X-Sieve: CMU Sieve 2.2
X-Mailer: Openwave WebEngine, version 2.8.12 (webedge20-101-197-20030912)
From: John Hannan <jhannan@verizon.net>
To: <DraftFips201@nist.gov>
CC: <rschweickhardt@gpo.gov>, <jhannan@gpo.gov>
Subject: Comments on Public Draft FIPS 201
Date: Fri, 24 Dec 2004 16:10:01 -0500
X-Authentication-Info: Submitted using SMTP AUTH at out011.verizon.net from [192.168.1.3] at Fri, 24 Dec 2004 15:10:02 -0600
X-MailScanner:
X-MailScanner-From: jhannan@verizon.net

Attached are comments submitted by the U.S. Government Printing Office (GPO) on the public Draft FIPS 201.

If there are any questions on the attachment, please contact me at 202-512-1021 or by email at jhannan@gpo.gov.

Thank you.

Sincerely,

John Hannan
Director, IT Security Division
U.S. Government Printing Office
202-512-1021 (office)


Comments_on_Draft_FIPS_201.doc

Comments on Public Draft FIPS 201

Submitted by: U.S. Government Printing Office (GPO)
Contact: John Hannan, 202-512-1021

December 23, 2004

1. Consideration should be given in FIPS 201 to allow for a common operating system, based on the biometric passport operating system, to be used for the contactless portion of the PIV card. This is recommended since the operating system for the biometric passport has and will continue to receive high levels of assurance analysis from the US government, and since a common software baseline for the contactless chip will tend to reduce costs to manufacture and procure cards compliant with FIPS 201 as a result.
2. Consideration for more detailed technical specifications for the contactless interface for the PIV cards per ISO 14443 should be considered to ensure interoperability is achieved.
3. "Anti-skimming" protection for the contactless interface of the PIV card via technical controls should be specified in FIPS 201 to mitigate potential privacy concerns. That is, technical controls should be specified which require the contactless chip in the PIV card to positively authenticate any reader device as a trusted reader before transmitting any information, especially personal identifying information about the cardholder.
4. Strong encryption, using Triple DES as a minimum acceptable standard or using AES-128, should be required for all contactless transmission of information between PIV cards and PIV compliant reader devices, to ensure that any personal identifying information cannot be read to mitigate the risks against potential interception of the wireless communication.
5. For section 2.2.3, are these same procedures required if a federal employee with a valid PIV card from another federal agency, who has current background investigation information up to date, transfers to an agency at the same position sensitivity level (or lower level sensitivity)? That is, must the background investigation required for the employee and employee's position be repeated before a long term agency credential could be issued to that transferring federal employee?
6. For section 2.2.3, is any provision contemplated to permit new employees to obtain a credential which is stronger than a visitor credential during the period in which the NACI investigation is underway?
7. Why are PIN pads required for all physical access readers? (See section 4.5.3). It is stated in section 3.3.1 that PIN pad devices would be envisioned to be used at secure locations where a higher level of authentication assurance of the cardholder is required. Thus, it seems inefficient (more costly) to require all physical access readers to have PIN pads. In addition, the standard is inconsistent as a result.

8. Section 4.1.6 implies that all PIV cards will implement PIN activation. Does this mean that for authentication of a PIV card holder at a physical access proximity reader that if biometric authentication is not used, that PIN authentication is required? Please clarify this. If so, this requirement will significantly increase the time required for personnel to enter the building at the main entrances over current methods, and may require changes in space or employee/cardholder expectations concerning entry time.
9. The reference in the third paragraph of Section 4.3 ("The PIV card may include additional asymmetric…") to optional functions such as key pair generation and trust anchor storage is confusing, since paragraph 2 of section 4.3 requires that RSA key pair generation be implemented. Key pair generation on the card should not be optional. Recommend that this standard require that PIV cards be required to perform key pair generation on card, and that paragraph 2 of section 4.3 be updated to include that requirement for clarity. The same comment applies to trust anchor (root CA) storage.
10. Section 4.3, 5th paragraph, page 27, what level of validated software cryptographic module is referred to? FIPS 140-2 Level 1? Recommend that this be specified.
11. Section 2.2.2 implies that when re-issuing credentials to current employees, another set of fingerprints will be taken? Is this intended as a requirement?
12. A minimum PIN length is not specified. Recommend that this be specified.
13. Section 5.2.1.1, this section states that the Registration Authority may optionally photograph the applicant. It would seem this would have to mandatory if a facial image is required as biometric data for the applicant. Recommend that this be changed to mandatory, or modify tasks of the PIV Issuing Authority to photograph the applicant.
14. It is stated that specifications regarding information exchange between agencies concerning PIV system components is outside the scope of this standard. That implies that such communications between agency PIV systems is not required, and communication protocols and technical security requirements (strong authentication between systems, along with confidentiality, integrity and availability controls) will be specified at a later date if such requirements arise. Is that the correct interpretation of the current state of HSPD-12, PIV and FIPS 201 for inter-agency PIV system electronic communications for access control?