CRYPTOGRAPHIC MODULE VALIDATION PROGRAM

Random Number Generators

Randall J. Easter

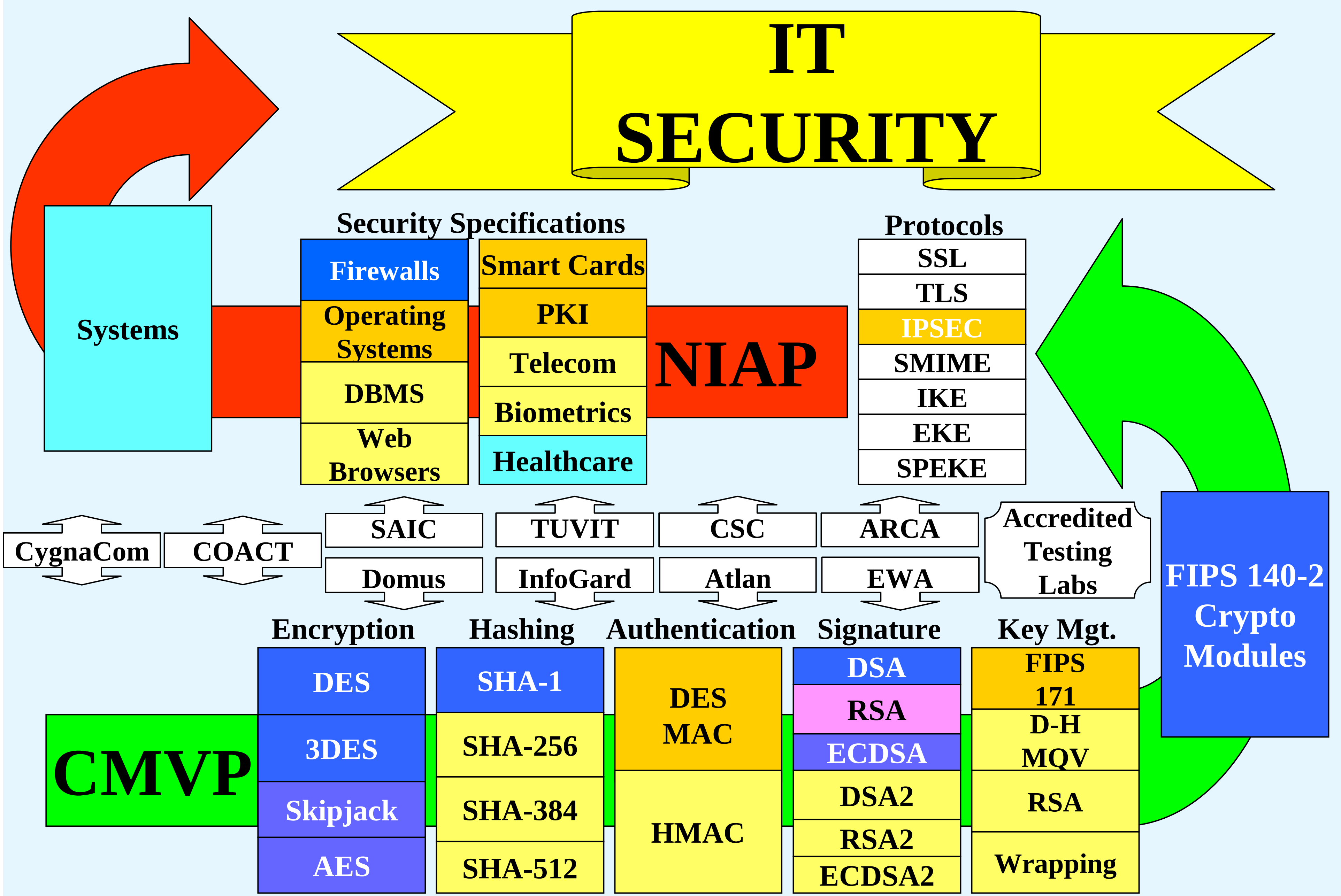
NIST

Computer Security Division

August 2002

FIPS
VALIDATED
140-1
™

FIPS
VALIDATED
140-2
TM



IT SECURITY

Systems

NIAP

Security Specifications

Firewalls

Operating Systems

DBMS

Web Browsers

Smart Cards

PKI

Telecom

Biometrics

Healthcare

Protocols

SSL

TLS

IPSEC

SMIME

IKE

EKE

SPEKE

CygnaCom

COACT

SAIC

Domus

TUVIT

InfoGard

CSC

Atlan

ARCA

EWA

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

HMAC

Signature

DSA

RSA

ECDSA

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

Philosophy

- Strong commercially available cryptographic products are needed
- Government must work with the commercial sector and the cryptographic community for:
  - security,
  - interoperability, and
  - assurance

