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

Ken Lu

CSE CMVP

September 28, 2005

Agenda

- FIPS 140-2: Security Requirements for Cryptographic Modules
- Testing Cryptographic Modules
- Maintaining Validation Status
- Cryptographic Algorithm Validation System (CAVS)

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
- Work in progress on FIPS 140-3

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 – ISO/IEC FDIS 19790

➢ 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.

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)

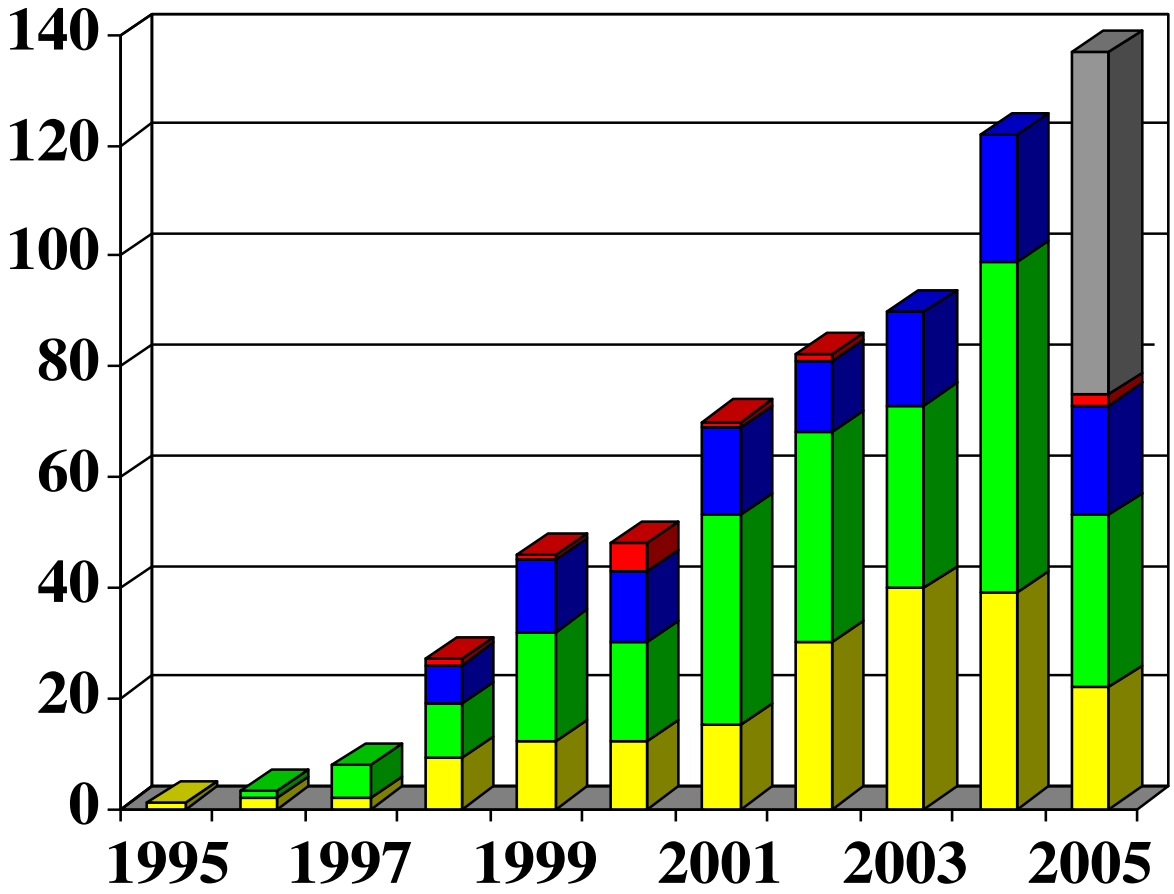
- Cryptographic Modules
  - Experienced
    - 20% security-relevant flaws
    - 100% documentation flaws (primarily the security policy)
  - New to the Process…
    - 50% security-relevant flaws
    - 100% documentation flaws (primarily the security policy)
- Cryptographic Algorithms
  - 30% non-conformant

