The Cryptographic Module Validation Program and FIPS 140-2

Randall J. Easter

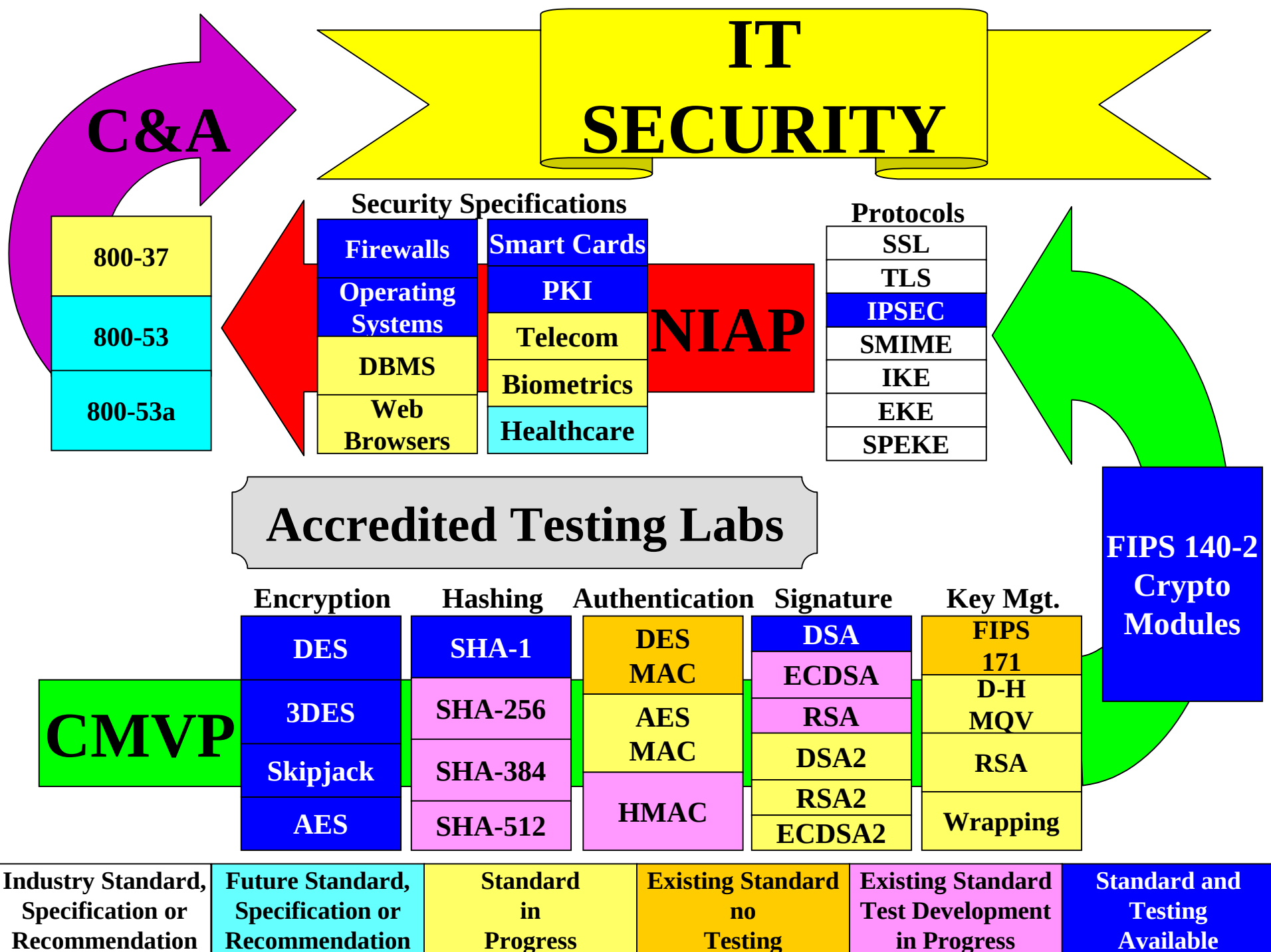
Senior Engineer, Cryptographic Module Validation Program

National Institute of Standards and Technology

December 4, 2002

Agenda

- The Cryptographic Module Validation Program
- The Importance of Testing – Making a Difference!
- FIPS 140-2 and Testing
- CMVP Status and General Information
- Additional Slides for Background and Information
  - Web Site Examples
  - Revalidation of Cryptographic Modules
  - JAVA and FIPS 140-2


IT SECURITY
C&A
800-37
800-53
800-53a
Security Specifications
Firewalls
Operating Systems
DBMS
Web Browsers
Smart Cards
PKI
Telecom
Biometrics
Healthcare
NIAP
Protocols
SSL
TLS
IPSEC
SMIME
IKE
EKE
SPEKE
Accredited Testing Labs
FIPS 140-2 Crypto Modules
CMVP
Encryption
DES
3DES
Skipjack
AES
Hashing
SHA-1
SHA-256
SHA-384
SHA-512
Authentication
DES MAC
AES MAC
HMAC
Signature
DSA
ECDSA
RSA
DSA2
RSA2
ECDSA2
Key Mgt.
FIPS 171
D-H MQV
RSA
Wrapping
Industry Standard, Specification or Recommendation
Future Standard, Specification or Recommendation
Standard in Progress
Existing Standard no Testing
Existing Standard Test Development in Progress
Standard and Testing Available

Cryptographic Module Validation Program (CMVP)

- 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
- Seven NVLAP-accredited testing laboratories
  - True independent 3rd party accredited testing laboratories
  - Can not test and provide design assistance

CMVP: Philosophy

- Strong commercially available cryptographic products are needed

- Government must work with the commercial sector and the cryptographic community for:
  - security,
  - interoperability, and
  - assurance