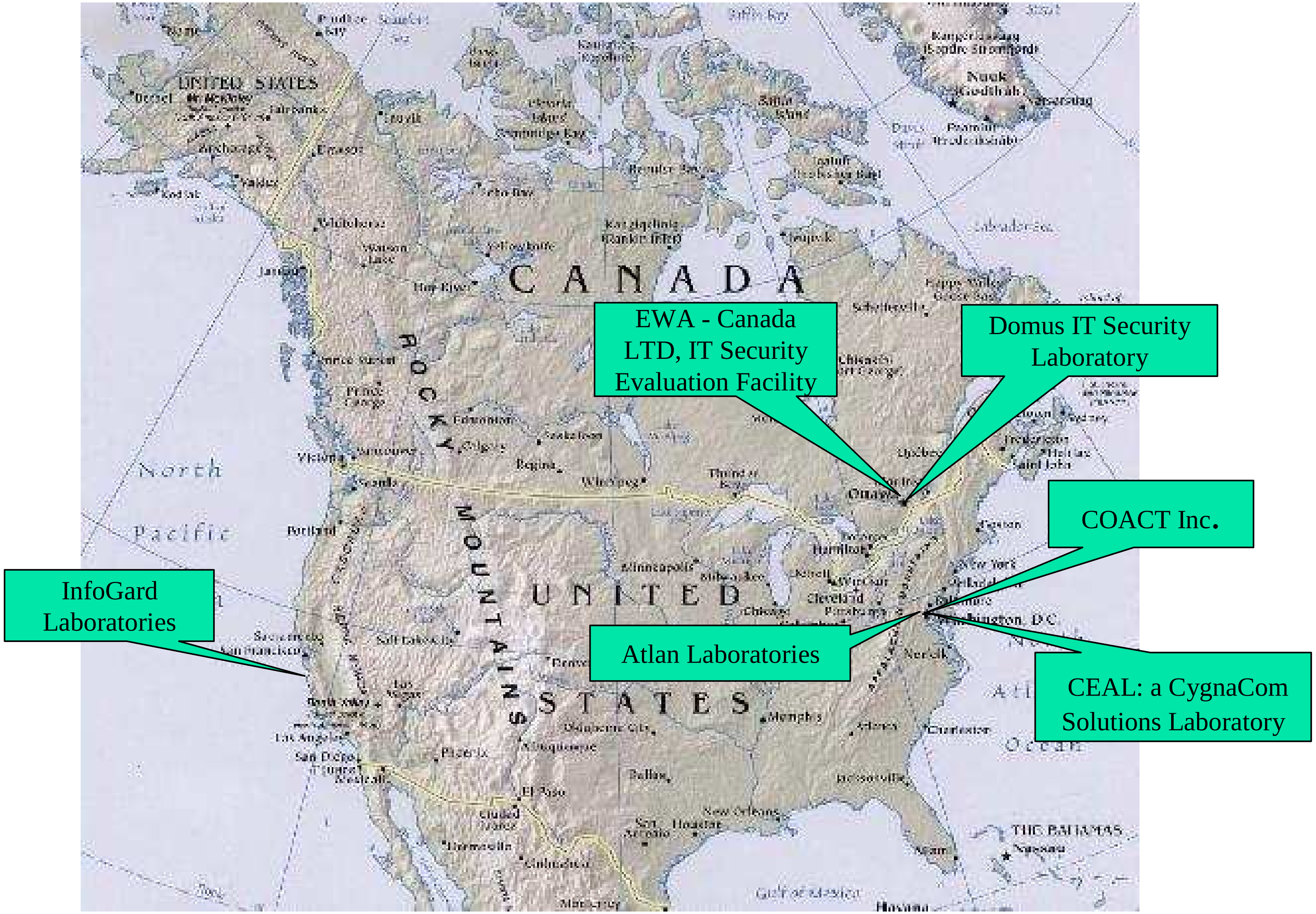
Cryptographic Module Validation Program (CMVP)

