

Cryptographic Module Evaluation Protection Profile (PP) project



Annabelle Lee
Director, CMVP
March 27, 2002



Project Objectives

- Determine if FIPS 140-2 can be successfully expressed in Common Criteria (CC) Protection Profile (PP) format/language
 - includes mapping the FIPS 140-2 Derived Test Requirements (DTR) Document into CC language and structure
- Maintain the intent and effectiveness of FIPS 140-2
- Analyze the impact of the CC methodology on the Cryptographic Module Validation Program (CMVP)



Specific Tasks

- Develop a FIPS 140-2/CC Mapping
- Develop a Cryptographic Module Evaluation PP (CME PP), which will be evaluated to determine its consistency and completeness with FIPS 140-2
- Produce a report documenting and analyzing the issues associated with the CME PP



Status

- Mapping document draft with initial analysis delivered March 2000
- Draft CME PP commensurate with FIPS 140-2 Level 4 delivered October 2000
- Draft CME PPs commensurate with FIPS 140-2 Levels 1-3 terminated



Technical Issues

- Final format for the CME PPs are four separate documents corresponding to the four security levels of FIPS 140-2
- FIPS 140-2 contains a level of detail difficult to express in the CME PP without extensive use of application notes and requirement extensions
- FIPS 140-2 is a **mandatory** standard
- FIPS 140-2 is approximately 50 pages and the CME PPs encompass several hundred pages



Programmatic Issues and Conclusions

- The CC and the CMVP use different testing paradigms
 - CMVP: Conformance/Compliance testing
 - CC: Evaluation
- The CC testing methodology requires substantial oversight by the validation authority, which is not required by the CMVP



Programmatic Issues and Conclusions

- Differences in testing methodologies may severely impact time and cost to vendors
- Project terminated

Specifying Cryptography in a CC PP

Certificate Issuing and Management Components (CIMC) Family of Protection Profiles

- The requirements for **FIPS 140-1 validated cryptographic modules** and specific FIPS 140-1 levels are based on the level of risk and specific threats identified for each CIMC PP. The FIPS 140-1 requirements are intended to provide additional assurance.
- **O.Cryptographic functions** The TOE must implement approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification; approved key generation techniques and use validated cryptographic modules. **(Validated is defined as FIPS 140-1 validated.)**

Specifying Cryptography in a CC PP

Certificate Issuing and Management Components (CIMC) Family of Protection Profiles

- **FDP_ACF_CIMC.2.1** CIMS personnel private keys shall be stored in a FIPS 140-1 validated cryptographic module or stored in encrypted form. If CIMS personnel private keys are stored in encrypted form, **the encryption shall be performed by the FIPS 140-1 validated cryptographic module.**

<http://csrc.nist.gov/pki/secreqmts/welcome.html>

Special Publication 800-23



Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

- 800-23 does **not** mandate the use of tested/evaluated products
- NSTISSP 11 mandates the use of tested/evaluated products to be used on systems entering, processing, storing, displaying, or transmitting **national security information**