CMVP
Conformance through Testing

FIPS VALIDATED 140-2

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Cryptographic Module Validation Program

Where security starts ….

Randall J. Easter

Director, NIST CMVP

September 14, 2004

Agenda

- FIPS 140-2: Security Requirements for Cryptographic Modules
- Testing Cryptographic Modules
- Maintaining Validation Status
- Additional Information and Links

Cryptographic Module Validation Program (CMVP)

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

Applicability of FIPS 140-2

- U.S. Federal organizations must use validated cryptographic modules
- GoC departments are recommended by CSE to use validated cryptographic modules
- International recognition

The Importance of Testing: Buyer Beware!

- Does the product do what is claimed?
- Does it conform to standards?
- Was it independently tested?
- Is the product secure?

Making a Difference…

(Certificates 165 through 275)

- Cryptographic Modules
  - Experienced
    - 20% security-relevant flaws
    - 100% documentation flaws (primarily the security policy)
  - New to the Process...
    - 50% security-relevant flaws
    - 100% documentation flaws (primarily the security policy)
- Cryptographic Algorithms
  - 30% non-conformant

Using FIPS Validated Cryptographic Modules

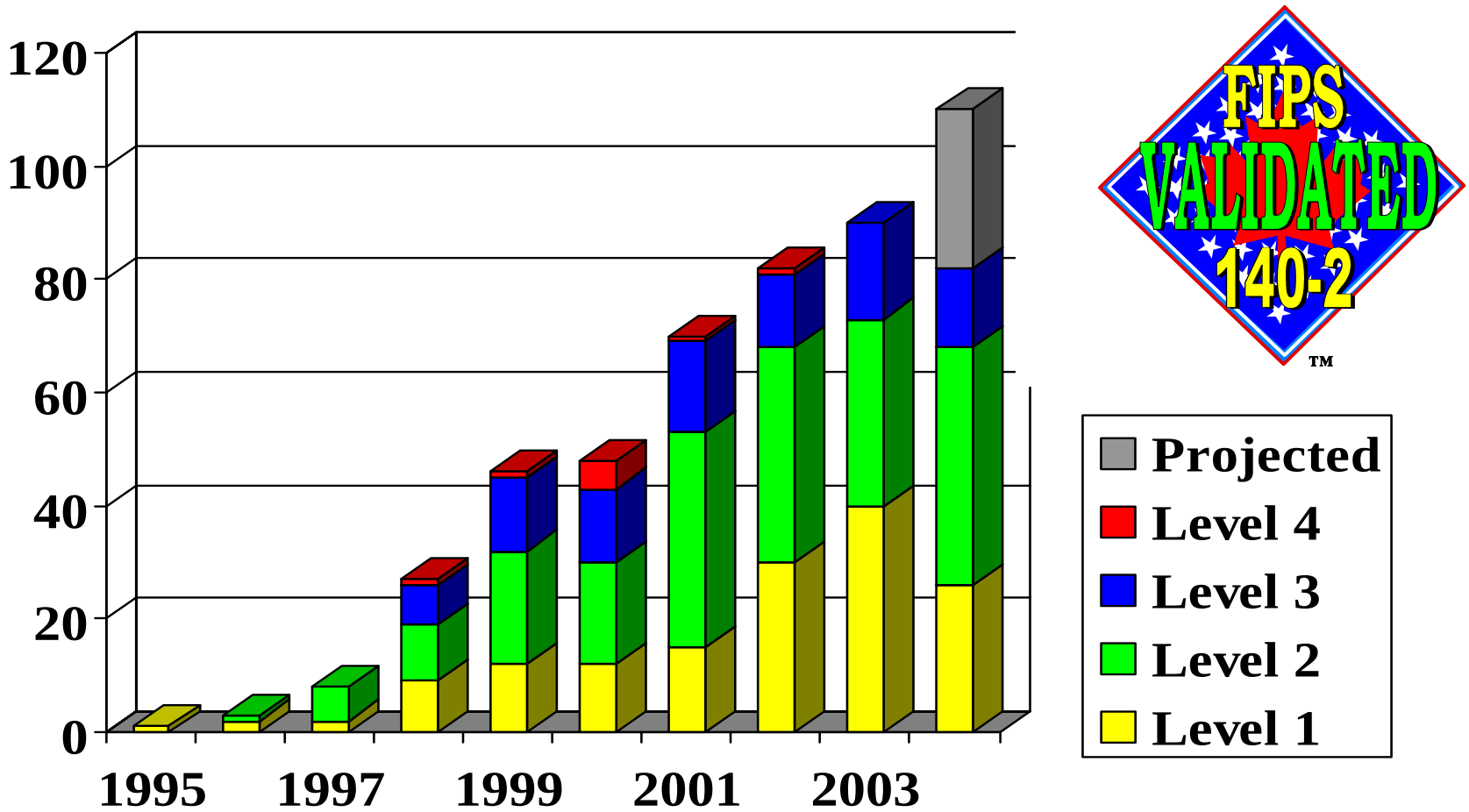
- Cryptographic modules *may* be embedded in other products
  - Applicable to hardware, software, and firmware cryptographic modules
  - Must use the validated version and configuration
  - e.g. software applications, cryptographic toolkits, postage metering devices, radio encryption modules
- Does not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

