSEC
  - Validate tested cryptographic modules

FIPS140-2 Testing: Primary Activities

- **Documentation Review**
  - (e.g., Security Policy, Finite State Model, Key Management Document)
- **Source code Analysis**
  - Annotated Source Code
  - Link with Finite State Model
- **Testing**
  - Physical Testing
  - FCC EMI/EMC conformance
  - Operational Testing
  - CAVP Algorithm and RNG Testing

Direct traceability between the FIPS and the DTR

Each assertion levies requirements on the vendor and the tester of the cryptographic module

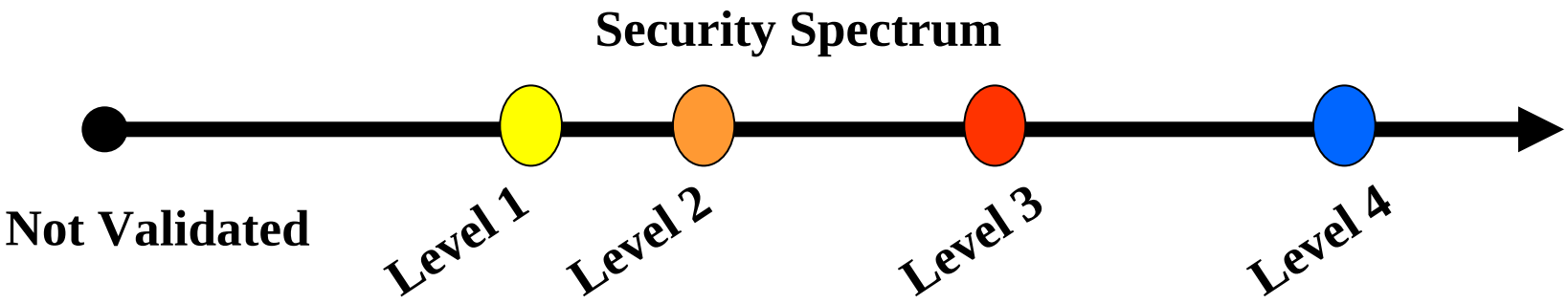


Derived Test Requirements

FIPS 140-2: Security Areas

1. Cryptographic Module Specification
2. Cryptographic Module Ports and Interfaces
3. Roles, Services, and Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. EMI/EMC requirements
9. Self Tests
10. Design Assurance
11. Mitigation of Other Attacks

FIPS 140-2: Security Levels



- Level 1 is the lowest, Level 4 most stringent
- Requirements are primarily cumulative by level
- Overall rating is lowest rating in all sections
- Validation is applicable when a module is configured and operated in accordance with the level to which it was tested and validated

Physical Security

- **Level 1**: Production Grade Components
- **Level 2**: Provide Evidence of an Attack
  - Tamper evident seals
  - Opacity
- **Level 3**: Deterrence of Moderately Aggressive Attacks
  - Strong enclosure or covered with hard coating or potting material
  - Tamper response and zeroization for any doors or removable covers
- **Level 4**: Deterrence of Aggressive Attacks
  - Attacker assumed to have prior knowledge, specialized tools, unfettered access and no time restriction.
  - Tamper Response and Zeroization Envelope
  - Mitigation of Temperature and Voltage Attacks

