X-Sieve: CMU Sieve 2.2
Date: Thu, 23 Dec 2004 14:23:52 -0500
From: Debb Blanchard <dblanchard@enspier.com>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.4) Gecko/20030624 Netscape/7.1 (ax)
X-Accept-Language: en-us, en
To: DraftFips201@nist.gov
CC: Russ Weiser <rweiser@betrusted.com>,
Judith Spencer <judith.spencer@gsa.gov>
Subject: Comments on Public Draft FIPS 201
X-AntiAbuse: This header was added to track abuse, please include it with any abuse report
X-AntiAbuse: Primary Hostname - zeta.sitelutions.com
X-AntiAbuse: Original Domain - nist.gov
X-AntiAbuse: Originator/Caller UID/GID - [47 12] / [47 12]
X-AntiAbuse: Sender Address Domain - enspier.com
X-Source:
X-Source-Args:
X-Source-Dir:
X-MailScanner:
X-MailScanner-From: dblanchard@enspier.com

To Whom It May Concern:

Attached are the comments from the I-CIDM Bridge-to-Bridge Working Group (BBWG) with respect to the proposed FIPS 201.

Regards,
Deborah Blanchard
Chairperson, I-CIDM BBWG
office: 410-871-0836


CommentTemplate-2004-12-21-BBWG.xls

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
1	BBWG	Deborah Blanchard	T	2.2, Page 4, last sentence	What are the minimum requirements and position sensitivity for people required to perform these roles, e.g., education, level of experience, etc.?	
2	BBWG	Deborah Blanchard	T	2.2.1, Page 5, 2nd para., sentence 4	"...and photocopies of identity source documents.." - some states in which Regional and Field offices are located have deemed it illegal to make photocopies of a state-issued picture ID. What is the legality of the standard to require this with respect to state laws?	
3	BBWG	Deborah Blanchard	T	2.2.1, Page 5, 2nd bullet	What are the requirements for the identified roles (Authorizing Official, Registration Authority, Issuing Authority) to "...maintain information...", e.g., date of birth, about the Applicant in a secure fashion IAW privacy concerns? See also comment #5	
4	BBWG	Deborah Blanchard	T	2.2.1, Page 6, Table 2-2	Given the time frame to obtain a NACIC, is it the goal of the standard to have people who need this, obtain a lower level position while waiting for the NACIC? a. The requirement to wait for completion of the background check applicable to the position sensitivity level before the PIV is issued is not feasible as applied to logical access. A minimum acceptable background investigation should be established and allowed for issuance of the PIV, at least for an interim period until the background investigation required for the particular position sensitivity level is complete. b. Preferably, the standard should not be repeating or establishing the background investigations required for each position sensitivity level at all. The standard should only set the minimum investigation required for issuance of ALL PIV cards c. If the standard must state background investigation requirements for each position sensitivity level, the background investigation requirements should be stated as a minimums rather than as absolute requirements.	
5	BBWG	Deborah Blanchard	T	2.2.1, Page 6, Table 2-1, Table 2-2	If the standard must state background investigation requirements for each position sensitivity level, (2-1) the necessary background investigation form is dependant on the type of investigation, not the position sensitivity level as indicated in the table; (2-2) the background investigation specified for each position sensitivity level should be expressed as a minimum rather than an absolute.	
6	BBWG	Deborah Blanchard	T	2.2.1, Page 7, bullet list (all items)	At what level and how should the Registration Authority maintain this information? Refer to #3	"The Registration Authority shall be responsible to maintain the following in a secure manner in accordance with privacy requirements as noted <law?> and in section <???> of this standard:..."

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
7	BBWG	Deborah Blanchard	T	2.2.2, Page 7,	What is the time frame allocated to a "most recent previous check"? What is the maximum time frame between background checks?	Suggest that the timeframe be mentioned for background checks.
8	BBWG	Deborah Blanchard	T	2.2.3, Page 7	Refer to comment #4, if a person is slotted for a NACIC, is that person to be treated according to visitor procedures or shall that person be afforded a lesser position while the NACIC is being completed? a. The requirement to wait for completion of the background check applicable to the position sensitivity level before the PIV is issued is not feasible as applied to logical access. A minimum acceptable background investigation should be established and allowed for issuance of the PIV, at least for an interim period until the background investigation required for the particular position sensitivity level is complete. b. Preferably, the standard should not be repeating or establishing the background investigations required for each position sensitivity level at all. The standard should only set the minimum investigation required for issuance of ALL PIV cards c. If the standard must state background investigation requirements for each position sensitivity level, the background investigation requirements should be stated as a minimums rather than as absolute requirements.	
9	BBWG	Deborah Blanchard	T	2.3, Page 7	At what level, e.g.m, sensitive, classified, etc., and how should the Issuing Authority maintain this information?	
10	BBWG	Deborah Blanchard	T	4.1.3, Page 18	The card topology should allow for the card to be punched at the top left (front)/top right (back). The barcode generally does not need to run from edge to edge and should be oriented to the bottom of the card. The photo on the front can be adjusted accordingly.	
11	BBWG	Deborah Blanchard	T	4.1.4.1.a, Page 19	WRT changing physical characteristics, e.g., facial hair, hair color, eyeglasses vs contact lenses/lasik, etc, is there a requirement to change the photograph with each change of physical representation?	
12	BBWG	Deborah Blanchard	T	5.2.3.1, Page 43, 2nd sentence	To what does "these Cas" refer in this sentence?	
13	BBWG	Deborah Blanchard	T	5.2.3.6, Page 46	Does this mean that all Cas operated and supported by an agency and that have cross-certified with the FBCA must now be signed by the root of the Common Policy CA?	
14	BBWG	Deborah Blanchard	T	5.2.3.6, Page 46	WRT the agency that is operating their own CA that has cross-certified with the FBCA - is the agency now required to meet all the requirements of the Common Policy?	

