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

March 03, 2006

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
- FIPS 140-3 – *under development*

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
  - ISO/IEC 19790 *Security Requirements for 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

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?

Benefits! … Making a Difference

- **Cryptographic Modules Surveyed (during testing)**
  - 48.8% Security Flaws discovered
  - 96.3% FIPS Interpretation and Documentation Errors
- **Algorithm Validations (during testing) (DES, Triple-DES, DSA and SHA-1)**
  - 26.5% Security Flaws
  - 65.1% FIPS Interpretation and Documentation Errors
- **Areas of Greatest Difficulty**
  - Physical Security
  - Self Tests
  - Random Number Generation
  - Key Management

Using FIPS Validated Cryptographic Modules

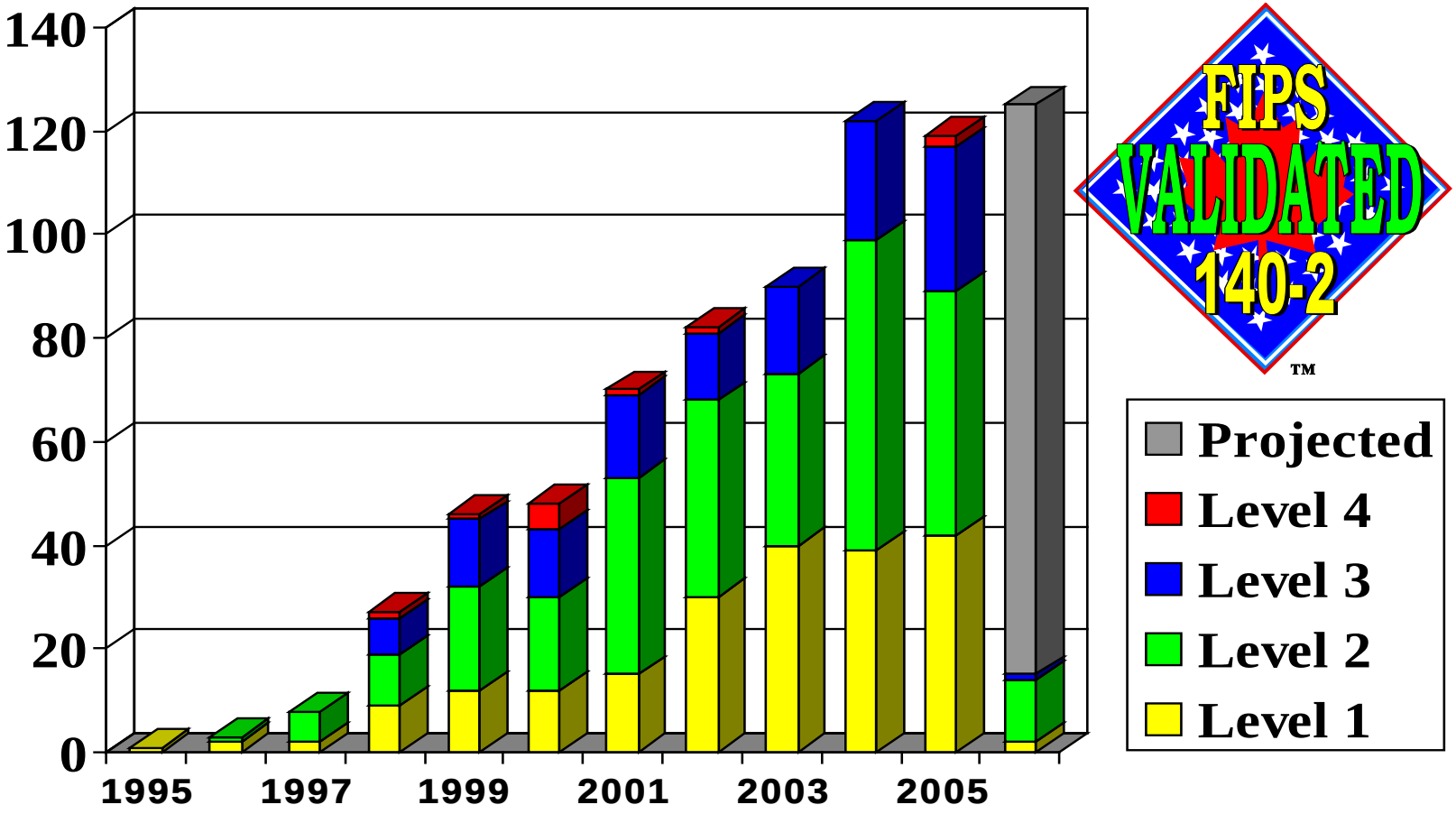
- Cryptographic modules *may* be embedded in other products
  - Applicable to hardware, software, and firmware cryptographic modules
  - Must use the validated version and configuration
  - e.g. software applications, cryptographic toolkits, postage metering devices, radio encryption modules
- Does not 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 >630 Validations representing over 1000 modules
- All four security levels of FIPS 140-2 represented on the Validated Modules List
- Over 150 participating vendors
- New NVLAP accredited Cryptographic Module Testing Laboratories

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

(January 31, 2006)



Participating Vendors

(December 31, 2005 – 157 Total)

3Com Corporation
3e Technologies International, Inc.
3S Group Incorporated
ActivCard
ActivCard Inc., Atmel, Inc. and MartSoft, Inc.
Admiral Secure Products, Ltd.
AEP Systems
Airespace, Inc.
AirMagnet, Inc.
AKCode, LLC
Aladdin Knowledge Systems, Ltd.
Alcatel
Algorithmic Research, Ltd.
Altarus Corporation
Aruba Wireless Networks, Inc.
Atalla Security Products of Hewlett Packard Corporation
Attachmate Corp.
Axalto
Avaya, Inc.
Backbone Security.com, Inc.
Blue Ridge Networks
Bluefire Security Technologies
Bluesocket, Inc.
Bodacion Technolgies
C4 Technology, Inc.
Carrier Access Corporation and TeamF1
Caymas Systems, Inc.
Certicom Corp.
Check Point Software Technologies Ltd.
Chunghwa Telecom Co., Ltd Telecommunications Labs
CipherOptics, Inc.
Cisco Systems, Inc.
Colubris Networks, Inc.
Communications Devices, Inc.
Control Break International Corp.
Corsec Security, Inc.
Cranite Systems, Inc.
Credant Technologies Corporation
Cryptek Inc.
CTAM, Inc.
CyberGuard Corporation
D'Crypt Pte Ltd.
Dallas Semiconductor, Inc.
Decru, Inc.
Dreifus Associates Limited Inc.
ECI Systems & Engineering
E.F. Johnson Co.
Encotone Ltd.
Entrasys Networks
Entrust Inc.
Entrust CygnaCom
Eracom Technologies Group, Eracom Technologies Australia, Pty. Ltd.
F-Secure Corporation
Fortinet, Inc.
Fortress Technologies, Inc.
Forum Systems, Inc.
Francotyp-Postalia
Funk Software, Inc.
Gemplus Corp.
Gemplus Corp. and ActiveCard Inc.
General Dynamics Decision Systems
Giesecke & Devrient
Good Technology
GTE Internetworking
Hasler, Inc.
High Density Devices AS
IBM® Corporation
iDirect Technologies
IMAG Technologies, Inc.
Information Security Corporation
Intel Network Systems, Inc.
IP Dynamics, Inc.
ITServ Inc.
ITT
JP Mobile, Inc.
Juniper Networks, Inc.
Kasten Chase Applied Research
L-3 Communication Systems
Lipman Electronic Engineering Ltd.
Litronic, Inc.
Lucent Technologies
M/A-Com, Inc.
Meganet Corporation
Microsoft Corporation
Mitsubishi Electric Corporation
Motorola, Inc.
Mykotronx. Inc
National Semiconductor Corp.
nCipher Corporation Ltd.
Neopost
Neopost Industrie

Participating Vendors

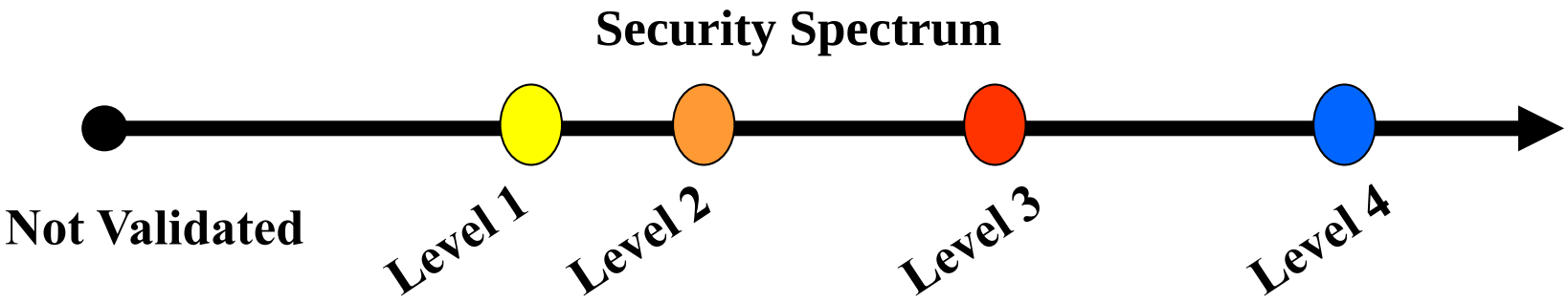
(December 31, 2005 – 157 Total)

Neopost Ltd.
Neopost Online
NeoScale Systems, Inc.
Netscape Communications Corp.
NetScreen Technologies, Inc.
Network Security Technology (NST) Co.
Nokia Enterprise Mobility Systems
Nortel Networks
Novell, Inc.
Oberthur Card Systems
Oceana Sensor Technologies, Inc.
Oracle Corporation
Palm Solutions Group
PalmSource, Inc.
PC Guardian Technologies, Inc.
PGP Corporation
Phaos Technology Corporation
Pitney Bowes, Inc.
Pointsec Mobile Technologies
Prism Payment Technologies (Pty) Ltd
Priva Technologies, Inc.
PrivyLink Pte Ltd
PSI Systems, Inc.
Real Time Logic, Inc.
Realia Technolgies S.L.
RedCannon Security
RedCreek Communications
ReefEdge, Inc.
RELM Wireless Corporation
Research In Motion
Rockwell Collins, Inc.
RSA Security, Inc.
SafeNet, Inc.
SafeNet, Inc. and Cavium Networks
SchlumbergerSema
Schweitzer Engineering Laboratories, Inc.
Secure Systems Limited
Security-e-Doc, Inc.
Sigaba Corporation
Simple Access Inc.
SkyTel Corp.
Snapshield, Ltd.
SonicWall, Inc.
SPYRUS, Inc.
SSH Communications Security Corp.
Stamps.com
Standard Networks, Inc.
StoneSoft Corporation
Sun Microsystems, Inc.
Symantec Corporation
Symbol (Columbitech)
Technical Communications Corp.
Telkonet Communications Inc.
Thales e-Security
TimeStep Corporation
Transcrypt International
Tricipher, Inc.
Trust Digital, LLC
Tumbleweed Communications Corp.
Utimaco Safeware AG
Voltage Security, Inc.
V-ONE Corporation, Inc.
Vormetric, Inc.
Wei Dai
WinMagic Incorporated
WRQ, Inc.

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



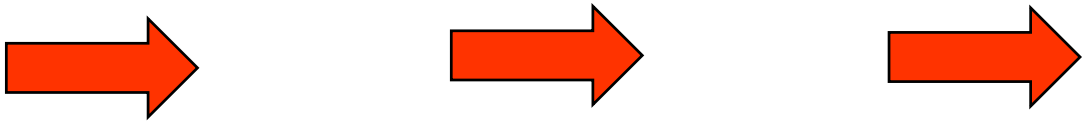
- Level 1 is the lowest, Level 4 most stringent
- Requirements are primarily cumulative by level
- Overall rating is lowest rating in all sections
- Validation is applicable when a module is configured and operated in accordance with the level to which it was tested and validated

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

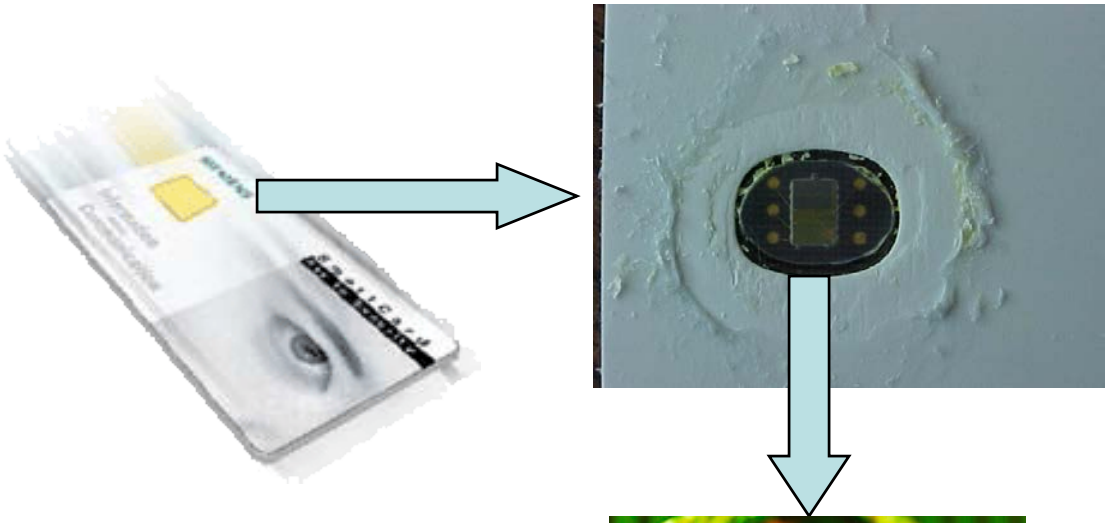
CMVP Testing and Validation Flow

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**



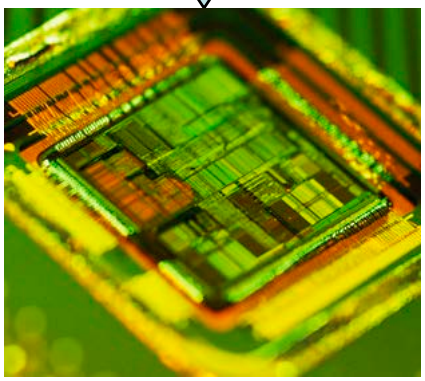
Cryptographic Module Specification

- 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



FIPS 140-2 boundary defined as the single chip. Includes:

- Hardware
- Firmware
- Software/Applets



Any modification, addition and/or deletion of a component or part invalidates the validated module.

CMVP Testing: Process

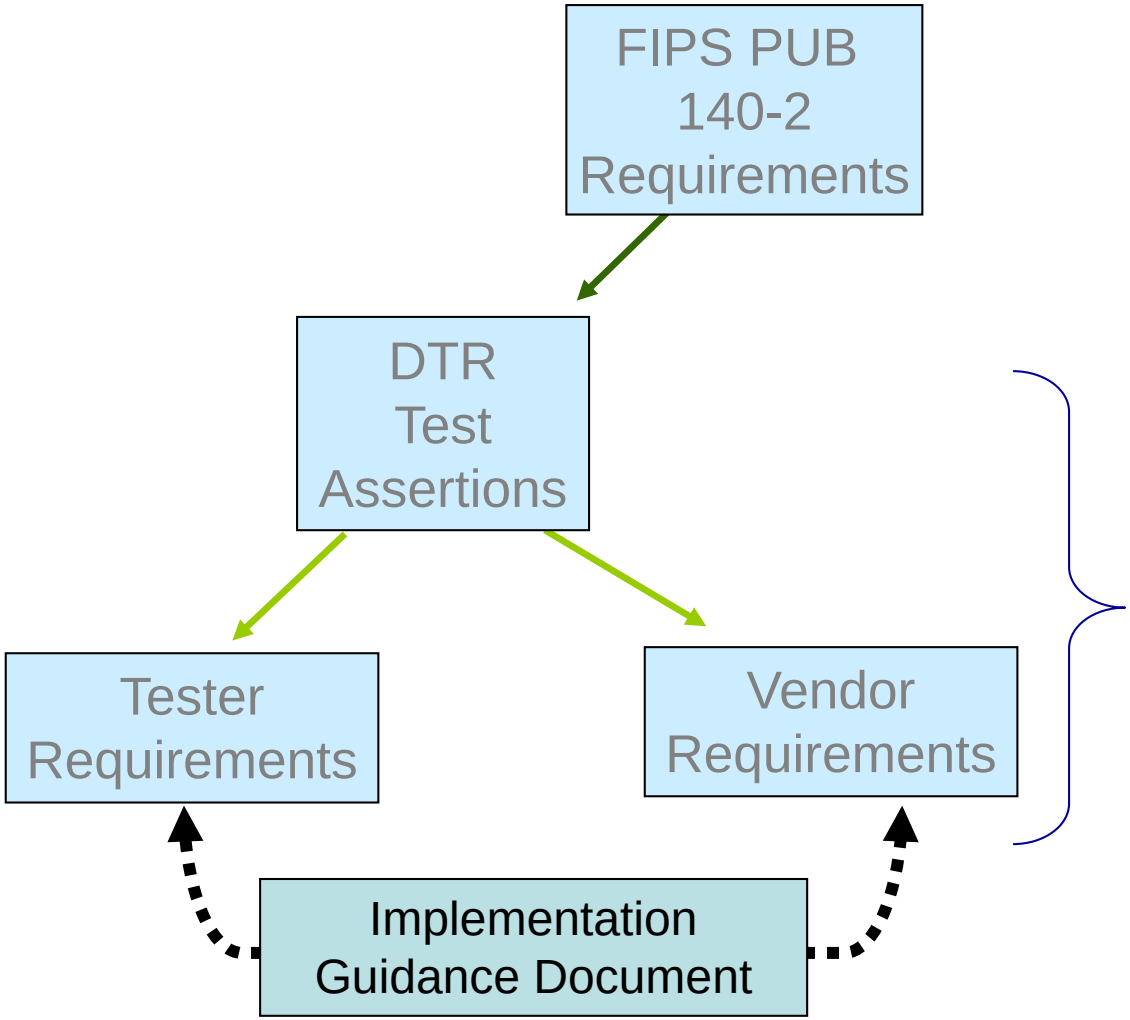
- CMVP
  - Conformance testing of cryptographic modules using the Derived Test Requirements (DTR)
  - Not evaluation of cryptographic modules. Not required are:
    - Vulnerability assessment
    - Design analysis, etc.
- Laboratories
  - Test submitted cryptographic modules
- NIST/CSE
  - Validate tested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

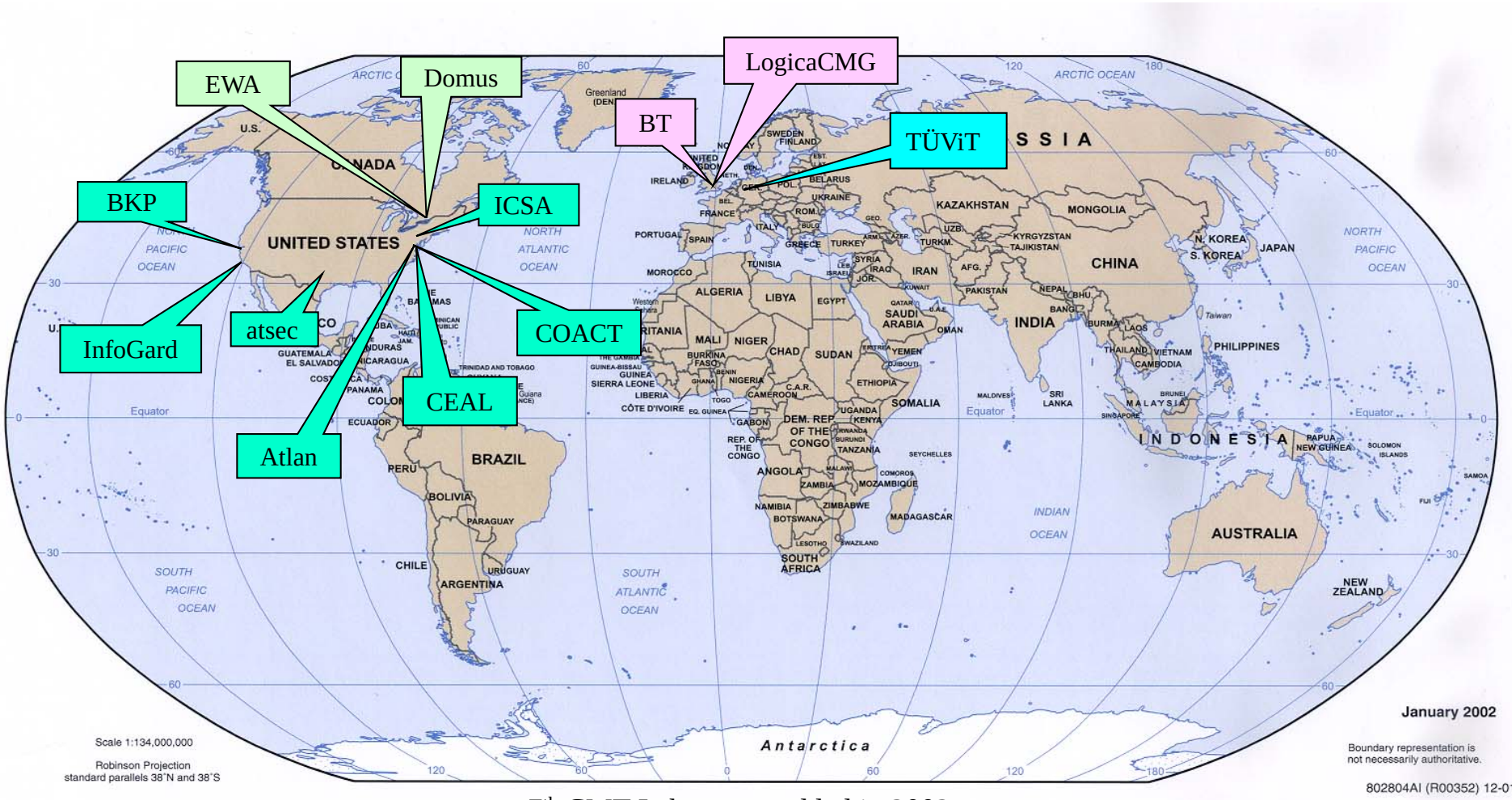


Derived Test Requirements

Cryptographic Module Testing (CMT) Laboratories

- Twelve 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



7th CMT Laboratory added in 2002
8th CMT Laboratory added in 2003
9th CMT Laboratory added in 2004
10th, 11th and 12th CMT Laboratories added in 2005

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
- Assumes same CMT laboratory performed the original full testing.

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
- Assumes same CMT laboratory performed the original full testing.

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

CMVP
Conformance through Testing

FIPS VALIDATED 140-2

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

NVLAP Accredited FIPS 140-2 CMT Lab

Vendor selects a lab;
Submits module for testing;
Module IUT

1

Cryptographic Module Vendor

Test for conformance To FIPS 140-2; Writes test report

1a

Lab submits questions for guidance and clarification

NIST/CSE issue testing and Implementation Guidance

4 Module Coordination

Issue validation certificate (via lab to the vendor)

5a

Cost Recovery Fee Received Prior to Validation

Module's Test Report

2 CMT Test Report to NIST/CSE for validation; Module Review Pending

NIST/CSE

3

Reviewer Assigned Module Under Review

List of Validated FIPS 140-2 Modules

5 Finalization; NIST adds module to validated modules list at www.nist.gov/cmvp

The Cryptographic Algorithm Validation System

- Designed and developed by NIST
- Supplied to NVLAP accredited testing laboratories
- Provides uniform validation testing for *Approved* cryptographic algorithms
- Provides thorough testing of the implementation
- Types of errors found by CAVS range from pointer problems to incorrect behavior of the algorithm implementation.

CAVS Testing

Currently provides validation testing for

- Data Encryption Standard (DES)
- Triple Data Encryption Standard (TDES)
- Advanced Encryption Standard (AES)
- Digital Signature Standard (DSS)
- SHA1, SHA224, SHA256, SHA384, SHA512
- Random Number Generator (RNG)
- RSA Signature Algorithm
- Keyed Hash Message Authentication Code (HMAC)
- Counter with Cipher Block Chaining (CBC) MAC (CCM)
- Elliptic Curve Digital Signature Algorithm (ECDSA)

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

CMVP Conformance Through Testing — FIPS 140-2 — NIST National Institute of Standards and Technology

Withdrawal of DES

DES Transition Plan

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

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:

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.

The CMVP was established by NIST and the Communications Security Establishment (CSE) of the Government of Canada in July 1995. All of the tests under the CMVP are handled by third-party laboratories that are accredited as Cryptographic Module Testing (CMT) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). Vendors interested in validation testing may select any of the twelve accredited labs.

A diagram is available, which maps the general flow of the CMVP FIPS 140-2 testing process.

Need assistance?

Last Modified: December 16, 2005
Computer Security Division
National Institute of Standards and Technology

NIST is an agency of the U.S Commerce Department's Technology Administration

NIST

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

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

CSE

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