CMVP Status

- Continued record growth in the number of cryptographic modules validated
  - Over 450 Validations representing over 850 modules (457 08/12/2004)
- All four security levels of FIPS 140-2 represented on the Validated Modules List
- Over 110 participating vendors
- FIPS 140-2 moves to ISO
- FIPS 140-3 work begins

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

(July 31, 2004)



Participating Vendors

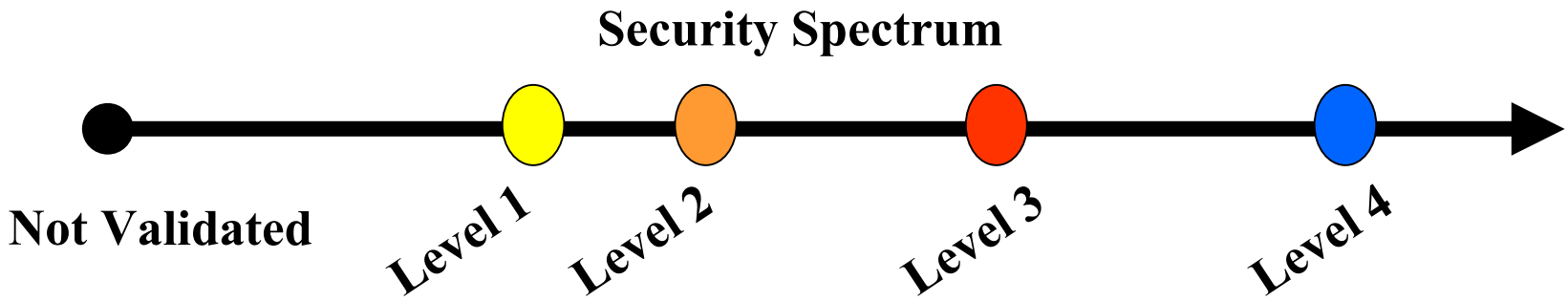
(April 30, 2004 – 114 Total)