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
15	BBWG	Deborah Blanchard	T	5.2.4.1, Page 46, last sentence	A role should perform this verificaiton	"The Requesting Official and Registration Authority shall verify that the employee remains in good standing and personnel records are current prior to renewing the card and associated credentials."
16	BBWG	Deborah Blanchard	T	5.2.4.2, Page 46, 1st paragraph, 2nd sentence	A role should perform this verificaiton	"The Requesting Official and Registration Authority shall verify that the employee remains in good standing and personnel records are current prior to renewing the card and associated credentials."
17	BBWG	Deborah Blanchard	E	5.2.4.2, Page 47, 1st sentence, 1st statement	should be a bullet and incorporated as part of the bulleted list	"...must be in place to ensure that: * The PIV card itself is revoked.... * The PIV Certificate Issuer....."
18	BBWG	Deborah Blanchard	E	6.1, Page 49, 2nd Paragraph, last sentence	run on sentence; should be divided into 2 sentences	"For privacy reasons, contactless use of PINs and biometrics is not supported.. PINs and biometrics may be used with the PIV card using contact readers."
19	BBWG	Russel Weiser	G		The number of Roles as speified are overly burdensome to agencies.	consolidate Roles.
20	BBWG	Russel Weiser	E	section 2.2 page 4 and 5	Great care should be taken in the terminology of roles as the roles of PIV 201 and a Issuing CA are overloaded and can cause confusion of roles.	Possibly add a glossary and or prepend information to differentiate the roles.
21	BBWG	Russel Weiser	T	section 2.2.1	What are the security and document storage requirements for handling and storing Identity Proofing, Registration and Background check information. Is it electronic? And how is it protected. Who has access? How is it updated? This should be explicitly stated.	
22	BBWG	Russel Weiser	T	Section 3.2.2	The applicant should also be responsible for notifying or updating information such as Name changes or other personal information in a time fashion.	
23	BBWG	Russel Weiser	T	Section 4.1.3.1	Clarify the meaning of OVDs	
24	BBWG	Russel Weiser	E	Section 4.1.4	All text subsections of the topography should clearly state Manadtory or Optional for each Zone of the topography just for clarity (note the figure text is harder to read then the verbage)	
25	BBWG	Russel Weiser	T	Section 4.1.4.1.e	Should add a note that the certificates on a card should not expire after the card expiration date. Just for clarity	
26	BBWG	Russel Weiser	G	Section 4.1.4	I see no use in allowing multiple topologies. Select one and stick with it.	
27	BBWG	Russel Weiser	T	Section 4.2	Is the CHUID updateable (so that the position Sensitivity maybe changed)? This would require the card management system to update a card.	

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
28	BBWG	Russel Weiser	T	Section 4.2	The PIV CHUID is suppose to be digitally signed and no where does this document specify that issuance of a signing certificate for this purpose. This mechanism of signing data should detail the certificate(s) and the Subject DN naming of certificates used for this purpose. It should only be used for this pourpose and how is it protected?	
29	BBWG	Russel Weiser	T	Section 4.2.2	States that the signature of the on CHUID shall be generated by the Issuing Authority using the Issuing Authority's PKI Private Key. This is impractical to have a CA directly sign data elements on a card.	Have the CA issue a Signing certificate for this purpose. This certificate would have specific use for signing data elements such as the CHUID and the Biometric information on the card. I would think a specific policy OID might be designated for this certificate type in the common policy.
30	BBWG	Russel Weiser	G		Migration of agencies which already have smart card issuance system to the PIV standard should coincide with the Keysize migration to 2048 keys, This would reduce the expense of having to replace cards prematurely. And save additional expense to the Government.	
31	BBWG	Russel Weiser	E	Section 4.3	The mention of the" Local authentication" key should be explicitly mentioned in Section 4.1.5 in the third bullet of the option credentials on the card for clarity	
32	BBWG	Russel Weiser	T	Section 4.4.1	Same issue as in 11 and 12 above.	
33	BBWG	Russel Weiser	T	Section 5.2.3.2.1	The first Bullet indicates that the SIA,AIA and CDP extensions are optional for this specification while the Federal Common Policy does not make them Optional. This seems to be a conflict which may cause interoperability issues.	Reconcile this with the Common CP
34	BBWG	Russel Weiser	T	Section 5.2.3.2.1	Second Bullet. The OCSP extension is optional in the Common Policy.	Reconcile this with the Common CP
35	BBWG	Russel Weiser	T	Section 5.2.3.2.1	Bullet List does not mention the profile for the local authentication certificate to adhere too. Assuming that it us Asymetrical	Add to the bullet 5.
36	BBWG	Russel Weiser	E	5.2.4.1	Seems that the last paragraph should actually be the 1st in this section.	
37	BBWG	Russel Weiser	T	5.2.4.3	Should include "where a position sensitivity level is increased **or decreased"**	
38	BBWG	Russel Weiser	G-T		Conside defining a standard "friendly name" for all of the certificates that may be placed on a card. This would increase useability for the user allowing them to easily destinguish between the different uses of the certificates (such as properly selecting the signing certificate from the key managment certificate when configuring local applications such as email.	Tim should know what I mean here. ------- 1) "auth - *common name*", 2) "local auth - *common name*", 3) "signing - *common name*" 4)" key mgmt - *common name*" for example.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Submitted by: _Deborah Blanchard, I-CIDM BBWG
Date: _12/23/2004___

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical