X-Sieve: CMU Sieve 2.2
Date: Thu, 23 Dec 2004 08:19:05 -0500
From: APRIL GILES <agiles1@jhu.edu>
Subject: FIPS 201 Comments
To: DraftFips201@nist.gov
Reply-to: agiles1@jhu.edu
X-Mailer: Sun Java(tm) System Messenger Express 6.1 HotFix 0.05 (built Oct 21 2004)
X-Accept-Language: en
Priority: normal
X-MailScanner:
X-MailScanner-From: agiles1@jhu.edu

Please accept my personal comments on FIPS201.

Thanks
April Giles

FIPS201 Comments r1.doc

Memorandum

To: NIST Draft FIPS201 Comments Group

CC: David Temoshok

From: April Giles

Date: 12/23/2004

Re: Comments on Draft FIPS 201 Standard

Greetings,

Great job, especially considering the accelerated completion requirements! Here are my comments on the FIPS 201 standard for review. Please contact me with any questions at 202-501-1123 or email april.giles@gsa.gov.

Ref#	FIPS 201 Section	Reference Text	Page / Para #	Comments
1	1.3 Document Organization	*The first part……………but does not address the interoperability of PIV Cards and systems among agencies.*	2/2	One could surmise that implementing PIV-I requirements without factoring in requirements of PIV-II apriori, may cause additional unnecessary costs due to potential incompatibilities with the PIV Front End system and PIV II requirements. Realizing that one of the desired outcomes of breaking up the PIV requirements into 2 parts is to reduce the agency's anxiety level concerning expedited compliance dates, is it possible that we are sacrificing aggregate system cost and PIV-II implementation schedule? Maybe consider adding a statement that would suggest agencies consider PIV-II requirements when acquiring PIV front end system components.
2	2.1 Control Objectives	*Issue credentials…….whose reliability has been established by the agency…….in writing;*	4/2	The term "reliability" may be too indefinite. Indefinite terms tend not to support compliance testing efforts. Suggest adding specific criteria linking "reliability" with 800-37 C&A.
3	2.2.1 Identity Proofing and Registration of New Employees and Contractors	*An Applicant…vetting process for Federal Employment.*	5/2	The term "applicant" could imply a much larger group than originally intended. As one could include persons who have not been officially selected for employment within the agency. Suggest replacing "applicant" with "agency selected candidate" throughout standard.

Ref#	FIPS 201 Section	Reference Text	Page / Para #	Comments
4	2.2.1 Identity Proofing and Registration of New Employees and Contractors	*The Applicant……Section 4.4.3*	6/1-2	It is unclear what criteria the Registration Authority (RA) should use to visually authenticate applicant submitted documentation. One could postulate that it is improbable that a typical RA would be capable of detecting forged documentation by visual scrutiny alone, without the benefit of input from source indicated on forged document. Conducting background checks on retrieved identity source documentation only confirms that said identity exists, and applicant/agency selected candidate has knowledge of said identity. How will the RA confirm that the submitted identity is bound to the individual presenting the identity source documentation? Perhaps, verification of the binding between the **individual** submitting identity source documentation and submitted identity source documentation is the single most important purpose of HSPD 12. Suggest disassociating background checks with identity verification, and focusing on means which provide out of band verification of identity binding (i.e. verification of submitted identity documentation validity, and/or incorporating attestations of identity binding with dissimilar sources).
5	2.2.1 Identity Proofing and Registration of New Employees and Contractors	*Based on…..form listed Table 2-1.*	5/3	It is unclear which entity determines position sensitivity level. In the informative section 1.2 (paragraph 1), position sensitivity level is determined by issuing Agency. But in the appendix, position sensitivity level is determined by OPM. Perhaps adding "OPM specified" or "Agency specified" before "position sensitivity level" (as well as removing conflicting references) would help readers to understand the origin of said levels as they are initially introduced in the standard. As stated in section 1.2 "*Therefore, the scope of this standard is limited to authentication of an individual's identity. Access authorization decisions are outside the scope of this standard*", the basis of the standard is to provide identity authentication. As identity authentication is purely a binary state (user binding to an identity is either validated or not validated), how is it possible for multiple levels of authentication/sensitivity to coexist? Could