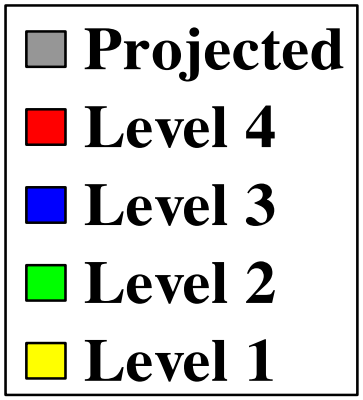
CMVP Status

- Continued record growth in the number of cryptographic modules validated
  - Over 570 Validations representing over 950 modules (573 09/20/2005)
- All four security levels of FIPS 140-2 represented on the Validated Modules List
- Over 150 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

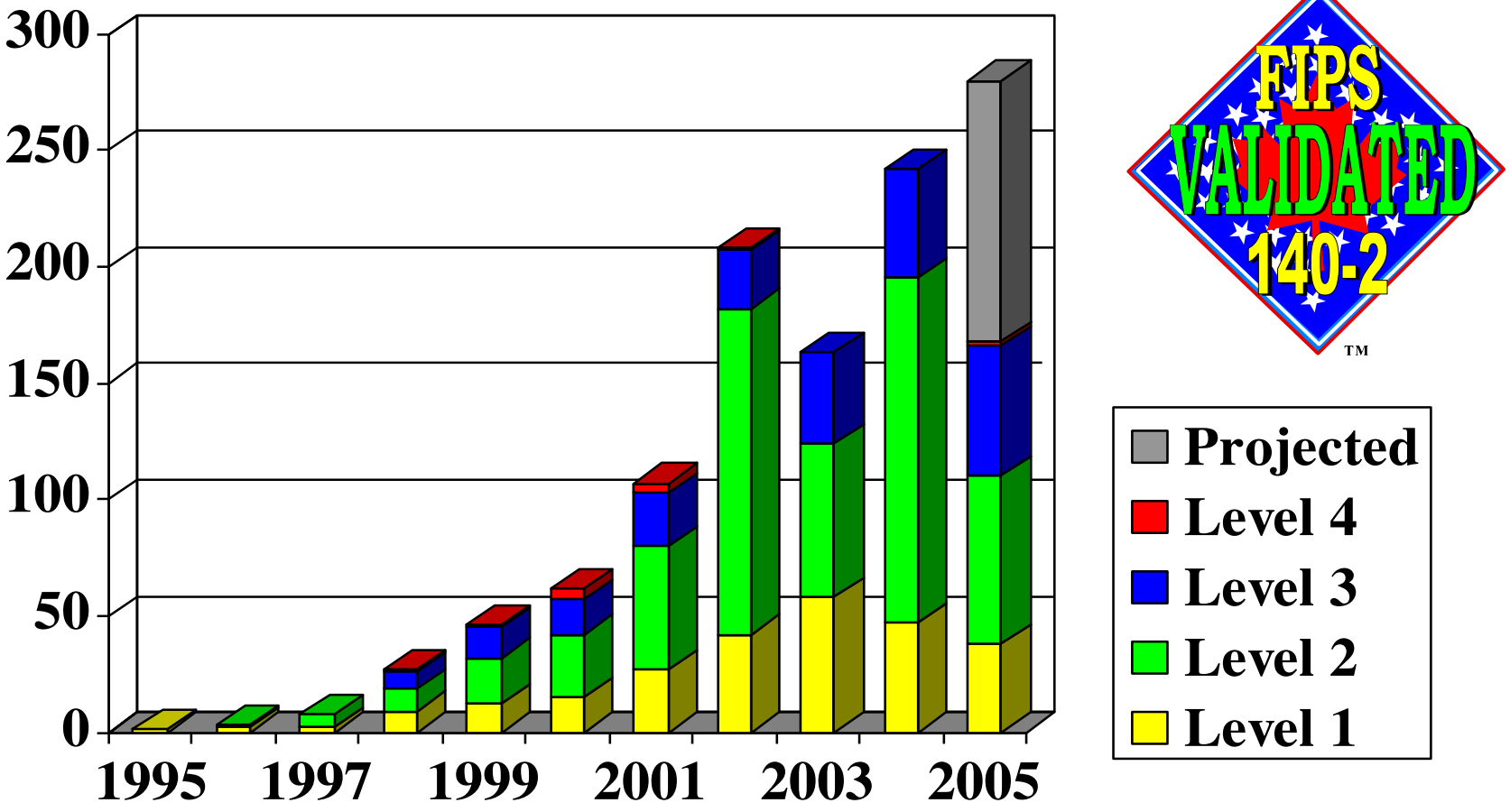
(August 31, 2005)





FIPS 140-1 and FIPS 140-2 Validated Modules by Year and Level

(August 31, 2005)



Participating Vendors

(September 22, 2005 – 150 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
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.
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

(September 22, 2005 – 150 Total)

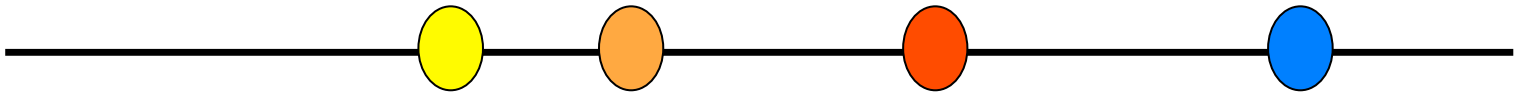
Neopost Ltd.
Neopost Online
Netscape Communications Corp.
NetScreen Technologies, Inc.
Network Security Technology (NST) Co.
Nokia Enterprise Mobility Systems
Nortel Networks
Novell, Inc.
Oberthur Card Systems
Oracle Corporation
Palm Solutions Group
PC Guardian Technologies, Inc.
PGP Corporation
Phaos Technology Corporation
Pitney Bowes, Inc.
Pointsec Mobile Technologies
Prism Payment Technologies (Pty) Ltd
PrivyLink Pte Ltd
PSI Systems, Inc.
Real Time Logic, Inc.
Realia Technolgies S.L.
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

Security Spectrum



Not

- 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

CMVP Testing: Validation Flow

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

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

Cryptographic Algorithm Validation System

- **Prerequisite to FIPS 140-2 Validation**
  - Very complex
  - Uniform validation testing for Approved cryptographic algorithms
  - 25% of algorithm implementations that are ready to go to market are incorrect
  - NIST developed tool provided to CMT Labs – CAVS
  - Generates Test Vectors to run on algorithm implementation
  - Results are verified by CAVS tool
    - Provides thorough testing of the implementation
    - Types of errors found by CAVS range from pointer problems to incorrect behavior of the algorithm implementation

Cryptographic Algorithm Validation System

- Approved Algorithms Tested
  - 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)

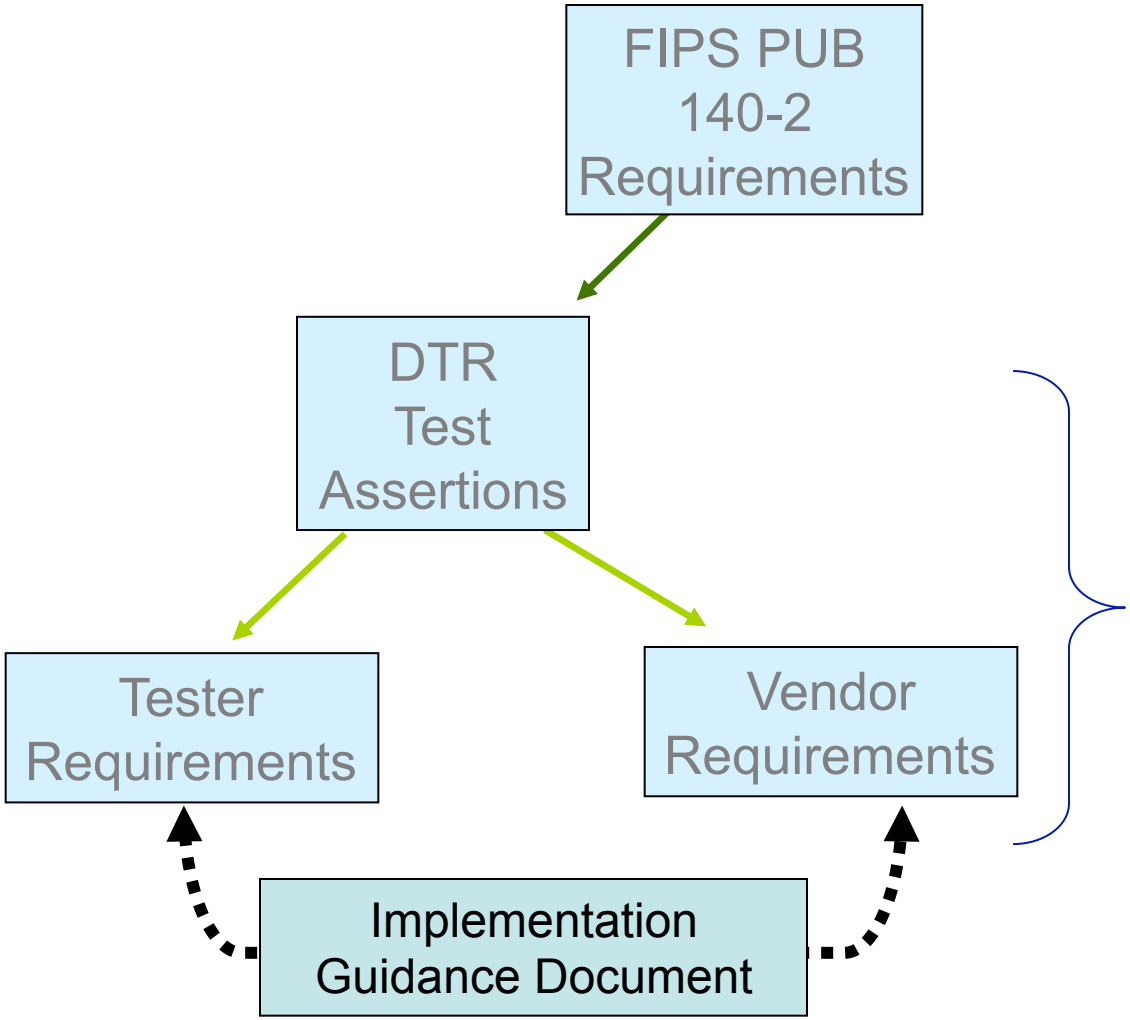
➢ A product or module does not meet the FIPS 140-2 applicability requirements by simply implementing FIPS Approved algorithms and acquiring algorithm validation certificates.

Cryptographic Algorithm Validation System

- Future Algorithm Validation Tests
  - AES and Triple-DES CMAC – NIST SP 800-38B
  - DSA – FIPS 186-3
  - Diffie-Hellman and MQV – NIST SP 800-56
- Future Protocol Validation Testing
  - TLS 1.0 (SSL 3.1)
  - IEEE 802.11i Wireless