- 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
- Six NVLAP-accredited testing laboratories
  - True independent 3rd party accredited testing laboratories
  - Cannot test and provide design assistance

Applicability of FIPS 140-2

- U.S. Federal organizations must use validated cryptographic modules
  - Set of hardware, and/or software, and/or firmware
  - Implements a cryptographic algorithm
  - Contained within a defined boundary
- Government of Canada departments are recommended by CSE to use validated cryptographic modules
- International recognition

CMVP Accredited Laboratories



EWA - Canada LTD, IT Security Evaluation Facility

Domus IT Security Laboratory

COACT Inc.

InfoGard Laboratories

Atlan Laboratories

CEAL: a CygnaCom Solutions Laboratory

Sixth CMT laboratory added in 2001

CMVP

Conformance through Testing

… Making a Difference

- **164 Cryptographic Modules Surveyed (during testing)**
  - 80 (48.8%) Security Flaws discovered
  - 158 (96.3%) FIPS Interpretation and Documentation Errors
- **332 Algorithm Validations (during testing) (DES, Triple-DES, DSA and SHA-1)**
  - 88 (26.5%) Security Flaws
  - 216 (65.1%) FIPS Interpretation and Documentation Errors

- **Areas of Greatest Difficulty**
  - Physical Security
  - Self Tests
  - Random Number Generation
  - Key Management

… Making a Difference

- **Web Access**
  - November 2001 – 125,000 hits
  - Monthly average – 80,000 hits

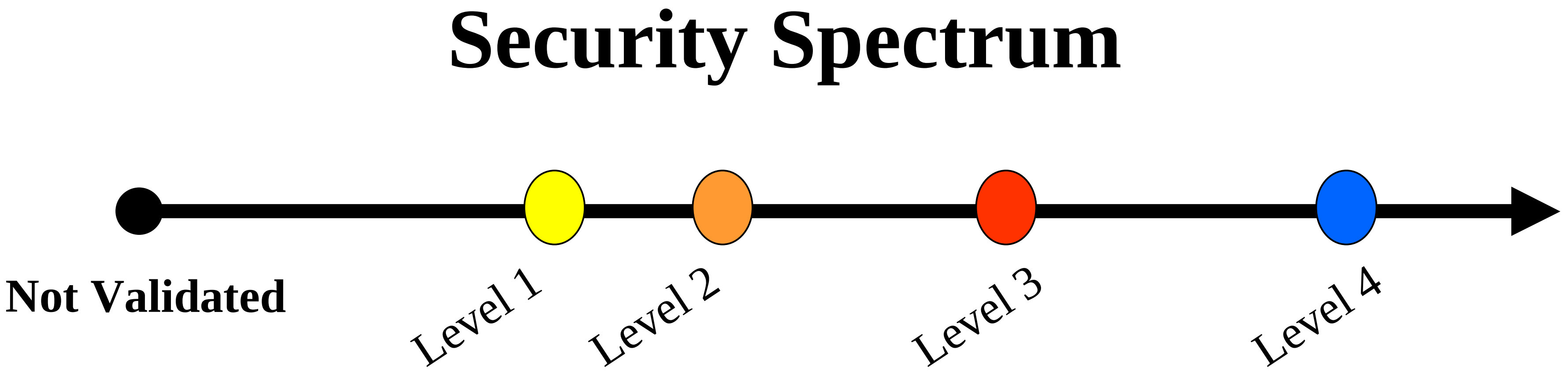
www.nist.gov/cmvp

csrc.nist.gov

CMVP Status
(August 2002)