3e Technologies International, Inc.
3S Group Incorporated
ActivCard
ActivCard Inc., Atmel, Inc. and MartSoft, Inc.
Admiral Secure Products, Ltd.
AEP Systems
Airespace, Inc.
Aladdin Knowledge Systems, Ltd.
Alcatel
Algorithmic Research, Ltd.
Atalla Security Products of Hewlett Packard Corporation
Altarus Corporation
Attachmate Corp.
Avaya, Inc.
Blue Ridge Networks
Bodacion Technolgies
Certicom Corp.
Check Point Software Technologies Ltd.
Chrysalis-ITS Inc.
Cisco Systems, Inc.
Colubris Networks, Inc.
Communications Devices, Inc.
Control Break International Corp.
Corsec Security, Inc.
Cranite Systems, Inc.
Cryptek Inc.
CTAM, Inc.
CyberGuard Corporation
Cylink Corporation
Dallas Semiconductor, Inc.
Datakey, Inc.
ECI Systems & Engineering
E.F. Johnson Co.
Encotone Ltd.
Ensuredmail, Inc.
Entrust Inc.
Eracom Technologies Group, Eracom Technologies Australia, Pty. Ltd.
Entrust CygnaCom
F-Secure Corporation
Fortress Technologies, Inc.
Francotyp-Postalia
Gemplus Corp. and ActiveCard Inc.
General Dynamics Decision Systems
Giesecke & Devrient
Good Technology
GTE Internetworking
Hasler, Inc.
Information Security Corporation
IBM® Corporation
Intel Network Systems, Inc.
IP Dynamics, Inc.
IRE, Inc.
ITT
Kasten Chase Applied Research
L-3 Communication Systems
Lipman Electronic Engineering Ltd.
Litronic, Inc.
Lucent Technologies
M/A-Com, Inc.
Microsoft Corporation
Mitsubishi Electric Corporation
Motorola, Inc.
Mykotronx. Inc
National Semiconductor Corp.
nCipher Corporation Ltd.
Neopost
Neopost Industrie
Neopost Ltd.
Neopost Online
Network Security Technology (NST) Co.
Netscape Communications Corp.
NetScreen Technologies, Inc.
Nortel Networks
Novell, Inc.
Oberthur Card Systems
Oracle Corporation
Palm Solutions Group
PGP Corporation
Phaos Technology Corporation
Pitney Bowes, Inc.
Pointsec Mobile Technologies
PrivyLink Pte Ltd
PSI Systems, Inc.
Rainbow Technologies
Real Time Logic, Inc.
RedCreek Communications
ReefEdge, Inc.
Research In Motion
RSA Security, Inc.
SafeNet, Inc.
SchlumbergerSema
Securit-e-Doc, Inc.
Sigaba Corporation
Simple Access Inc.
SingleSignOn.Net, Inc.
SonicWall, Inc.
SPYRUS, Inc.
Stamps.com
Standard Networks, Inc.
StoneSoft Corporation
SSH Communications Security Corp.
Sun Microsystems, Inc.
Symbol (Columbitech)
Technical Communications Corp.
Thales e-Security
TimeStep Corporation
Transcrypt International
Tumbleweed Communications Corp.
Ultra Information Systems, Inc.
ValiCert, Inc.
V-ONE Corporation, Inc.
Wei Dai
WinMagic Incorporated