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

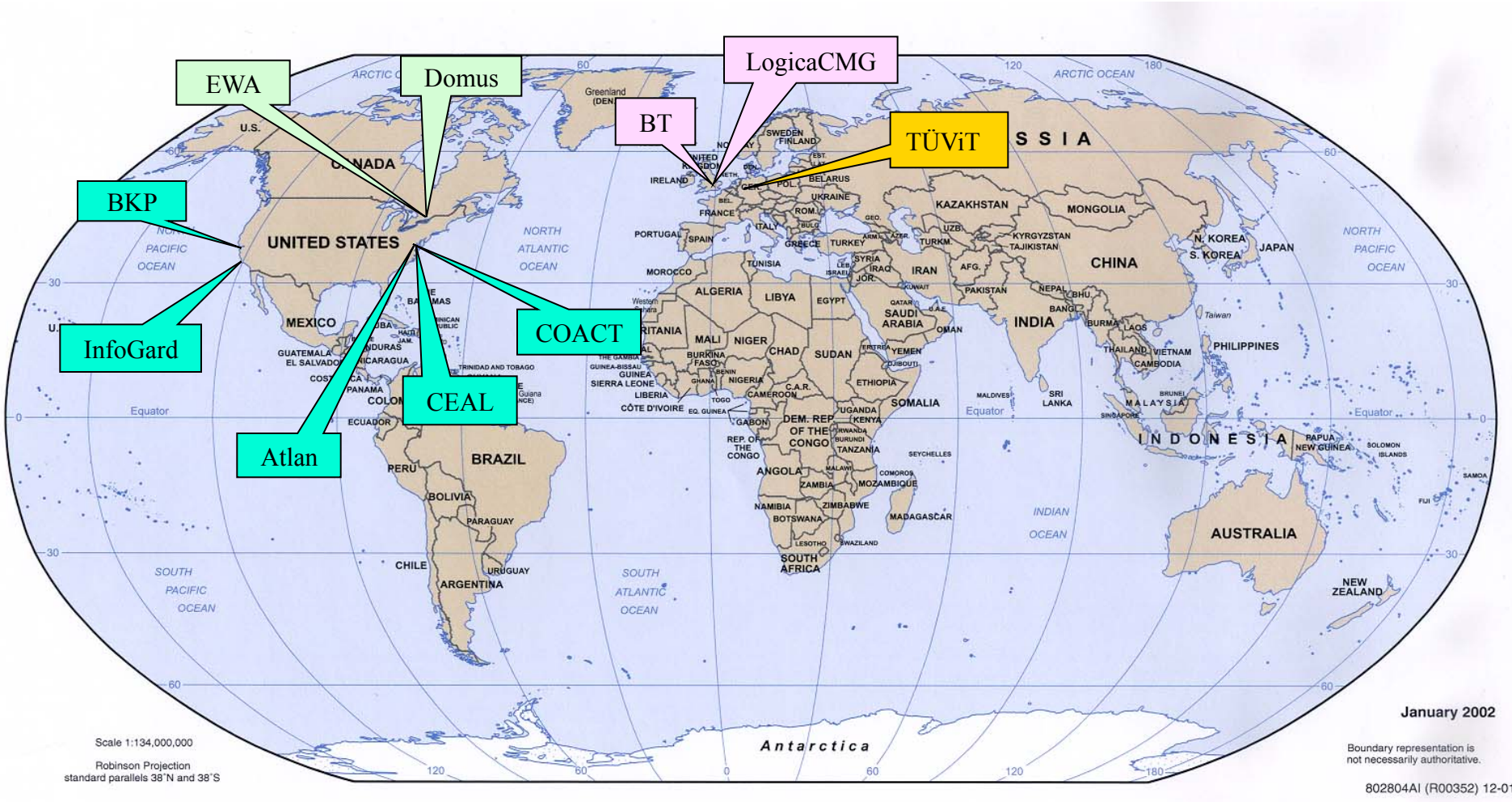


Derived Test Requirements

Cryptographic Module Testing (CMT) Laboratories

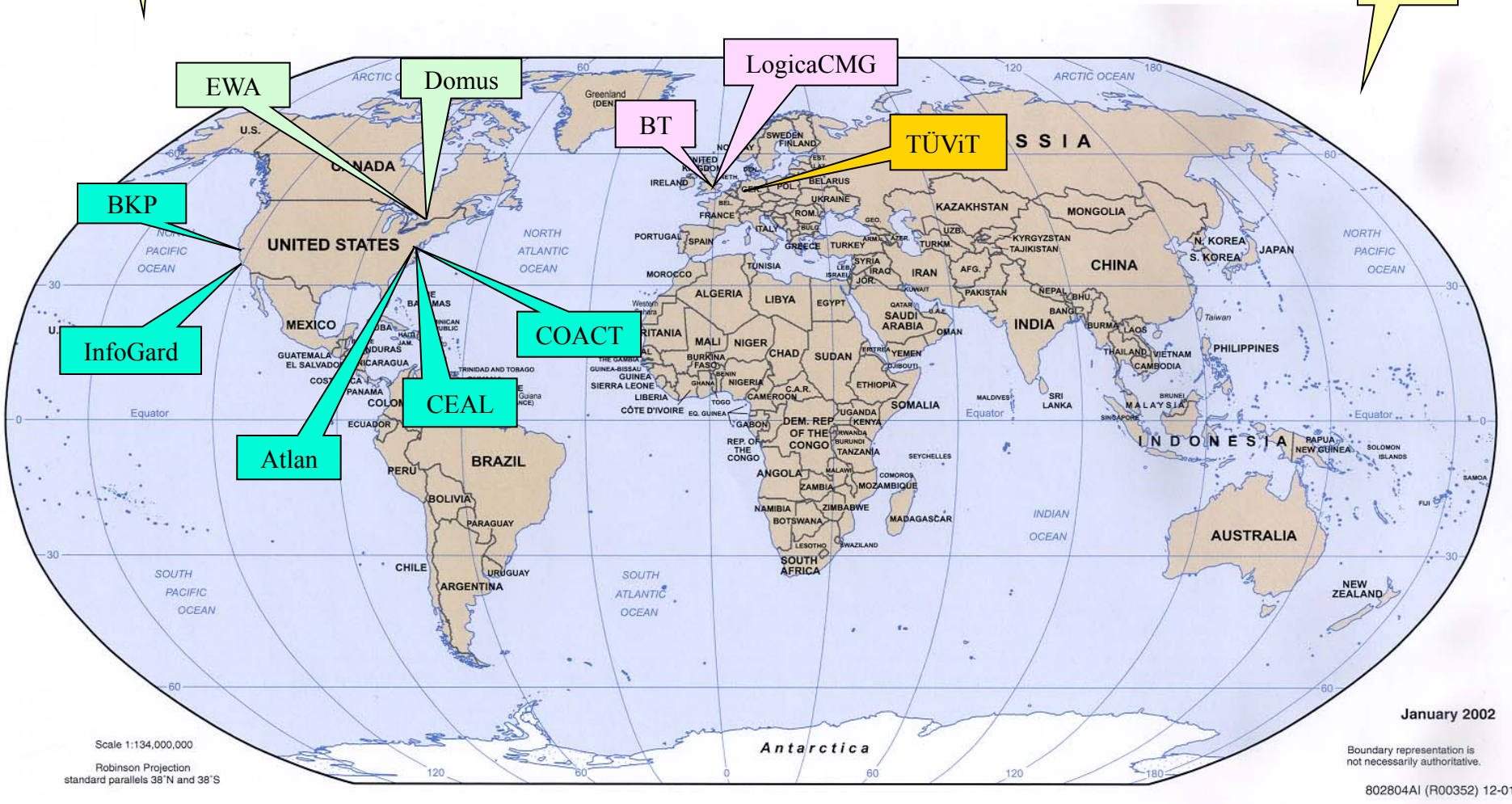
- Ten National Voluntary Laboratory Accreditation Program (NVLAP) - accredited testing laboratories
  - True independent 3rd party accredited testing laboratories
  - Cannot test and provide design assistance

CMT Accredited Laboratories



Seventh CMT laboratory added in 2002
Eighth CMT Laboratory added in 2003
Ninth CMT Laboratory added in 2004
Tenth CMT Laboratory added in 2005

CMT Accredited Laboratories



Seventh CMT laboratory added in 2002
Eighth CMT Laboratory added in 2003
Ninth CMT Laboratory added in 2004
10th, 11th and 12th …. CMT Laboratories added in 2005

Revalidation:

- **Non-Security Relevant**
  - Letter only submission to the CMVP
- **Relevant Changes (<30%)**
  - All changed assertions tested
  - Module regression tests
- **Relevant Changes (>30%)**
  - New module – full testing

Withdrawal of DES

1. Effective May 19, 2005: Federal Agencies may continue to use DES as a NIST recommended Approved security function in a FIPS Approved mode of operation in FIPS 140-1 or FIPS 140-2 validated cryptographic modules for a period of 2 years (until May 19, 2007). This provides a transition period to migrate to AES or Triple-DES.
   - Cryptographic modules validated to FIPS 140-1 or FIPS 140-2 that implement DES as an Approved security function will have the DES algorithm entry on the module validation list changed to include the caveat "transitional phase only – valid until May 19, 2007"
   - The Cryptographic Algorithm Validation Program (CAVP) has discontinued the issuance of new DES algorithm validation certificates as of February 9, 2005 (Note: DES implementations under contract for testing by a CMT Laboratory prior to February 9, 2005 will be completed).
   - Agencies must understand that NIST strongly recommends against any continued use of DES. Agencies must accept the security risks of the continued use of DES during the transition phase. In short, DES does not provide adequate protection for data whose confidentiality must be assured for more than near-transitory implementations.
2. After the 2-year transition period ends on May 19, 2007:
   - The reference to single DES will be removed from FIPS 140-2 Annex A, Approved Security Functions.
   - The CMVP will move all references of DES from an Approved security function to the non-Approved security function line on all FIPS 140-1 and FIPS 140-2 cryptographic module validation certificates. Modules validated to FIPS 140-1 or FIPS 140-2 that only implement DES as an Approved security function will have their entry on the module validation list annotated as not meeting FIPS 140-1 or FIPS 140-2 requirements anymore and can no longer be used by a Federal agency.
   - The DES validation list will be saved for historical reference only but annotated as no longer being Approved for use.
3. This transition also applies to DES MAC.
4. The use of DES in National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 27, 2000 – Appendix 3.2 is not affected.

NIST Special Publication 800-57

- Parts A and B published August 2005
- CMVP reviewing for impacts to module validations Caveat:

RSA (key wrapping, key establishment methodology provides 80 bits of encryption strength);

Table 2: Comparable Strengths

Bits of security	Symmetric key algorithms	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
80	2TDEA	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

FIPS VALIDATED 140-2 ™

- Overnight, Priority, & Express Mail
- Envelopes
- Packages
- Manila Envelopes
- Return Receipt
- Insured Mail
- Delivery Confirmation
- Certified Mail

http://www.nist.gov/cmvp

- FIPS 140-1 and FIPS 140-2
- Algorithm Standards and Testing
- 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
- Message Authentication

Validation Lists

Testing Laboratories

Announcements
Updated 11/04/2004

Notices
Updated 10/07/2004

FAQs
Updated 12/18/2003

Helpful Documentation

Contacts

Computer Security Resource Clearinghouse

NIST

Cryptographic Module Validation Program

CMVP Conformance Through Testing

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.

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 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

NIST

- **Randall J. Easter** – Director, CMVP, NIST
  reaster@nist.gov
- **Sharon Keller** – Director, CAVP, NIST
  skeller@nist.gov

CSE

- **Ken Lu** – Technical Authority, CMVP, CSE
  ken.lu@CSE-CST.GC.CA