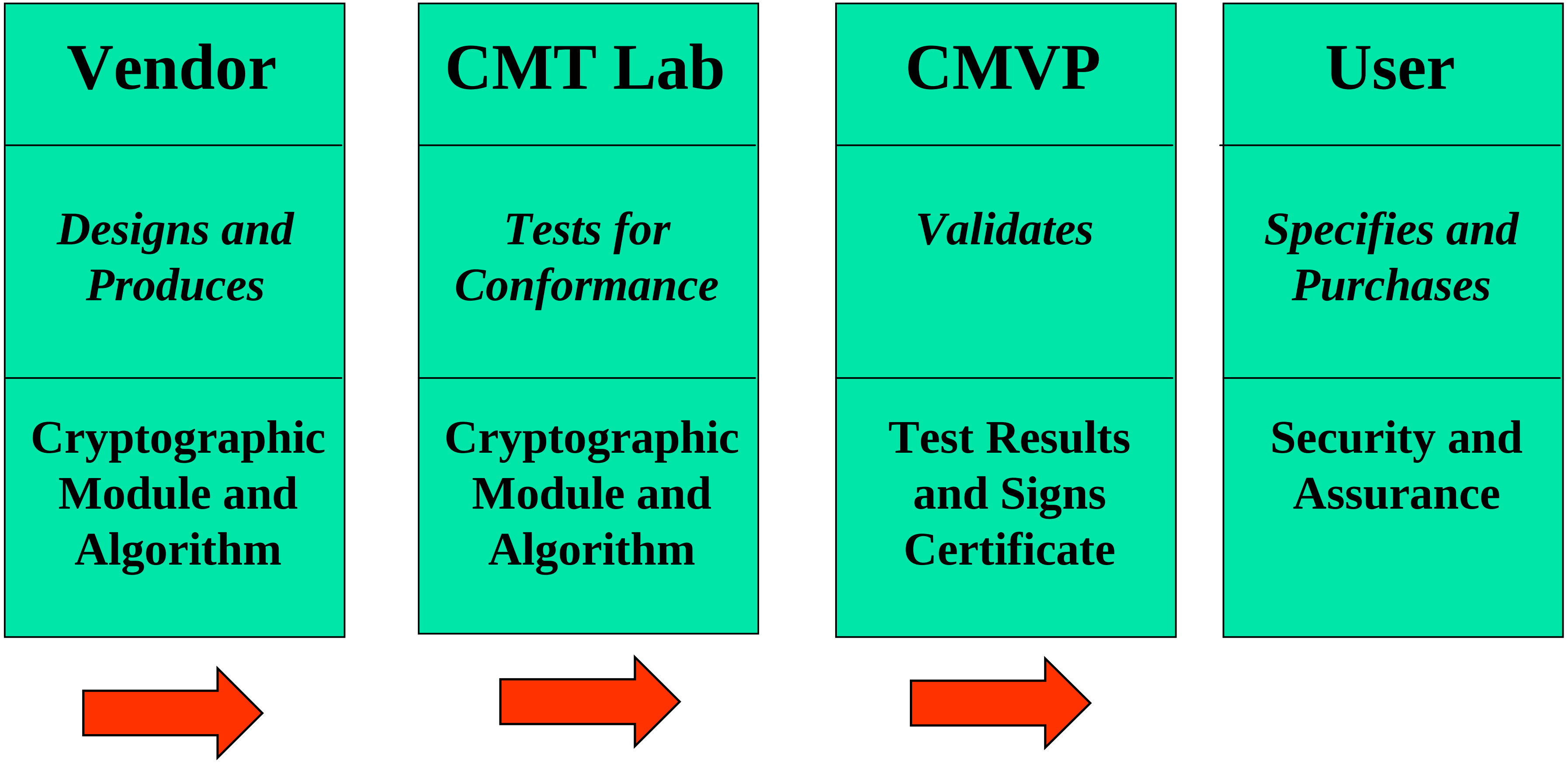
- Continued record growth in the number of cryptographic modules validated
  - Over 240 Validations representing nearly 280 modules
- All four security levels of FIPS 140-1 represented on the Validated Modules List
- Over *sixty* participating vendors