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

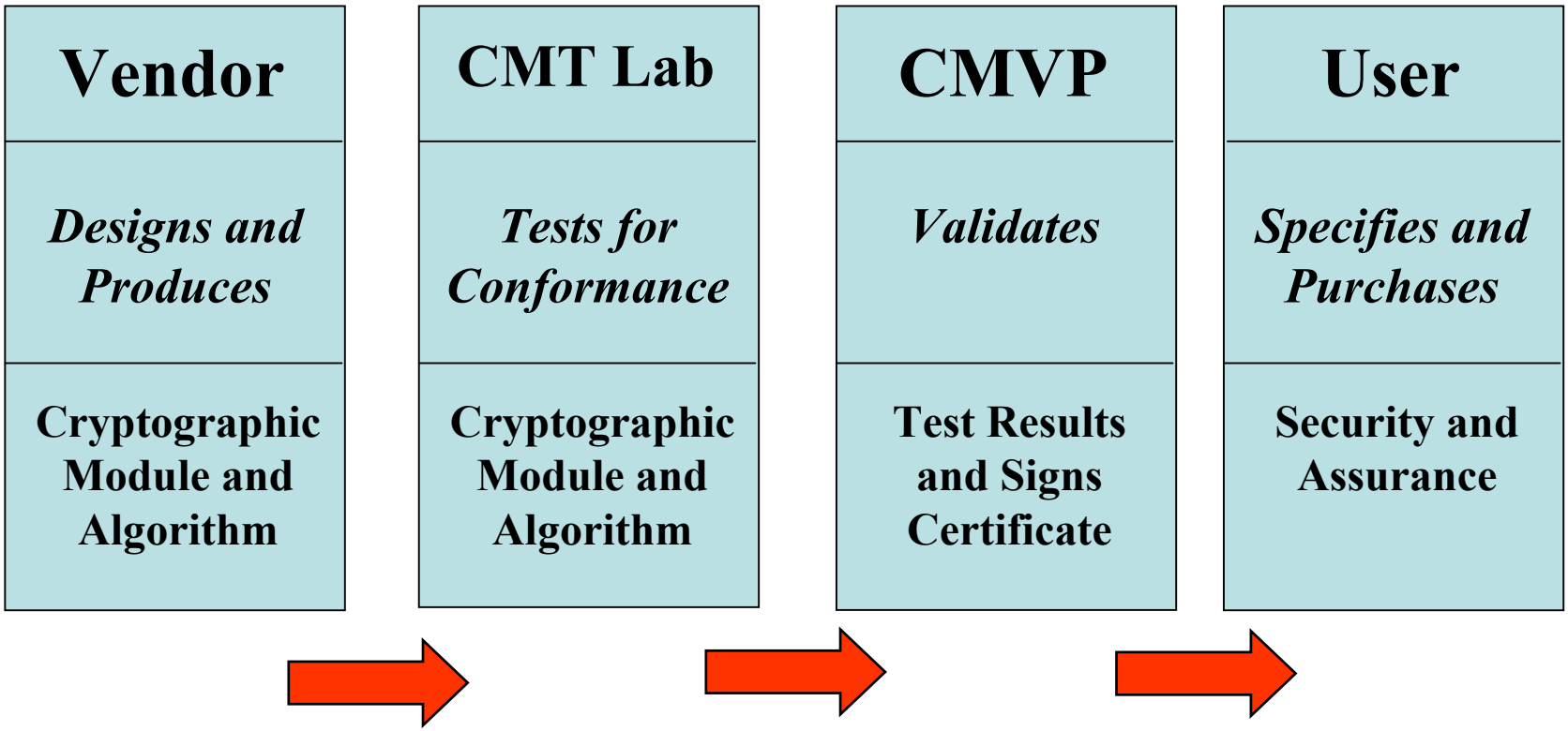


- Level 1 is the lowest, Level 4 most stringent
- Requirements are primarily cumulative by level
- Overall rating is lowest rating in all sections
- Validation is applicable when a module is configured and operated in accordance with the level to which it was tested and validated

Physical Security

- Single-Chip Cryptographic Module
- Testing
  - Level 1: Production Grade
  - Level 2: Evidence of Tampering
  - Level 3: Hard Opaque Tamper-Evident Coating
  - Level 4: Hard Opaque Removal Resistant Coating

CMVP Testing: Validation Flow



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

CMVP Testing: Process

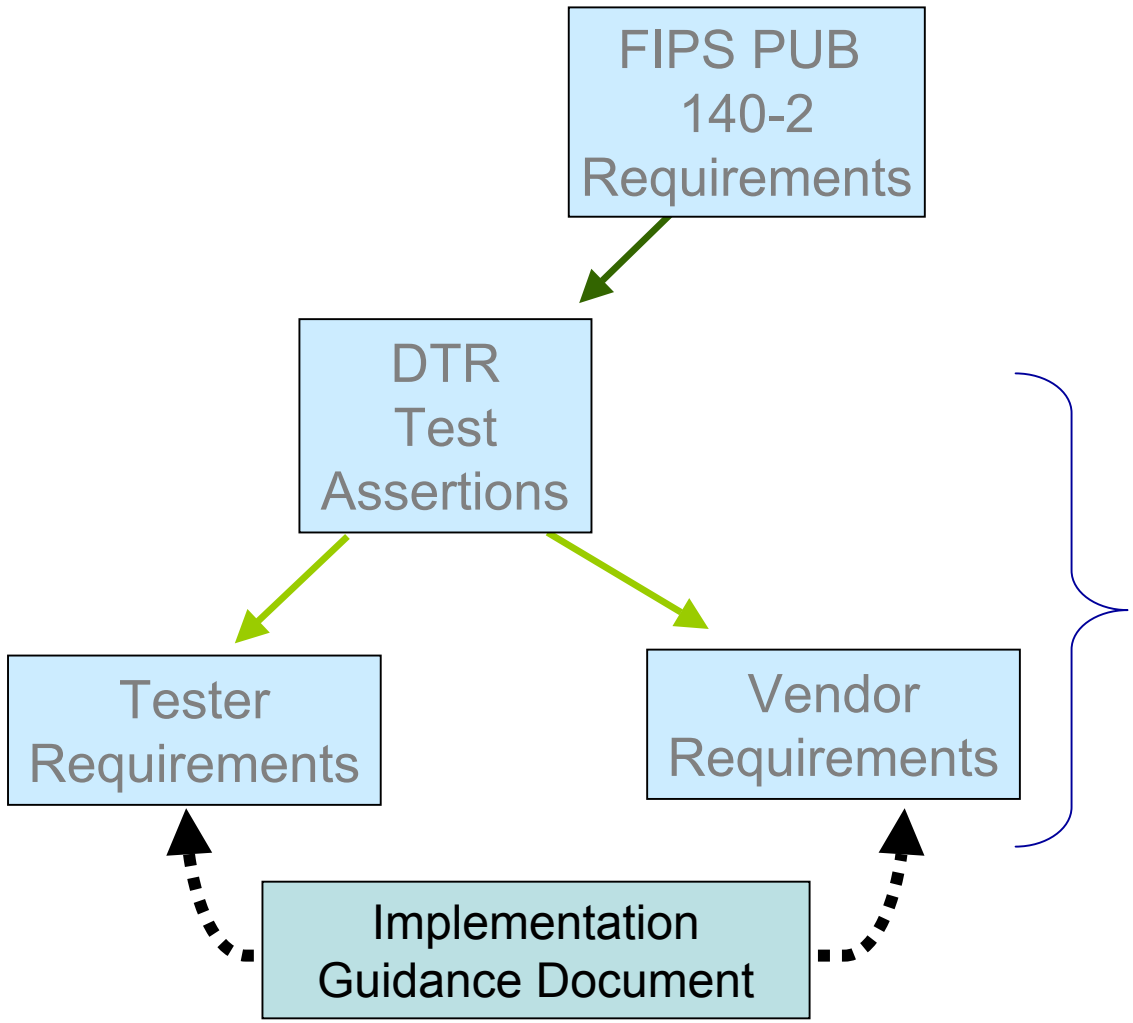
- CMVP
  - Conformance testing of cryptographic modules using the Derived Test Requirements (DTR)
  - Not evaluation of cryptographic modules. Not required are:
    - Vulnerability assessment
    - Design analysis, etc.
- Laboratories
  - Test submitted cryptographic modules
- NIST/CSE
  - Validate tested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

Derived Test Requirements

- Cryptographic module testing is performed using the Derived Test Requirements (DTR)
- Assertions in the DTR are directly traceable to requirements in FIPS 140-2
- All FIPS 140-2 requirements are included in the DTR as assertions
  - Provides for one-to-one correspondence between the FIPS and the DTR
- Each assertion includes requirements levied on the
  - Cryptographic module vendor
  - Tester of the cryptographic module

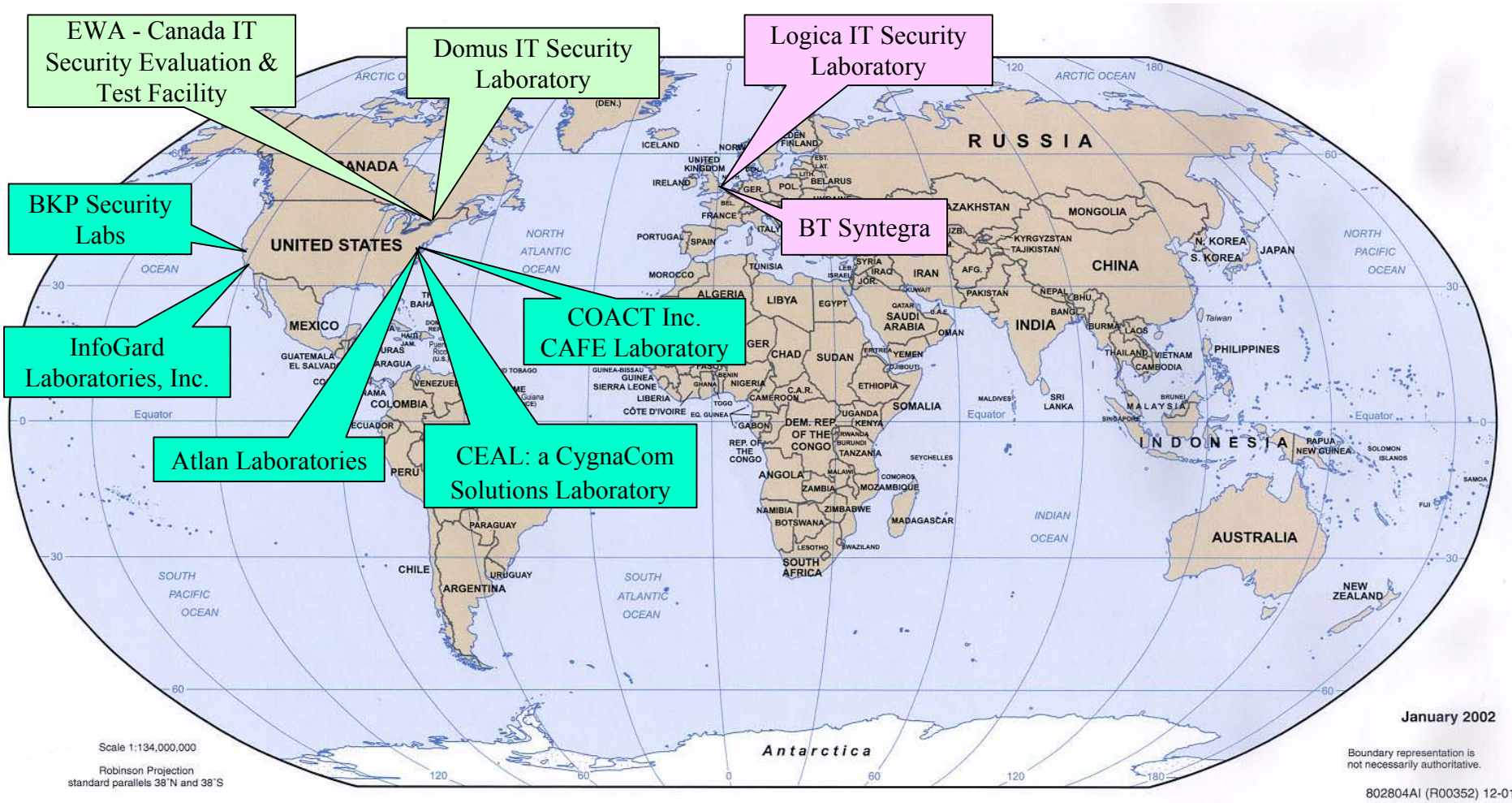


Derived Test Requirements

Cryptographic Module Testing (CMT) Laboratories

- Nine National Voluntary Laboratory Accreditation Program (NVLAP) - accredited testing laboratories
  - True independent 3rd party accredited testing laboratories
  - Cannot test and provide design assistance