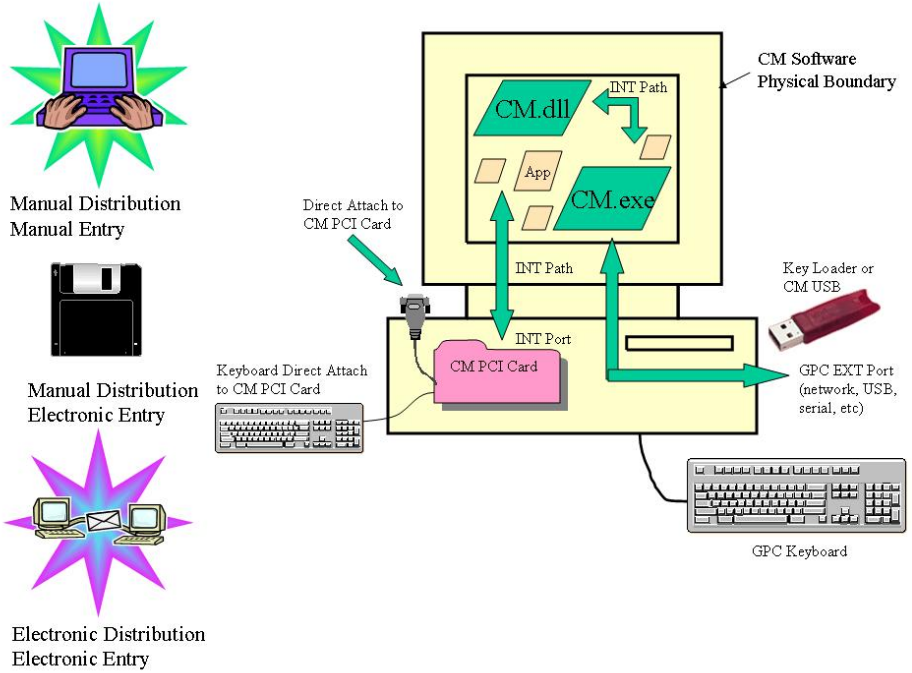
Cryptographic Module Specification

- Define the Cryptographic Module Boundary
  - Integrated Circuit
  - Integrated Circuit Plus Plastic Housing
- Define Approved Mode of Operation
- Provide Description of the Module
  - Hardware
  - Software
  - Firmware

Software Module

Cryptographic Module Boundary

- Physical boundary - GPC
- Logical boundary – Executable (e.g. DLL EXE)
- Operating system within the physical boundary but not part of the logical boundary



Security Policy

- Mandatory document developed by the vendor
- Security policy shall contain:
  - Description of the module: picture if hardware
  - Tested operating system if software
  - Description of how to place the module in FIPS Approved Mode
  - Roles, services, authentication method and strength of authentication
  - List of CSPs, and services and roles accessing them
  - Physical security policy
  - Mitigation of other attacks

Using FIPS Validated Cryptographic Modules

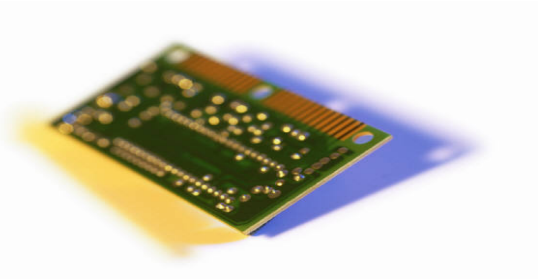
- Cryptographic modules *may* be embedded in other products
  - Applicable to hardware, software, and firmware cryptographic modules
  - Must use the validated version and configuration
  - e.g. software applications, cryptographic toolkits, postage metering devices, radio encryption modules
- Does <u>not</u> require the validation of the larger product
  - Larger product is <u>deemed compliant to requirements</u> of FIPS 140-2

Cryptographic Module vs. Product

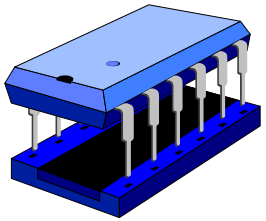
"Area" defined by the cryptographic boundary