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**

Flow of a FIPS 140-2 Validation

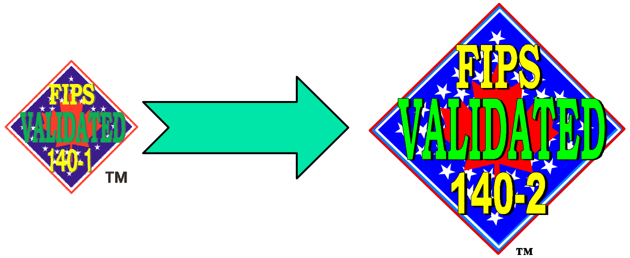


Vendor	CMT Lab	CMVP	User
Designs and Produces	*Tests for Conformance*	*Validates*	*Specifies and Purchases*
Cryptographic Module and Algorithm	**Cryptographic Module and Algorithm**	**Test Results and Signs Certificate**	**Security and Assurance**

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 - Testing Begins



- FIPS 140-2 testing officially began November 15, 2001
- FIPS 140-1 testing ends May 25, 2002
- Testing laboratories may submit FIPS 140-1 validation test reports until May 25, 2002
- After May 25, 2002 **<u>all</u>** validations and revalidations must be done against FIPS 140-2
- Agencies may continue to purchase, retain and use FIPS 140-1 validated products after May 25, 2002