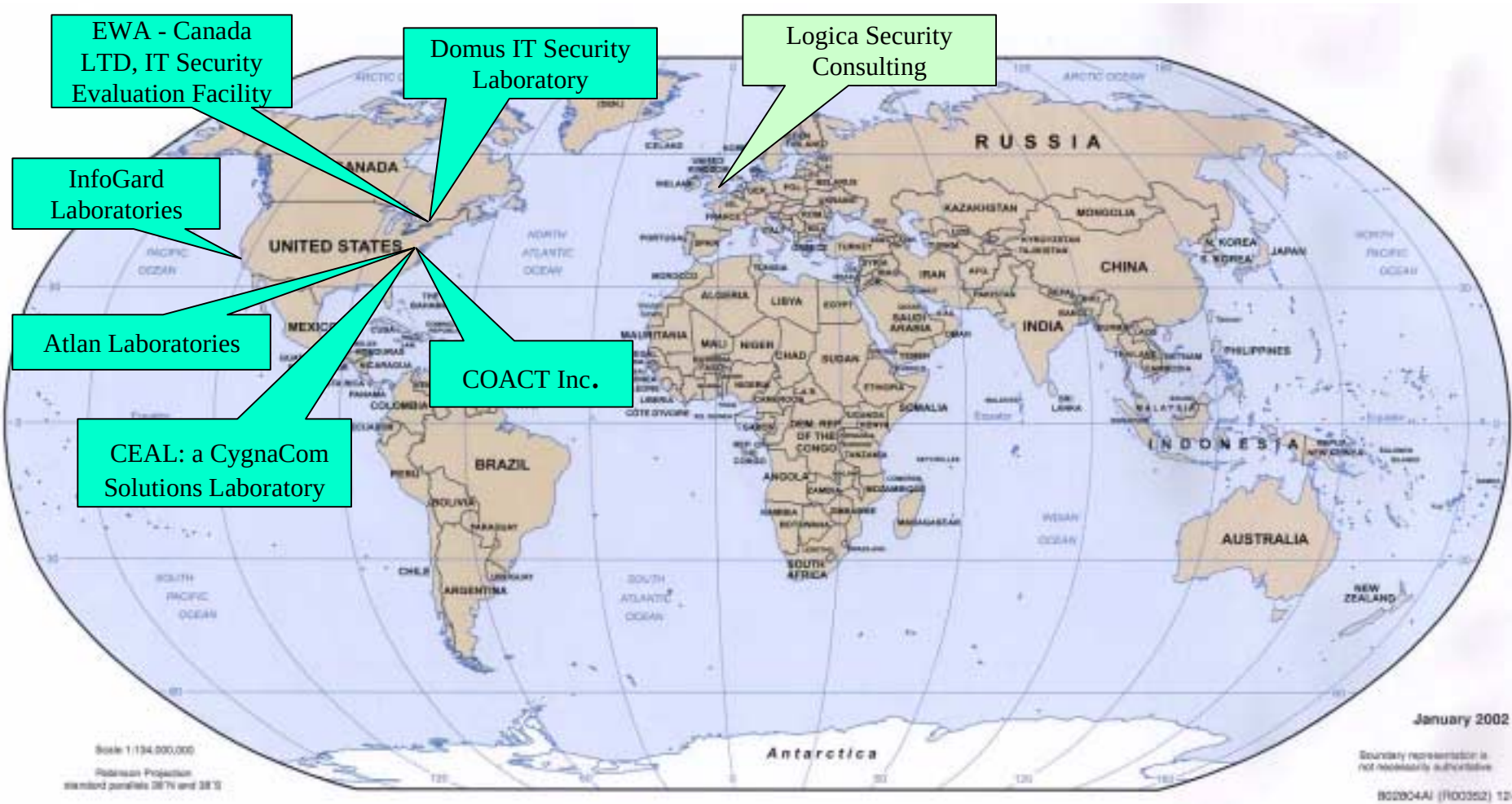
CMVP: Applicability of FIPS 140-2

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

Communications-Electronics Security Group (CESG) - UK

- December 28, 2001
  - CESG proposes the use of FIPS 140 as the basis for the evaluation of cryptographic products used in a number of UK government applications and encourages the setting up of accredited laboratories in the UK to perform these evaluations.

CMVP: Accredited Laboratories



Seventh CMT laboratory added in 2002

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?

CMVP

Conformance through Testing

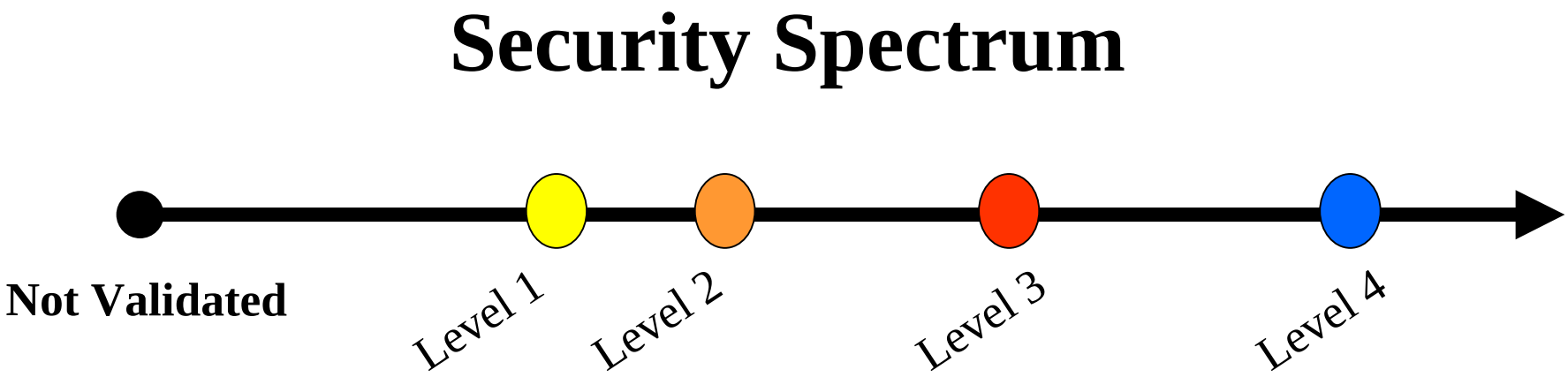
… Making a Difference

- **164 Cryptographic Modules Surveyed (during testing)**
  - 80 (48.8%) Security Flaws discovered
  - 158 (96.3%) Documentation Errors
- **332 Algorithm Validations (during testing) (DES, Triple-DES, DSA and SHA-1)**
  - 88 (26.5%) Security Flaws
  - 216 (65.1%) Documentation Errors
- **Web Access**
  - November 2001 – 125,000 hits
  - Monthly average – 80,000 hits


FIPS
VALIDATED
140-1
™


FIPS
VALIDATED
140-2
™

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**

FIPS 140-2: Security Areas

- Cryptographic Module Specification
- Cryptographic Module Ports and Interfaces
- Roles, Services, and Authentication
- Finite State Model
- Physical Security
- Operational Environment
- Cryptographic Key Management
- EMI/EMC requirements
- Self Tests
- Design Assurance
- Mitigation of Other Attacks

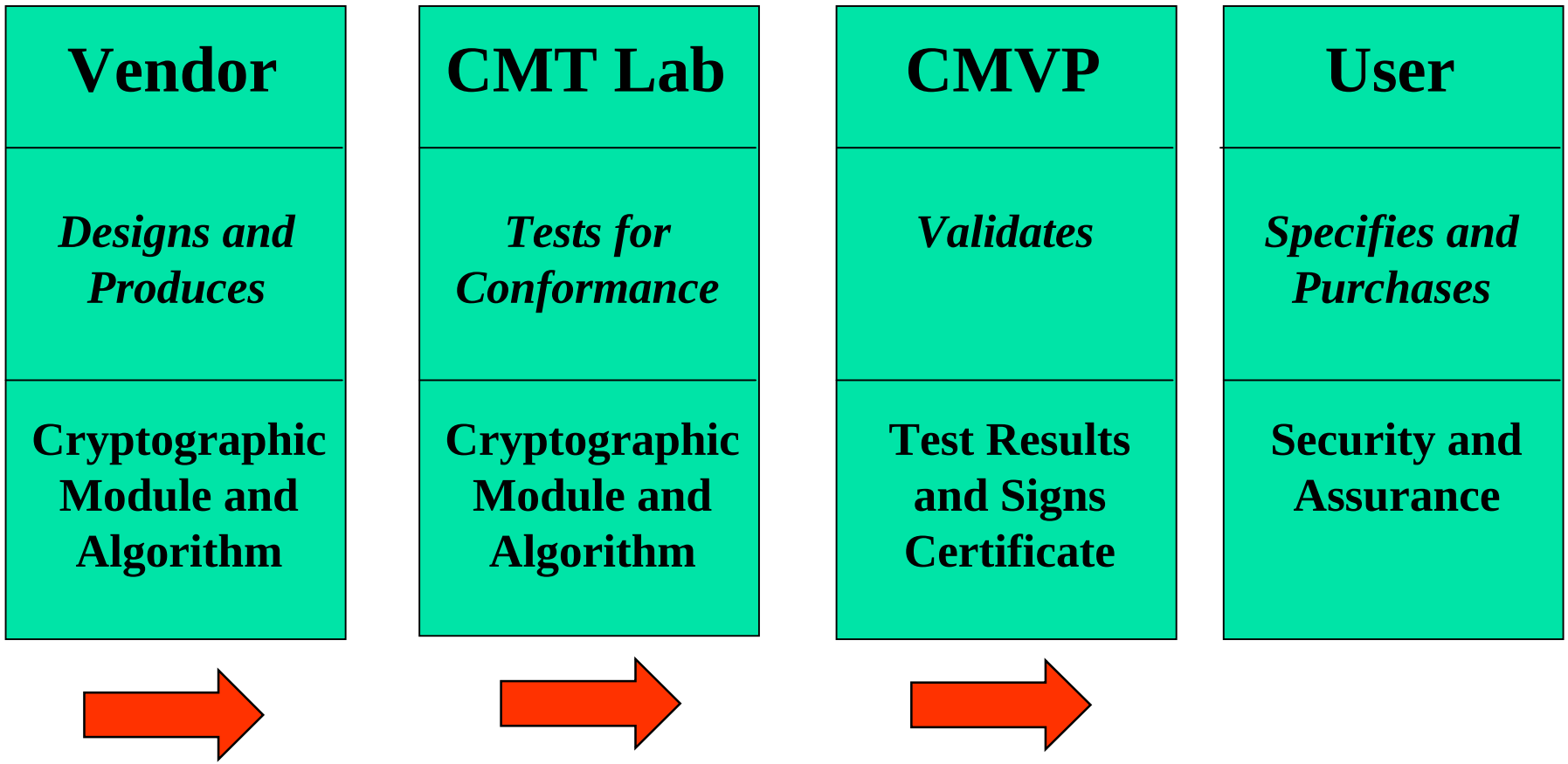
FIPS 140-2: Differences with FIPS 140-1

- Standard has not changed in **focus** or **emphasis**
- Language and terminology standardized
- Redundant and extraneous information removed
- Vague requirements removed or revised
- Standard was minimally restructured
- Authentication and Self-Test requirements strengthened
- Operating system requirements specified using the Common Criteria

FIPS 140-2 New Topics

- Configuration Management
- Delivery and Operation
- Development
  - Functional specifications
  - Formal model and informal proof
- Guidance documents
- Mitigation of Other Attacks

CMVP Testing: Validation Flow



CMVP Testing: Process

- Purpose of 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

CMVP Testing: Goals

- Among the laboratories...ensure
  - *Comparability* of test results
  - *Repeatability* of tests and test results
- Vendors
  - Required services are correctly performed by the laboratory
- Among users
  - Comprehensive testing of the module/product
  - Cryptographic and other security features correctly implemented

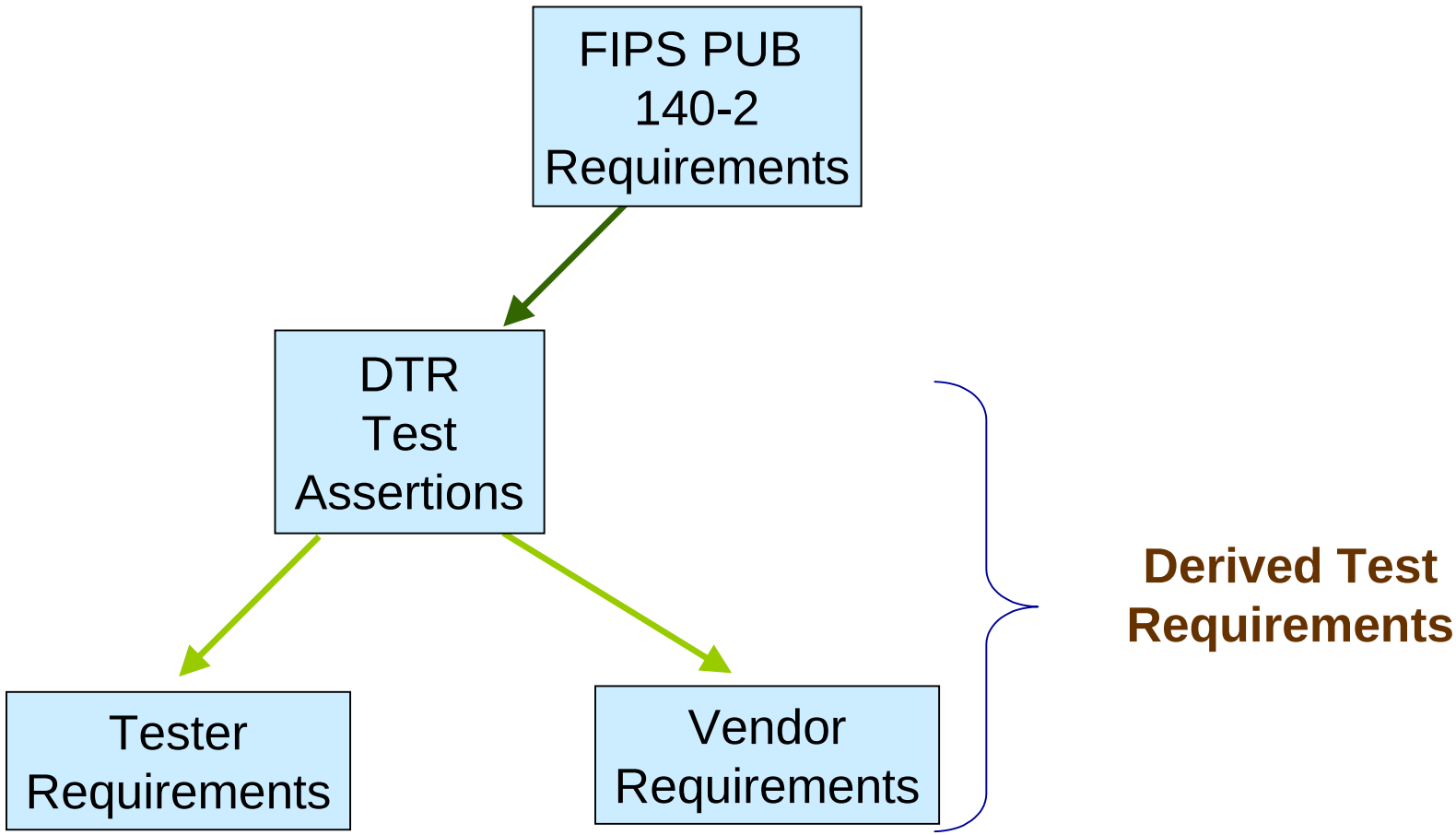
FIPS140-2 Testing: Primary Activities

- 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

FIPS 140-2 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

FIPS 140-2 Testing: Traceability

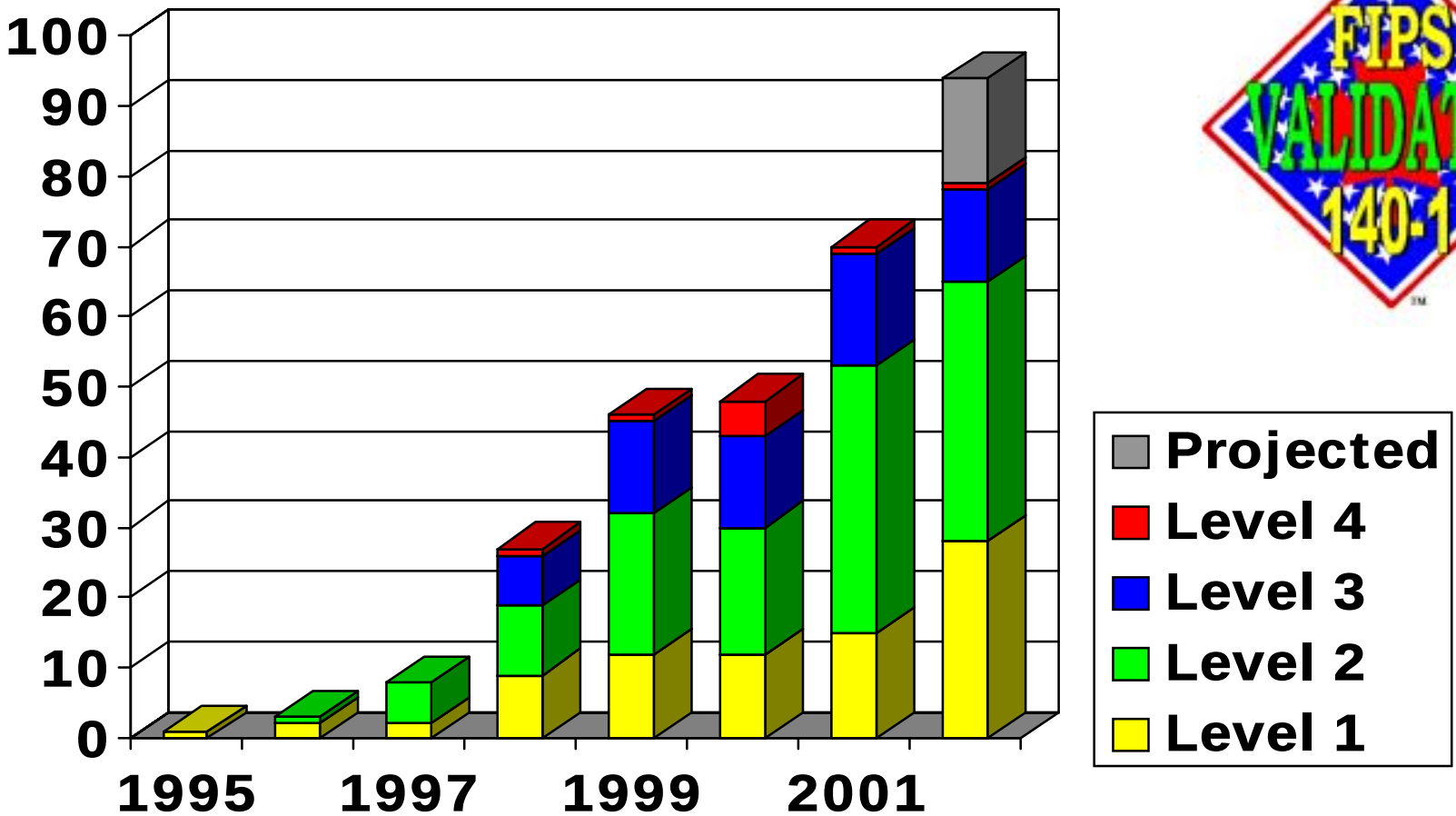


CMVP Status

- Continued record growth in the number of cryptographic modules validated
  - Over 275 Validations representing nearly 300 modules
- All four security levels of FIPS 140-1 represented on the Validated Modules List
- Over 75 participating vendors

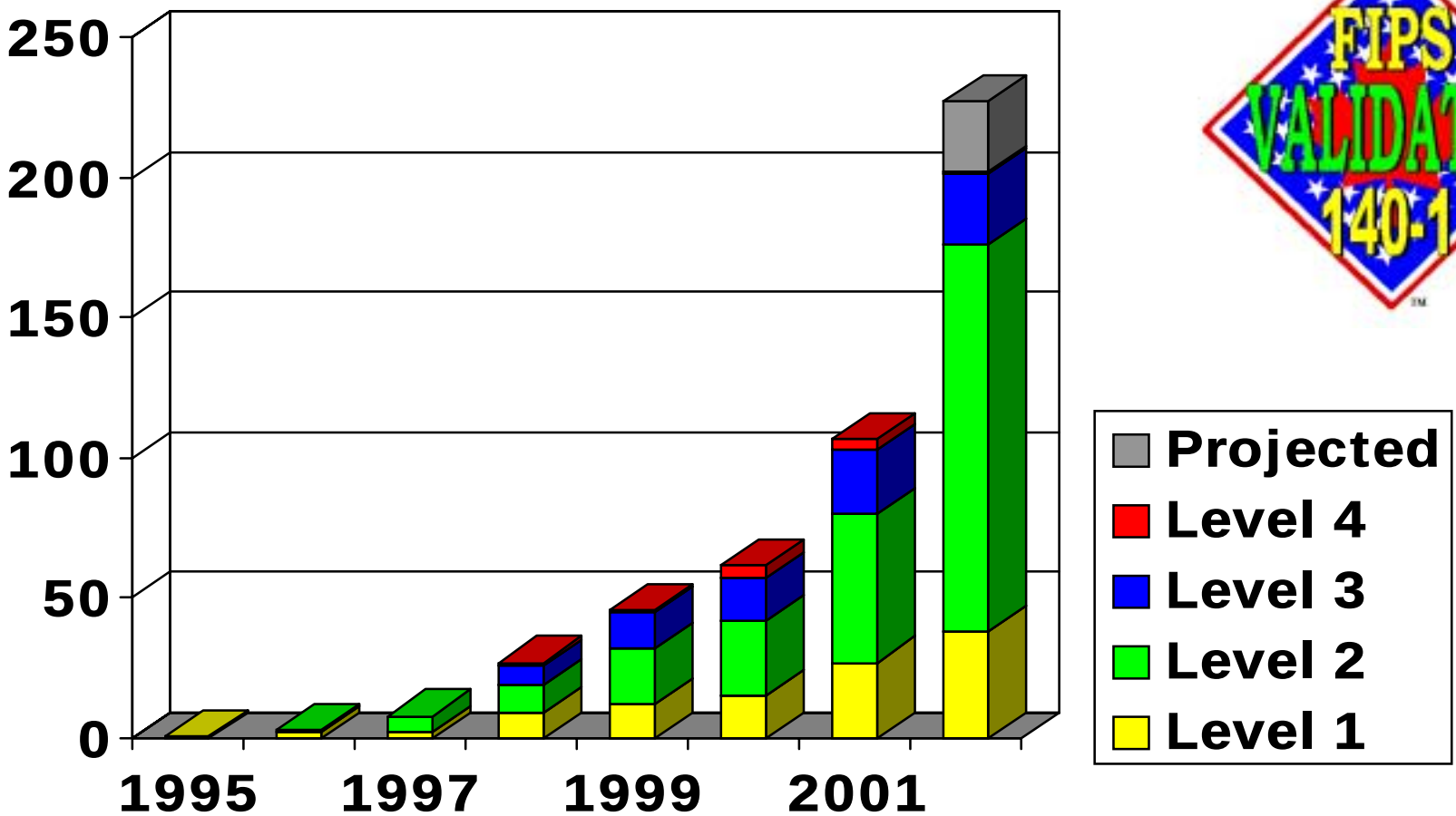
FIPS 140-1 and FIPS 140-2 Validations by Year and Level

(November 25, 2002 – Certificates Issued)

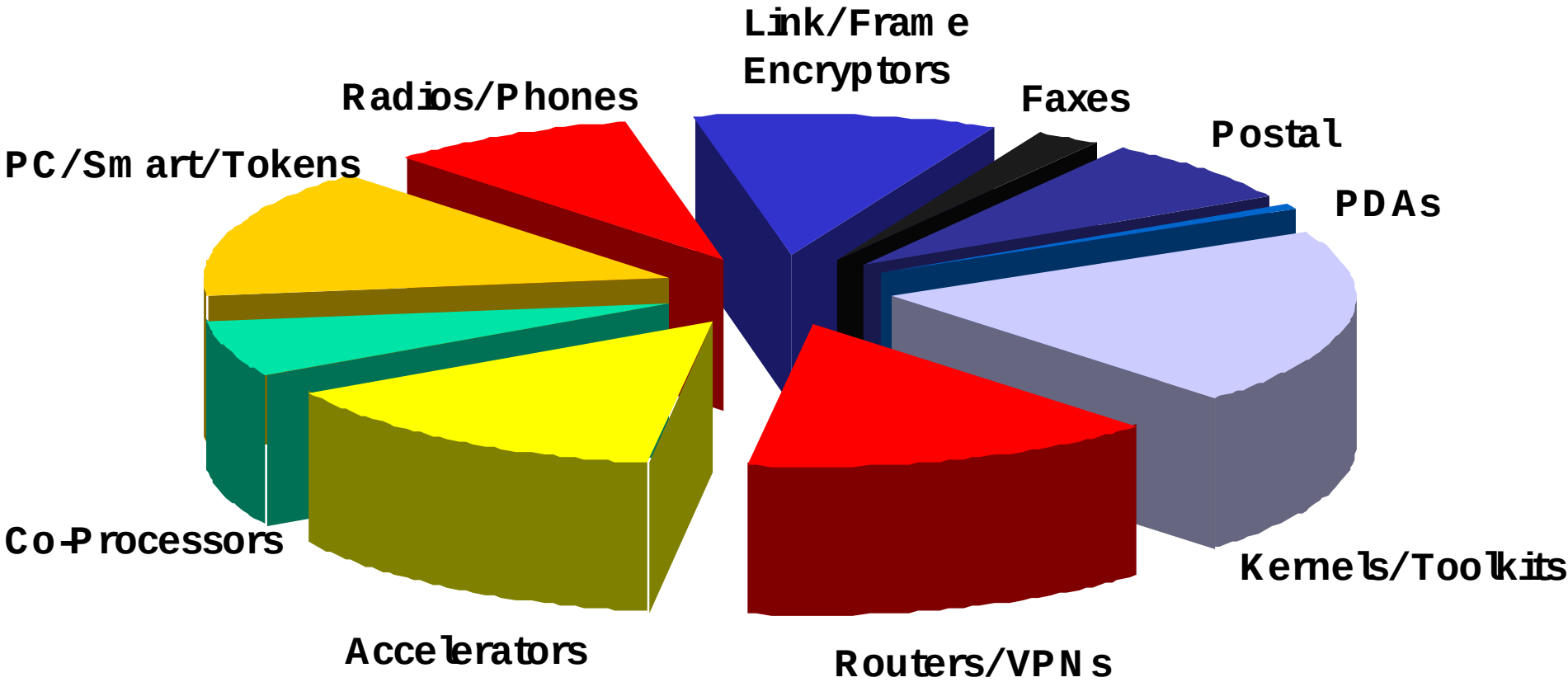


FIPS 140-1 and FIPS 140-2 Validations by Year and Level

(November 25, 2002 – Modules Validated)



Validated Modules By Type




FIPS
VALIDATED
140-1
TM
Overnight, Priority, & Express Mail
Envelopes
Packages
Manila Envelopes
Return Receipt
Insured Mail
Delivery Confirmation
Certified Mail

Participating Vendors

(November 25, 2002)

3S Group Incorporated
ActivCard
Admiral Secure Products, Ltd.
AEP Systems
Alcatel
Algorithmic Research, Ltd.
Altarus Corporation
Attachmate Corp.
Avaya, Inc.
Blue Ridge Networks
Check Point Software Technologies Ltd.
Chrysalis-ITS Inc.
Cisco Systems, Inc.
Communications Devices, Inc.
Control Break International Corp.
Corsec Security, Inc.
Cryptek Inc.
CTAM, Inc.
Cylink Corporation
Dallas Semiconductor, Inc.
Datakey, Inc.
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.
GTE Internetworking
Hasler, Inc.
IBM
Intel Network Systems, Inc.
IRE, Inc.
ITT
Kasten Chase Applied Research
L-3 Communication Systems
Litronic, Inc.
Lucent, Inc.
M/A Com Wireless Systems
Microsoft Corporation
Motorola, Inc.
Mykotronx. Inc
National Semiconductor Corp.
nCipher Corporation Ltd.
Neopost
Neopost Industrie
Neopost Ltd.
Neopost Online
Netscape Communications Corp.
NetScreen Technologies, Inc.
Network Associates, Inc.
Nortel Networks
Novell, Inc.
Oberthur Card Systems
Oracle Corporation
Pitney Bowes, Inc.
Pointsec Mobile Technologies
PrivyLink Pte Ltd
PSI Systems, Inc.
Rainbow Technologies
RedCreek Communications
Research In Motion
RSA Security, Inc.
SchlumbergerSema
Securit-e-Doc, Inc.
Spyrus, Inc.
Stamps.com
Sun Microsystems, Inc.
Technical Communications Corp.
Thales e-Security
TimeStep Corporation
Transcrypt International
Tumbleweed Communications Corp.
V-ONE Corporation, Inc.

Final Conclusion: Buyer Beware!

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

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

- Annabelle Lee - annabelle.lee@nist.gov
- Randy Easter - randall.easter@nist.gov
- Sharon Keller - sharon.keller@nist.gov
- Ron Tencati – ronald.tencati@nist.gov

CMVP

Conformance through Testing

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

Additional Background and Information

Web Site Examples

Cryptographic Module Validation Program

Standards and Their Related Documents:

- FIPS 140-1
- FIPS 140-2
- AES, Triple-DES, DES, Skipjack
- DSA, RSA, ECDSA
- SHA-1

- MAC
- X9.17

Announcements and Notices
Updated 05/29/2002

Validation Lists

Testing Laboratories

FAQs
Updated 06/14/2002

Helpful Documentation

Contacts

Computer Security Resource Clearinghouse

Computer Security Division

Cryptographic Module Validation (CMV) Program

NIST National Institute of Standards and Technology

Agencies may continue to purchase, retain and use FIPS 140-1 validated products after May 25, 2002.
All CMT Laboratories test cryptographic modules to FIPS 140-2.
As of May 26, 2002, NIST and CSE will only accept validation test reports for cryptographic modules against FIPS 140-2 and the FIPS 140-2 DTR.

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 (CMV) Program** encompasses validation testing for cryptographic modules and algorithms:

Cryptographic Modules

- FIPS 140-1: *Security Requirements for Cryptographic Modules*, January 4, 1994.
- FIPS 140-2: *Security Requirements for Cryptographic Modules*, May 25, 2001. Change Notice 1: 10/10/2001

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 186-2 and FIPS 180-1: *Digital Signature Standard (DSS)* and *Secure Hash Standard (SHS)*, which specify the **DSA**, **RSA**, **ECDSA**, and **SHA-1** algorithms
- FIPS 185: *Escrowed Encryption Standard (EES)*, which specifies the **Skipjack** algorithm

140-1 and 140-2 Validation List

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

2002, *2001*, *2000*, *1999*, *1998*, *1997-95*

****** 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. ******

Cert#	Vendor	Cryptomodule	Module Type	Val. Date	Level / Description
279	**Control Break International Corporation** 2338 Immokalee Road, #172, Naples , FL 34110 USA -Dawn Cole TEL: 941-596-8962 FAX: 941-430-1916	**SafeBoot Client** (Software Version 4.1) *(When operated in FIPS mode)* **Validated to FIPS 140-1** **Security Policy** **Certificate**	Software	11/20/2002	***Overall Level:*** **1** -Operating System Security: Tested as meeting Level 1 with Microsoft Windows 95 SR2 (single user mode) *-FIPS-approved algorithms:* AES (Cert. #21); DSA (Cert. #53); SHA-1 (Cert. #71) *-Other algorithms:* Diffie-Hellman (key agreement) Multi-chip standalone "SafeBoot is a high performance software solution that provides sector- level encryption of a PC's hard drive in a manner that is totally transparent to the user. In addition, the centralized SafeBoot management system provides robust recovery tools, administration, and implementation."
	Entrust CygnaCom 7927 Jones Branch Drive, Suite 100 West, McLean , VA 22101 USA				***Overall Level:*** **1** -Operating System Security: Tested as meeting Level 1 with SCO CMW+ V3.0.1 Operating System (single user mode) *-FIPS-approved algorithms:* Triple-DES

Advanced Encryption Standard Algorithm Validation List

Last Update: November 19, 2002

The page provides technical information about implementations that have been validated as conforming to the **Advanced Encryption Standard (AES) Algorithm**, as specified in Federal Information Processing Standard Publication 197, *Advanced Encryption Standard*.

The list below describes implementations which have been validated as correctly implementing the AES algorithm, using the tests found in The Advanced Encryption Standard Algorithm Validation Suite (AESAVS). This testing is performed by NVLAP accredited Cryptographic Module Testing (CMT) laboratories.

The implementations below consist of software, firmware, hardware, and any combination thereof. The National Institute of Standards and Technology (NIST) has made every attempt to provide complete and accurate information about the implementations described in this document. However, due to the possibility of changes made within individual companies, NIST cannot guarantee that this document reflects the current status of each product. It is the responsibility of the vendor to notify NIST of any necessary changes to its entry in the following list. A validation certificate issued to each vendor also indicates 1) the CMT laboratory that tested the implementation, and 2) the operating environment used to test the implementation (if software or firmware).

This list is ordered in reverse numerical order, by certificate number. Thus, the more recent validations are located closer to the top of the list. Also indicated after the date of validation are the **modes** (e.g., ECB, CFB, etc.), **states** (encryption(e) and/or decryption(d)), and **key sizes** (128-bit, 192-bit, and/or 256-bit) for which the implementation was validated:

Advanced Encryption Standard (AES) Algorithm Validated Implementations

Cert#	Vendor	Implementation	Val. Date	Modes/States/Key sizes/ Description
44	**IBM Zurich Research Laboratory** Saeumerstrasse 4, Rueschlikon, CH 8803 Switzerland -Michael Osborne TEL: (41) (1) 724 8458 FAX: (41) (1) 724 8953	**JCOP21id 32K** Version JCOP21id Mask 20 (firmware) Part #P8WE5033 AE9 1034 188i	11/14/2002	**ECB(e/d; 128,192,256); CBC(e/d; 128,192,256)** "The JCOP21id is IBM's multi-application smart card, designed to the Java Card v2.1.1 and Global Platform v2.0.1 specifications. The smart card features IBM's PKCS#15 applet which provides standardized high-level security services including, 2048 bit key generation, DES, 3DES, SHA, RSA and AES."
43	**Wei Dai** Groove Networks, Inc., 100 Cummings Center, Suite 535Q, Beverly, MA 01915	**Crypto++ Library** Version 5.01	11/14/2002	**ECB(e/d; 128,192,256); CBC(e/d; 128,192,256); CFB8(e/d; 128,192,256); CFB128(e/d; 128,192,256); OFB(e/d; 128,192,256)** "The Crypto++ Library is a free, open source C++ class library providing public key encryption, digital signatures, symmetric

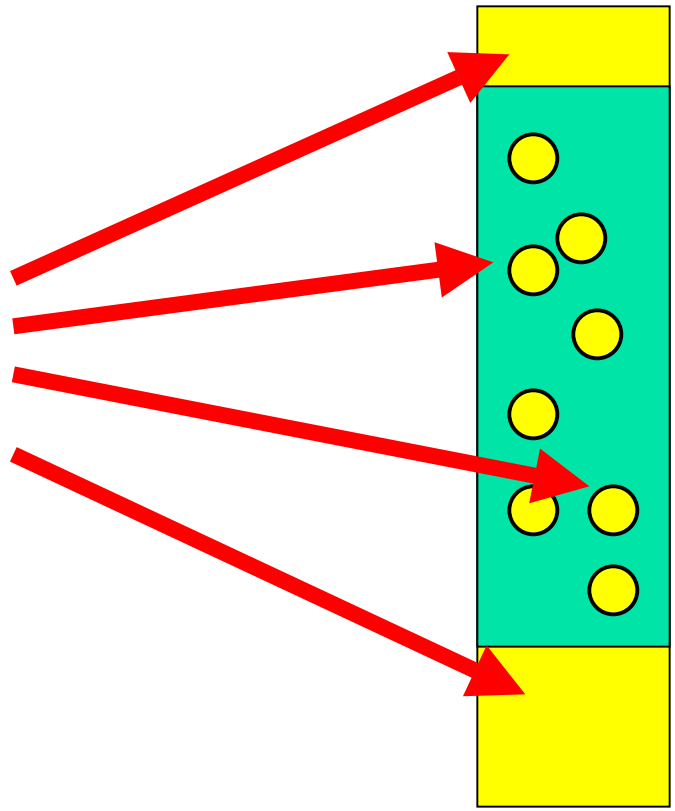
Revalidation Information

Revalidation: Specifics

- FIPS 140-2: An *updated* version of a previously validated cryptographic module
  - Modifications to hardware, software, firmware *do not* affect security
    - The testing laboratory reviews the changes and sends a letter to NIST/CSE
    - The Cryptographic Module Validation List is updated
  - Modifications to hardware, software, firmware affect *less than 30%* security relevant assertions
    - The testing laboratory tests:
      - The changed assertions (requirements)
      - All assertions listed in the regression test suite
      - New and updated assertions