CMT Accredited Laboratories



Seventh CMT laboratory added in 2002
Eighth CMT Laboratory added in 2003
Ninth CMT Laboratory added in 2004

Revalidation: No Security Relevant Changes

- FIPS 140-2: An *updated* version of a previously validated cryptographic module
  - Change to module does not affect FIPS 140-2 security relevant items
  - Cryptographic Module Testing (CMT) laboratory verifies vendor claims and submits letter to validation authorities (NIST and CSE)
  - CMVP updates website and no certificate is issued

Revalidation: Security Relevant Changes (<30%)

- Modifications to hardware, software, firmware affect *less than 30%* of the *operational* security relevant requirements
- The laboratory tests:
  - The changed assertions (requirements)
  - All assertions listed in the regression test suite
  - New and updated assertions
- Revised documentation (e.g., security policy) also submitted

Revalidation: Security Relevant Changes (>30%)

- Modifications to hardware, software, firmware affect *greater than 30%* of the security relevant assertions
  - The CMT laboratory performs full validation testing
- Full validation required for…
  - Overall security level change
  - Physical embodiment change

http://www.nist.gov/cmvp

- FIPS 140-1 and FIPS 140-2
- Derived Test Requirements (DTR)
- Annexes to FIPS 140-2
- Implementation Guidance
- Points of Contact
- Laboratory Information
- Validated Modules List
- Special Publication 800-23

Cryptographic Module Validation Program

Standards and Their Related Documents:

- FIPS 140-2 (current)
- FIPS 140-1 (former)

- Symmetric Key
- Asymmetric Key
- Hashing
- RNG
- MAC and X9.17

Validation Lists

Testing Laboratories

Announcements
Updated 05/13/2004

Notices
Updated 12/16/2003

FAQs
Updated 12/18/2003

Helpful Documentation

Contacts

Computer Security Resource Clearinghouse

NIST

Cryptographic Module Validation Program

CMVP Conformance Through Testing

FIPS VALIDATED 140-2

NIST National Institute of Standards and Technology

FIPS 140-2 is now in effect. However,
Agencies may continue to purchase, retain and use FIPS 140-1 validated modules.

CMVP Conference 2004

September 14-15, 2004

DoubleTree Hotel & Executive Meeting Center, Rockville, MD 20852

Watch for more details (reservations, accommodations, agenda, etc.).

The Computer Security Division at NIST maintains a number of cryptographic standards, and coordinates validation programs for many of those standards. The **Cryptographic Module Validation Program (CMVP)** encompasses validation testing for cryptographic modules and algorithms:

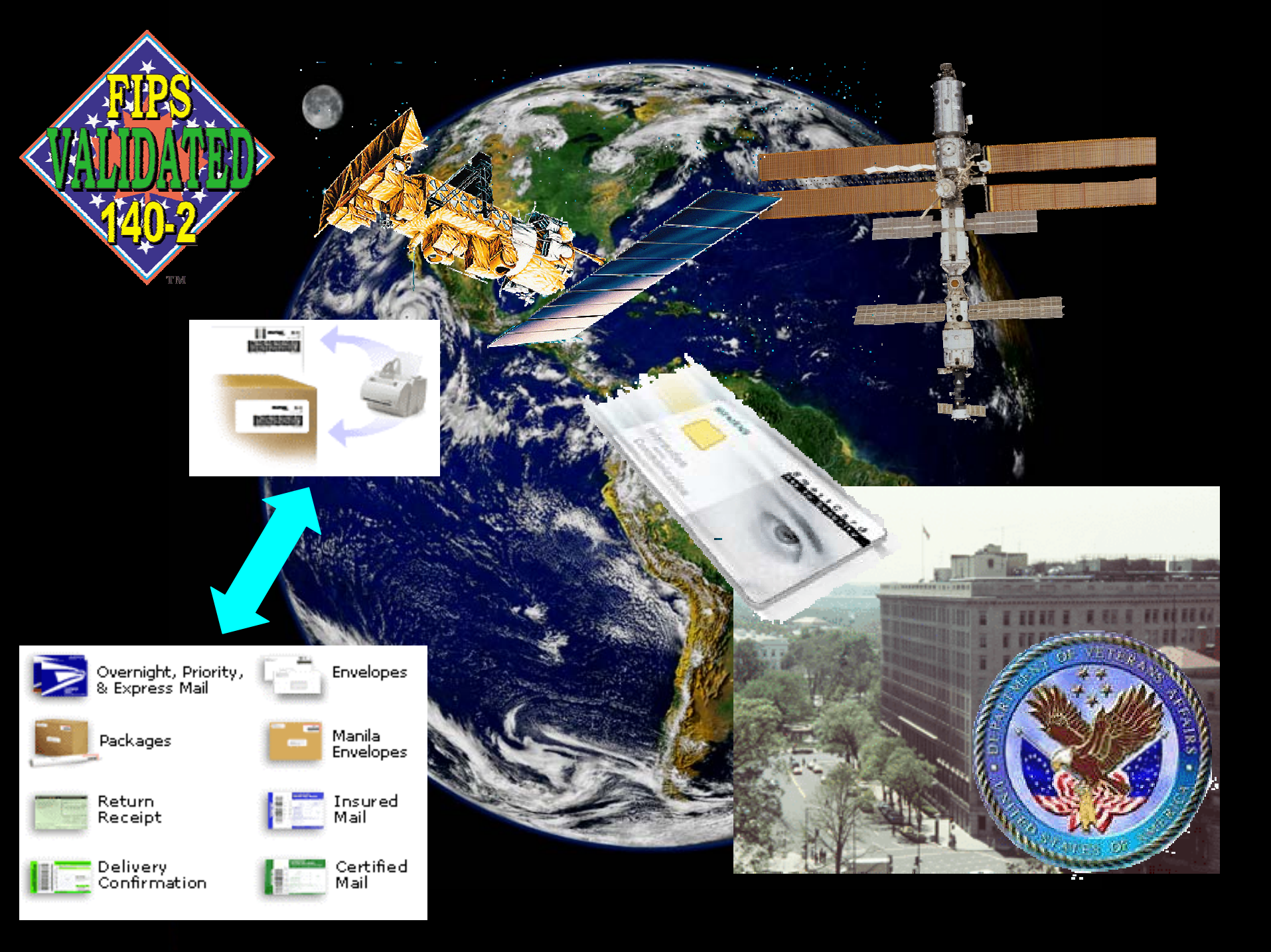
Cryptographic Modules

What is the applicability of CMVP to the US government?
How does Common Criteria (CC) relate to FIPS 140-2?

- FIPS 140-2: *Security Requirements for Cryptographic Modules*, May 25, 2001. Change Notices 2, 3 and 4: 12/03/2002
- FIPS 140-1: *Security Requirements for Cryptographic Modules*, January 4, 1994.

Cryptographic Algorithms

- FIPS 197: *Advanced Encryption Standard (AES)*. FIPS 197 specifies the **AES** algorithm.
- FIPS 46-3 and FIPS 81: *Data Encryption Standard (DES)* and *DES Modes of Operation*. FIPS 46-3 specifies the **DES** and **Triple DES** algorithms.


FIPS
VALIDATED
140-2
TM
Overnight, Priority, & Express Mail
Envelopes
Packages
Manila Envelopes
Return Receipt
Insured Mail
Delivery Confirmation
Certified Mail

NIST

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

CSE

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