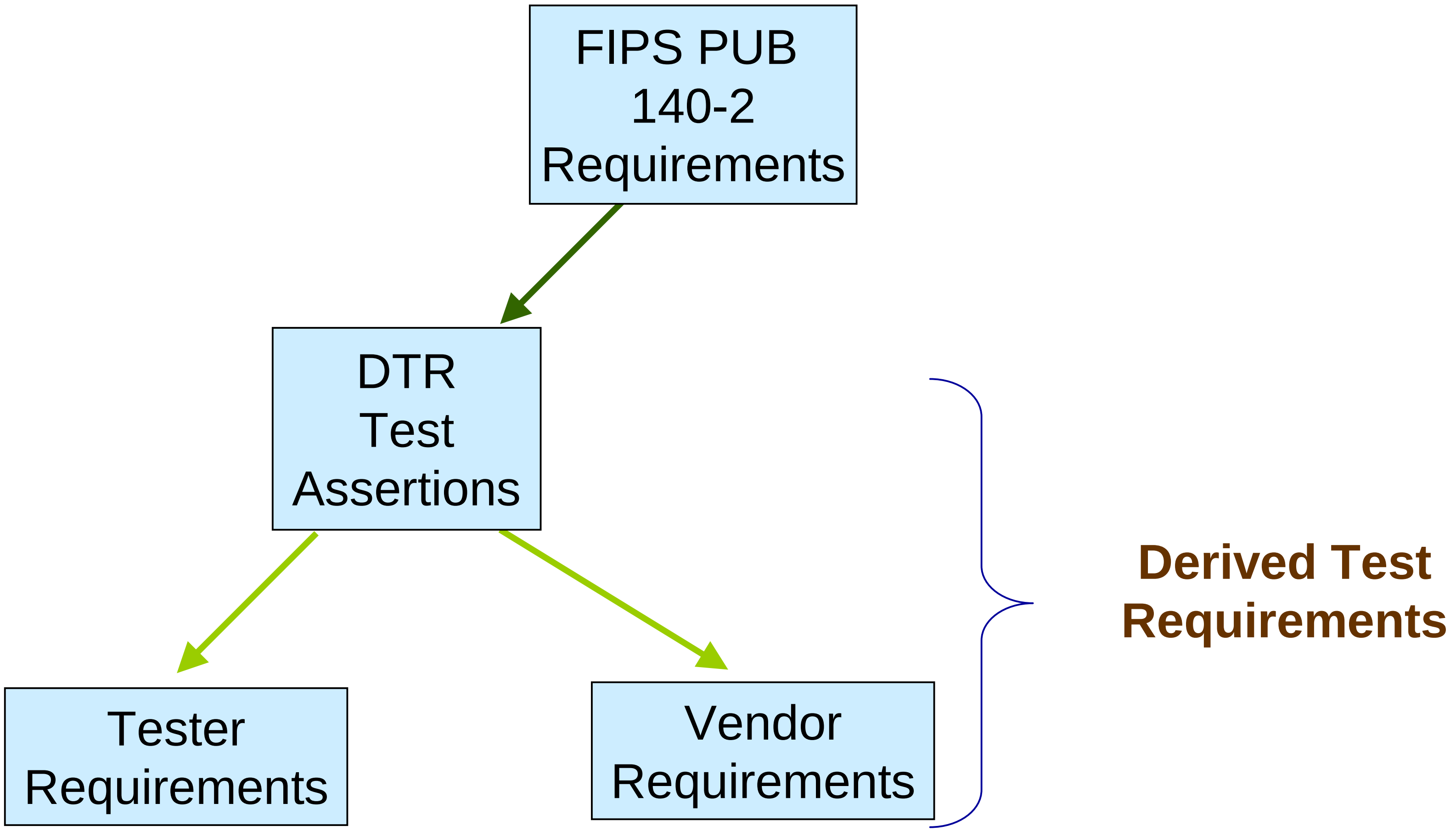
CMVP Testing Process

- Purpose of CMVP
  - Conformance testing of cryptographic modules using the 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 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 Traceability



