X-Sieve: CMU Sieve 2.2
From: Jean.Campbell@CSE-CST.GC.CA
To: draftfips201@nist.gov
Cc: randall.easter@nist.gov, ray.snouffer@nist.gov
Subject: Comments on Draft FIPS PUB 201 and Draft SP 800-73
Date: Thu, 23 Dec 2004 14:03:07 -0500
X-Mailer: Internet Mail Service (5.5.2653.19)
X-MailScanner:
X-MailScanner-From: jean.campbell@cse-cst.gc.ca

Classification: UNCLASSIFIED

Good afternoon,

Attached are comments on the Draft FIPS PUB 201 and Draft Special Publication 800-73.

Do not hesitate to contact the undersigned should you have any questions.

Best regards,

Jean Campbell

<<Comments on SP 800-73.doc>> <<Comments on FIPS PUB 201.doc>>

Jean Campbell
Information Technology Security Engineer
Cryptographic Module Validation Program
Industry Program Group
Communications Security Establishment
Tel: (613) 991-8121
Fax: (613) 991-7149
URL: www.cse-cst.gc.ca
e-mail: Jean.Campbell@cse-cst.gc.ca

 Comments on SP 800-73.doc

 Comments on FIPS PUB 201.doc

Comments on:
NIST Special Publication 800-73
Integrated Circuit Card for Personal Identity Verification
Initial Public Draft (Version 1.0)

Prepared by: Jean Campbell

Cryptographic Module Validation Program
Industry Program Group
Communications Security Establishment
Tel: (613) 991-8121
e-mail: Jean.Campbell@cse.cst.gc.ca

3. Concepts and Constructs

Section 3.4.2 Cryptographic Information Application.

Draft FIPS PUB 201 is very specific about the mandatory use of FIPS 140-2. This Special Publication seems to specify that it must implement cryptography per ISO/IEC 7816-15. Are the two compatible or should this document be amended to require FIPS 140-2?

Comments on:
FIPS PUB 201
Personal Identity Verification (PIV)
for Federal Employees and Contractors
Public Draft (Version 1.0)

Prepared by: Jean Campbell

Cryptographic Module Validation Program
Industry Program Group
Communications Security Establishment
Tel: (613) 991-8121
e-mail: Jean.Campbell@cse.cst.gc.ca

General Comments

While FIPS 140-2 provides assurance for cryptographic functionality, several other IT security features provided by smart cards are not tested or evaluated. It is interesting to see that there are no requirements for evaluation by a Common Criteria scheme.

Work has begun for the revision of FIPS 140-2 and future publishing of FIPS 140-3. FIPS PUB 201 should consider also referring to the upcoming standard.

PART 1: PIV–I

Section 2.2 Identity Proofing and Registration Process

There should a *role* be defined for approved Cardholders. The utilization of the card would completely be described (i.e., from the time the applicant requests the card to the time the card is disposed of).

PART 2: PIV–II

Section 4.1.3 – Physical Characteristics and Durability

The section should clarify the fact that the stated physical requirements are only intended for daily normal usage and are not intended to sustain determined attacks. As indicated in section A.2.1 *Scope of FIPS 201 Validation Testing*, the requirements aimed at alleviating those threats are addressed by requiring that the module meet Security Level 3 for Physical Security under FIPS 140-2.

Section 4.1.6.1 – Activation by Cardholder

FIPS 140-2 levies requirements on the strength of authentication (i.e., the number of possibilities that authentication data can be guessed). These requirements are 1 in a million bit-wise which translates to a PIN of at least 6 numbers. Will FIPS PUB 201 levy similar requirements?

FIPS 140-2 levies requirements on the number of allowed retries. These requirements are1 in 100,000 unsuccessful tries in a one minute period. Will FIPS PUB 201 levy similar requirements?

Section 4.1.6.2 – Activation by Card Management System

The term *update* should be replaced by *PIV Update*. This distinction clearly identifies that they are changes to the information or data contained within the PIV as described in section 5.2.4.3 *PIV Update* instead of changes to the loaded software as described in section A.2.4 *Validation Maintenance*.

Table 4-1 Card Management Algorithm and Key Size Requirements. Asymmetric cryptography provides greater authentication assurance than symmetric cryptography does. Why is RSA, DSA or ECDSA not an option, even if not possibly supported by [GP] Global Platform, Open Platform Card Specification, Version 2.0.1?

Section 4.2.2 – Asymmetric Signature Field in CHUID

Table 4-4: Algorithm and Key Size Requirements. The footnote n° 5 found on page 44 should also be included with this table. It clarifies the reason why such a limited number of cryptographic algorithms are allowed. Consideration should be given to include DSA and SHA-[redacted]. The RSA implementation type (e.g. PKCS#1) should be specified. RSA specifies several key size increments between 1024 and 2048. Are there some specified?

Section 4.3 – Cryptographic Specifications

The section should specify, early in the text, cryptographic module should be validated to FIPS 140-2.

In the second paragraph, is the importation of private certificates allowed? Several sections allude to that possibility.

The third paragraph offers the possibility of performing off-card hashing. This allowance is redundant since, to be validated to FIPS 140-2 and be able to perform digital signatures, the hash function needs to be present within the card. In the e.g. of the fifth paragraph, why is digital signature verification considered as a function that does not use cryptographic keys?

Table 4-5: PIV Key Types. This table does not seem consistent with Table 4-4 and footnote n° 5 found on page 44. There seems to be a different list of cryptographic algorithms.

In the last bullet of page 29, last sentence, what is Section **xx** ("Activation by Card Management System")?

ANNEX A: PIV VALIDATION, CERTIFICATION, AND ACCREDITATION

Section A1 – FIPS 140-2 Testing and Validation

In the first paragraph, the first sentence should read: "*All of the cryptographic modules in the PIV system (both on-card and issuer software) shall be **validated to FIPS 140-2 with an Overall Security Level 2 or higher***". In the second last sentence, the end should read: "... *and **the** Communications Security Establishment (CSE) of **the Government of** Canada.*"

Section A.2.1 – Scope of FIPS 201 Validation Testing

In the third paragraph, the second last and last sentences should read: "*At a minimum, the cryptographic module used in a PIV component (on-card or in the issuer software) shall be **validated to FIPS 140-2 with an Overall Security Level 2**. In addition, PIV cards shall be validated at **Security** Level 3 for Physical Security and **Roles, Services and Authentication sections**.*"

While only on-card or in the issuer software are considered by this standard, is there any consideration given to the software authenticating the users of the PIV?

Section A.2.4 Validation Maintenance

FIPS 140-2 does not allow, while operating in a FIPS mode of operation, that the cryptographic module to load untrusted or un-validated code (i.e., un-validated to FIPS 140-2). Any new application intended to be loaded into a cryptographic module or the whole cryptographic module with the new application loaded will need to be validated.

ANNEX F: REFERENCES

The following references are missing:

[CMS]

[FIPS 140-2]