Ref#	FIPS 201 Section	Reference Text	Page / Para #	Comments
				one surmise that incorporating levels of authentication/sensitivity within FIPS201 facilitates access authorization? If so, isn't that out of the intended scope of FIPS201, and HSPD 12 section (3)? Suggest removing position sensitivity levels and replacing with specific guidelines that define requirements for authentication unilaterally across all agencies.
6	2.2.3 Access Pending Identity Proofing	*Until.... Shall not be issued long-term identity credentials....procedures.*	7/2	May want to consider including within this section a requirement for agency security personnel to require presentation of identification documentation prior to issuance of temporary credentials, as well as a time limit for re-issuance of temporary credentials (i.e. every 24 hours).
7	3.2.1 Agency Responsibilities	*Maintaining records of registration and PIV card status information*	11/2	How long should the agency maintain records of registration? Suggest adding a requirement defining minimum record holding period to section 2 of the standard.
8	3.2.1 Agency Responsibilities	*New bullet*	11/2	Suggest adding: • Establishing lost PIV card procedures to end of section 3.2.1
9	4.1.3 Physical Characteristics and Durability	*The card stock shall withstand the effects of high temperatures…………*	18/8	The phrase "*high temperatures*" is not definite. Indefinite terms tend not to support successful compliance testing efforts. Suggest precisely defining range of acceptable temperature.
10	4.1.5 Logical Credentials	*One asymmetric key pair and corresponding certificate associated with the cardholder.*	23	Suggest adding "authentication" before " *key pair*" thereby emphasizing key application.
11	4.1.5.2 File Structure	*Entire section*	24	Perhaps use of the term "file" should be more closely scrutinized (throughout standard) as it may imply preference of a particular smart card technology.
12	4.4 Biometric Specifications	• *An electronic facial image to be stored on the card for alternate identity verification process.*	30	It is well known in the biometric industry that facial biometrics systems are: costly to operate/maintain, offer no compensation for face changes, lack technology reliability, and require unreasonable limitations on operating environment. One could surmise that this technology is currently impractical. Also, additional storage space (~16K) required would reduce an Agency's ability to implement additional customizations, and virtually nixing attempts to futureproof Smart Card systems. Suggest removing the requirement for facial images to be installed on the PIV card, and replacing it with a hand biometric template (much smaller footprint (9bytes), easier to maintain, and less costly than facial

Ref#	FIPS 201 Section	Reference Text	Page / Para #	Comments
				biometric systems)
13	4.4.4 Fingerprint Requirements for Identity Verification	*These images shall be processed and compared to the images on the card and a subsequent threshold-based decision apparatus will render a verification decision.*	34/2	It may be a good idea to specify minimum threshold range required for a successful authentication. A biometric system can be rendered ineffective (high FAR) if the threshold is set too low, or frustrating (high FRR) if threshold set too high.
14	5.1.2 PKI Respository and OSCP Responders	*CAs that.....build a path to the FBCA.*	40/4	Perhaps X.500 and DAP protocol could be included here as well.
15	5.2.1 PIV Application and Approval	*The Registration Authority may optionally also photograph the Applicant for personalization of the ID card.*	41/4	Perhaps requiring the RA to photograph Applicant/agency approved candidate could prove to be helpful identifying imposter Applicant/agency approved candidates at issuance of PIV card.
16	5.2.1 PIV Application and Approval	*After successful completion of the appropriate background check.....*	42/1	The phrase "*successful completion*" is not definite. Indefinite terms tend not to support successful compliance testing efforts. Suggest precisely defining criterion indicative of a "successful completion of the appropriate background check".
17	5.2.1 PIV Application and Approval	*The Registration Authority shall be required to maintain....*	42/1	How long should the agency maintain records of registration? Suggest adding a requirement defining minimum record holding period.
18	5.2.3. Key Management	*PIV Cards consistent with this specification may have one,two, or three asymmetric private keys.*	43/4	Perhaps consider editing to: PIV Cards consistent with this specification may have at least one, but potentially three asymmetric private keys.
19	5.2.4 PIV Card Maintenance	*OCSP responders shall be updated so that queries with respect to certificates on the PIV card are answered appropriately.*	47/2	How often should the OCSP responders be updated? Suggest adding a specific timeframe here. The phrase "*answered appropriately* " is not definite. Indefinite terms tend not to support successful compliance testing efforts. Suggest precisely defining "*answered appropriately*".

If there are any questions, please do not hesitate contacting me at 202-501-1123 or april.giles@GSA.gov.

Thanks

April Giles