FIPS PUB 140-2 Requirements

DTR Test Assertions

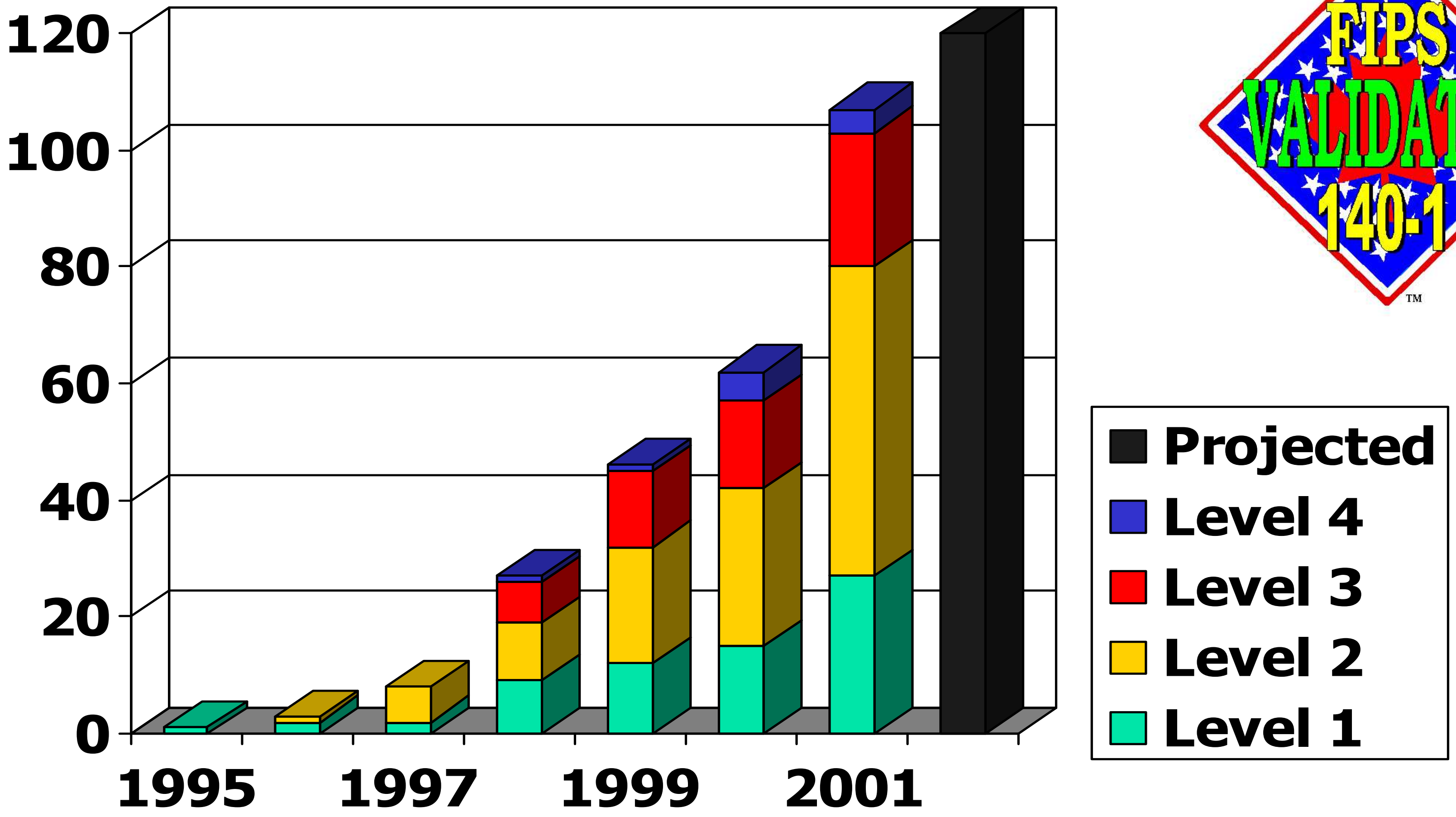
Tester Requirements

Vendor Requirements

Derived Test Requirements

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

(January 15, 2002)

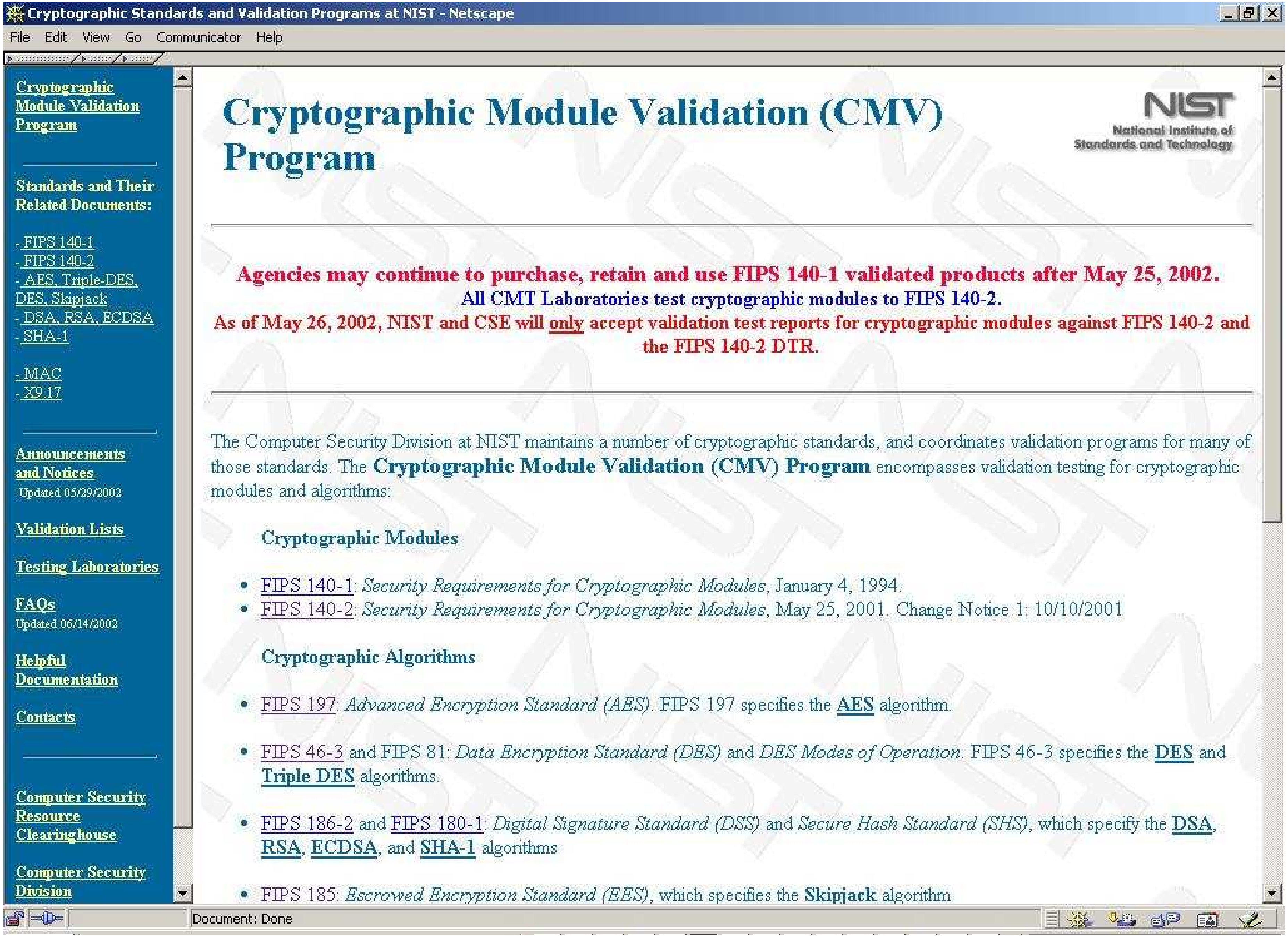


FIPS VALIDATED 140-1 ™

Participating Vendors

(January 15, 2002)