Revalidation under FIPS 140-2 (less than 30% change)

Lab tests all the identified and remaining TEs



DTR

FIPS 140-2

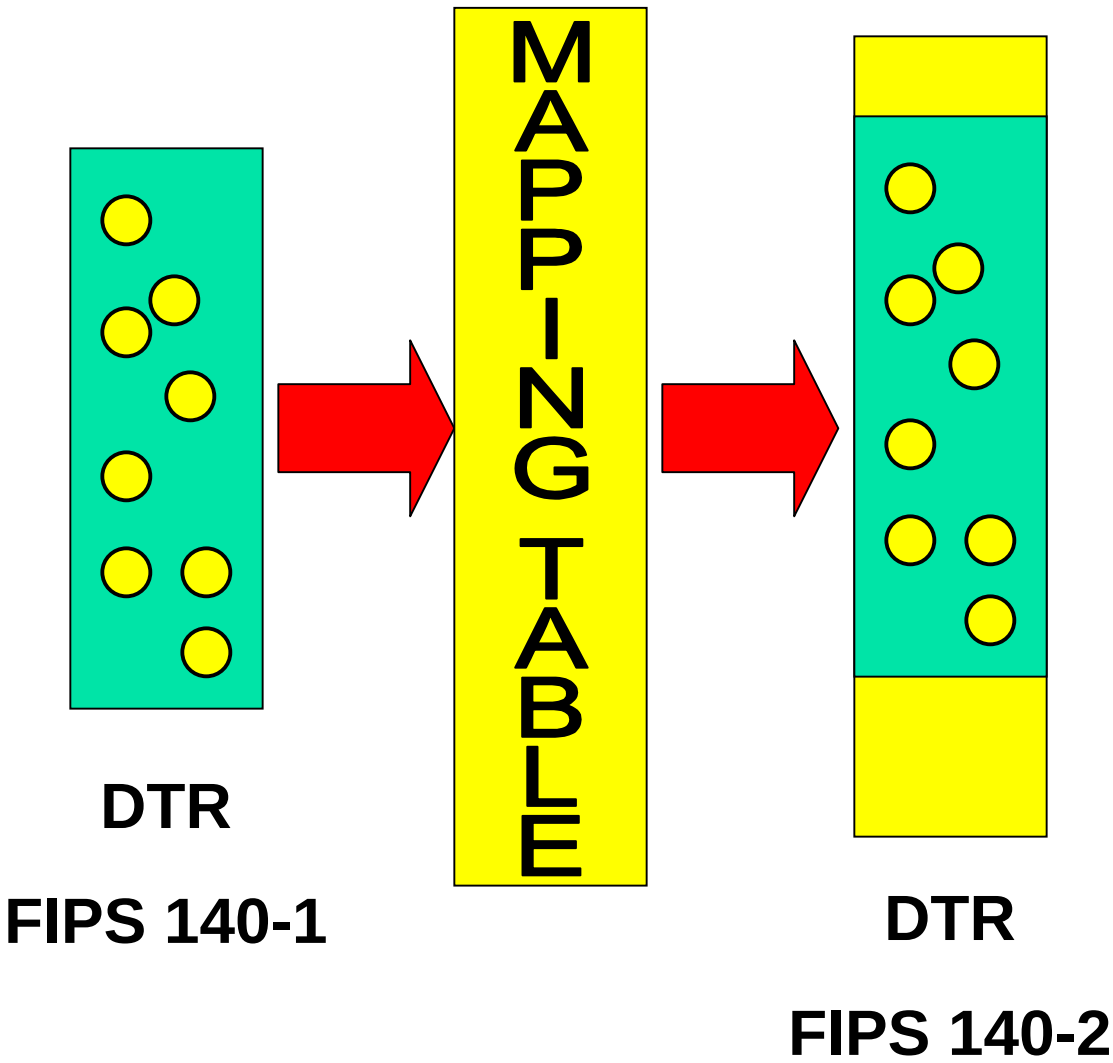
Revalidation (concluded)

- Modifications to hardware, software, firmware affect *greater than 30%* security relevant assertions
  - The testing laboratory performs a full validation testing
- Full validation required ...
  - Overall security level changes
  - Physical embodiment changes

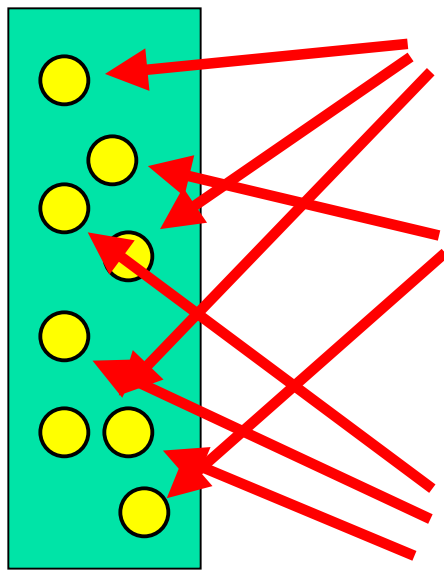
Revalidation: FIPS 140-1 to FIPS 140-2

- Significant increase in number of test items under FIPS 140-2 (+36%)
  - Some FIPS 140-1 assertions split into multiple FIPS 140-2 assertions
- CMVP intends to reuse the testing results from FIPS 140-1
- Draft mapping between FIPS 140-1 and 140-2

