CMVP Management Manual

Ghislain Lagacé
Communications Security Establishment

CMVP Symposium 2004

14 September 2004

Presentation Outline

- Purpose of Management Manual
- Scope
- Content
- Cryptographic module tester competency program
- Implementation schedule

Motivation

- Growing number of labs and validations reports
- Lack of quality control in some submissions
- Unstated behavior rules
- Reliance on trust
- International flavor: different labs have different practices

Purpose of Management Manual

- To provide effective guidance for the management of the CMVP and the conduct of activities necessary to ensure that the standards are fully met.

How does the cryptographic module validation program work?

Scope of Management Manual

- Outlines the management activities and specific responsibilities of each group.
- Incorporates general implementation guidance (IG G). Future IGs will only deal with technical issues.
- Does not deal with the actual standard and technical aspects of the standard.

Content of Management Manual

Process…Process…Process

- CMVP management processes
- CMT laboratory processes
- Cryptographic module validation processes
- Standards maintenance processes

CMVP Management Processes

- CMVP contacts at NIST and CSE
- Roles, responsibilities and relationships
- Management of the CMVP
- Confidentiality of information
- Handling of complaints
- Activities and functions of the program
- Policies of the CMVP

CMT Laboratory Processes

- Accreditation of CMT laboratories
- Maintenance of CMT laboratory accreditation
- Confidentiality of proprietary information
- CMVP tester competency program
- Permissible activities

CMVP Processes

- Algorithms and random number generator validation
- FIPS 140-2 validation (see next slide)
- Re-validation
- IG requests to NIST and CSE (RFG)
- Flaw discovery handling process
- CMVP web page update
- Request for implementation waivers
- Usage of FIPS 140-1 and FIPS 140-2 logos

CMVP Processes

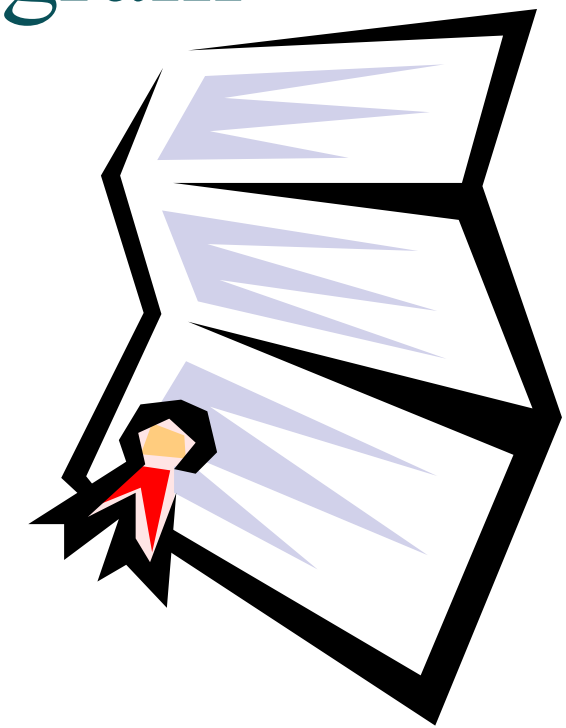
- FIPS 140-2 Validation Processes
  - Process overview
  - Pre-validation list
  - Cryptik tool
  - Certificate preparation
  - Cost recovery

Standards Maintenance Processes

- FIPS 140 publication
- FIPS algorithm publications
- DTR publication
- Implementation guidance (IG)
- Test tools
- CMT laboratory accreditation standards
- CMVP Management Manual

Cryptographic Module Tester Competency Program

- Purpose
- CMVP training packages
- Competency levels
- Examination



CMVP Training Packages

- The CMVP has developed two training packages:
  - CMVP Basic Training Package provides the basic knowledge about FIPS 140-2.
  - CMVP Advanced Training Package provides in-depth knowledge of FIPS 140-2 and the operation of the CMVP.

Competency Levels

- The CMVP tester competency program is comprised of two levels:
  - Competency Level 1 is required for all testers to test cryptographic modules against FIPS140-2.
  - Competency Level 2 is required for the technical authority submitting the test report.

Examination

- After completing a training package, the tester writes a closed-book exam.
- Competency Level 1: Exam is written at the laboratory under the supervision of a laboratory's signatory.
- Competency Level 2: Exam is written under the supervision of the CMVP.
- Exam is corrected by the CMVP.

Implementation Schedule

- Prepare draft document and discuss between CSE and NIST
- Finalize document in 2004
- Circulate for comments
- Active in 2005

Conclusion

- The CMVP family is growing…
- Documenting our processes will ensure that management activities and responsibilities are clearly defined and understood.
- This is a living document; processes will be added as the CMVP continues to grow.