- Could be a complete product

- Could be a sub-system of a larger product

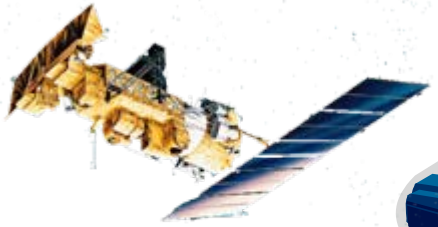


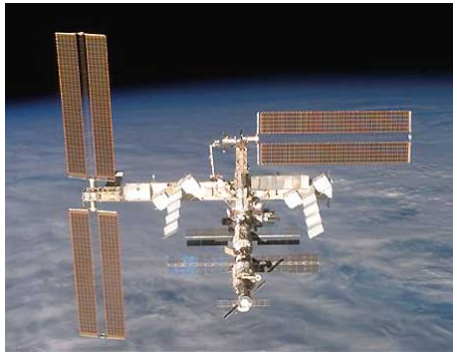
- Could be component of a product

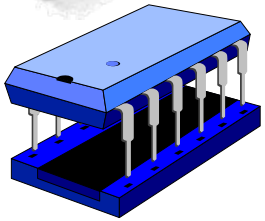


Examples








Available Colors*

FIPS 140-2 IG G.8 - Revalidation

- **No Security Relevant Changes**
  - **CMTL tests changes**
  - **Letter sent to CMVP**
  - **Existing certificate entry updated**
- **Additional Security Relevant Features Claimed**
  - **Testing of previously un-tested features**
  - **CMTL submits revalidation test report**
  - **Existing certificate entry updated**
- **<30% Security Relevant Changes**
  - **Testing of new features and operational regression testing**
  - **CMTL submits revalidation test report**
  - **New certificate issued**
- **Physical boundary only Change**
  - **Testing of physical features**
  - **CMTL submits physical test report**
  - **Existing certificate entry updated**
- **New Module**
  - **Full testing by CMTL**
  - **CMTL submits full test report**
  - **New Certificate**

- Certificate number
- Vendor Name
  - Address
  - Contact
- Module Name
  - Version
  - Security Policy
  - Certificate
- Module Type
- Validation Date
- Overall Level
  - Section Levels
  - Algorithms
  - Embodiment
  - Vendor supplied text

CMVP Main Page

Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules

1995-1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008,

All

Last Update: 3/19/2008

****** NOTE: Module descriptions were provided by the vendors, and their contents have not been verified for accuracy by NIST or CSE. The descriptions do not imply endorsement by the U.S. or Canadian Governments or NIST. Additionally, the descriptions may not necessarily reflect the capabilities of the modules when operated in the FIPS-approved mode. The algorithms, protocols, and cryptographic functions listed as "other algorithms" (non-FIPS-approved algorithms) have not been validated or tested through the CMVP. ******

Questions regarding modules on this list should first be directed to the appropriate vendor.

Cert#	Vendor	Cryptographic Module	Module Type	Val. Date	Level / Description
929	Kingston Technology Company 17600 Newhope Street Fountain Valley, CA 92708 USA -Mark Akoubian TEL: 714-438-2719 FAX: 714-427-3598	Kingston S2 CM (Hardware Version: P/N 8A-SFS-0000-09P, Version A; Firmware Version: 6.600) *(When operated in FIPS mode)* **Validated to FIPS 140-2** Security Policy Certificate	Hardware	03/18/2008	***Overall Level:*** **2** -EMI/EMC: Level 3 *-FIPS-approved algorithms:* AES (Cert. #464); RSA (Cert. #200); RNG (Cert. #263); SHS (Cert. #555) *-Other algorithms:* RSA (encrypt/decrypt) Multi-chip embedded "The Kingston S2 CM is the core component of this performance secure USB Flash Drive. All data stored in the userÆs private partition is encrypted in hardware without reducing performance. The Kingston S2 CM provides encryption, user authentication and access control independent of the host software and hardware."

Federal Acquisitions

What Specific Procedures Must an Agency Take to Confirm Validation?

Agencies must take the following steps to ensure they are:

1. acquiring and using only validated products or modules embedded within products;
2. obtaining from vendors evidence of product or module validation; and
3. confirming the vendor supplied evidence is accurate

Further information can be found at the NIST CMVP web site.

Technology Trends

- Systems on a Chip
  - multi-core processors
  - embedded crypto macros
- SmartCards
  - Adding applets to validated modules
- Hybrid modules
  - hardware/software
  - hardware/firmware
- Non-invasive attacks
  - SPA/DPA/EMA
- Readily available sophisticated tools/methods

www.nist.gov/cmvp

- FIPS 140-1, FIPS 140-2 and FIPS 140-3 *draft*
- Derived Test Requirements (DTR)
- Annexes to FIPS 140-2
- Implementation Guidance
- Points of Contact
- Laboratory Information
- Validated Modules List

Points of Contact

NIST

- **Randall J. Easter** – Director, CMVP, NIST
  reaster@nist.gov

- **Sharon Keller** – Director, CAVP, NIST
  skeller@nist.gov

CSEC

- **Jean Campbell** – Technical Authority, CMVP, CSEC
  jean.campbell@CSE-CST.GC.CA