Revalidation: FIPS 140-1 to FIPS 140-2



Revalidation: Approach



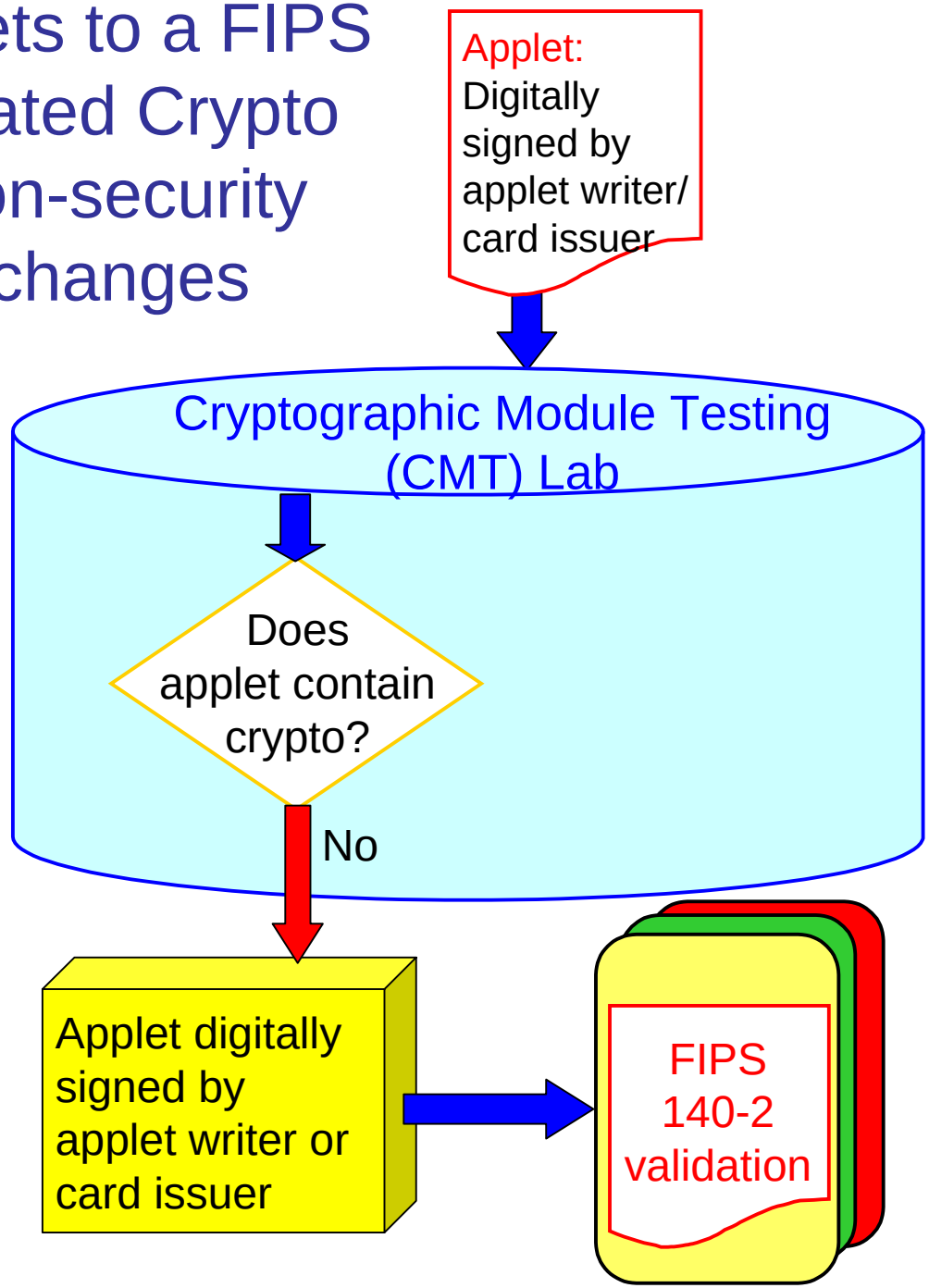
DTR

FIPS 140-2

- ✓ Lab identifies and tests TEs affected by change
- ✓ Lab identifies and tests TEs affected by new IGs and policies
- ✓ Operational tests per regression test suite

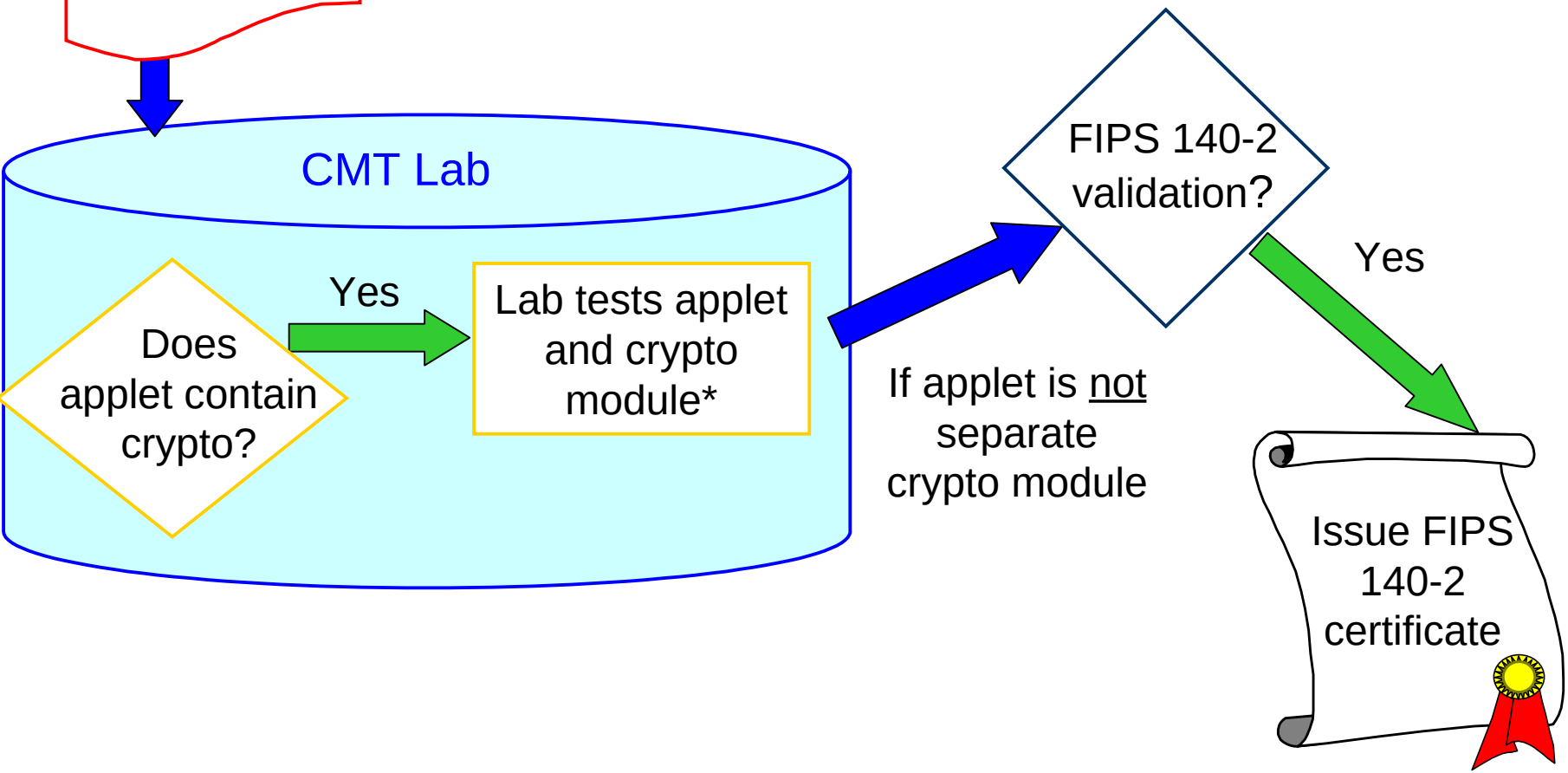
JAVA and FIPS 140-2

Adding Applets to a FIPS 140-2 Validated Crypto Module: non-security relevant changes



Adding Applets to a FIPS 140-2 Validated Crypto Module: revalidation

Applet: digitally signed by applet writer or card issuer



*Crypto module must be tested against regression test suite and new/modified assertions

Adding/Modifying Applets to a FIPS 140-2 Validated Crypto Module: revalidation