Alcatel
Algorithmic Research, Ltd.
Ascom Hasler Mailing Systems
Attachmate Corp.
Avaya, Inc.
Baltimore Technologies (UK) Ltd.
Blue Ridge Networks
Certicom Corp.
Chrysalis-ITS Inc.
Cisco Systems, Inc.
Cryptek Security Communications, LLC
CTAM, Inc.
Cylink Corporation
Dallas Semiconductor, Inc.
Datakey, Inc.
Ensuredmail, Inc.
Entrust Technologies Limited
Eracom Technologies Group, Eracom Technologies Australia, Pty. Ltd.
F-Secure Corporation
Fortress Technologies
Francotyp-Postalia
GTE Internetworking
IBM
Intel Network Systems, Inc.
IRE, Inc.
Kasten Chase Applied Research
L-3 Communication Systems
Litronic, 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.
Oracle Corporation
Pitney Bowes, Inc.
PrivyLink Pte Ltd
PSI Systems, Inc.
Rainbow Technologies
RedCreek Communications
Research In Motion
RSA Data Security, Inc.
SchlumbergerSema
Spyrus, Inc.
Stamps.com
Technical Communications Corp.
Thales e-Security
TimeStep Corporation
Transcrypt International
Tumbleweed Communications Corp.
V-ONE Corporation, Inc.


Cryptographic Standards and Validation Programs at NIST - Netscape
File Edit View Go Communicator Help
NIST National Institute of Standards and Technology
Document: Done

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

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

Pre-validation Status List

- Pre-validation phases
  - Implementation Under Test (IUT)
    - The crypto module and documentation are resident at the CMT lab
    - The vendor has a viable contract with the CMT lab
  - Validation Review Pending
    - Testing documentation submitted to NIST and CSE
  - Validation Review
    - Comments developed by NIST and CSE
    - Combined comments sent to CMT lab

Pre-validation Status List (concluded)

- Pre-validation phases
  - Validation Coordination (process may be iterative)
    - Testing documents revised
    - Additional documentation (if required)
    - Additional testing performed (if required)
    - Resubmission to NIST and CSE
  - Validation Finalization
    - Final resolution of validation review comments
    - Certificate number assigned
    - Certificate printing and signature process initiated

Random Number Generators

- A Cryptographic Module may employ random number generators (RNGs)
  - Approved RNG Output
    - Generation of cryptographic keys
  - Non-Approved RNG Output
    - Input seed and/or seed key for Approved RNG
    - Generate IV's
- Self-Tests
  - Continuous RNG Test
  - Statistical tests
    - Levels 3 and 4
    - All levels CMT Lab Testing

Approved Random Number Generators (RNGs) FIPS 140-2 Annex C

Deterministic Random Number Generators

1. NIST, Digital Signature Standard (DSS), FIPS Pub 186-2, January 27, 2000 – Appendix 3.1.
2. NIST, Digital Signature Standard (DSS), FIPS Pub 186-2, January 27, 2000 – Appendix 3.2.
3. ABA, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA),* ANSI X9.31-1998 - Appendix A.
4. ABA, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, ANSI X9.62-1998 – Annex A.4.

Nondeterministic Random Number Generators

- There are no FIPS Approved nondeterministic random number generators**.**

RNG Self-Tests – FIPS 140-2

- Power Up Statistical Tests (20k bits)
    - Levels 3 and 4
    - All Levels CMT Lab Testing
  - The monobit test
  - The poker test
  - The runs test
  - The long runs test
- Continuous RNG Test

RNG Tests – Revised

- Statistical Tests
  - CMT Lab Algorithm Testing Suite (CAVS)
    - All Levels
  - No longer required within module (Levels 3 and 4)
- Deterministic Known Answer Test
    - All levels
- Continuous RNG Test

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