X-Sieve: CMU Sieve 2.2
From: Russ Weiser <Russ.Weiser@cybertrust.com>
To: DraftFips201@nist.gov
Cc: Tom Greco <Tom.Greco@cybertrust.com>
Subject: Comments on Public Draft FIPS 201
Date: Thu, 23 Dec 2004 14:03:22 -0500
X-Mailer: Internet Mail Service (5.5.2657.72)
X-MailScanner:
X-MailScanner-From: russ.weiser@cybertrust.com

The following represent comments on behalf of Cybertrust an SSP provider submitted by Russel Weiser.
Cheers
RFW

 CommentTemplateRFW.xls

 smime1.p7s

Submitted by: _____

Date: _____

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	Cybertrust	Russel Weiser	G		The number of Roles as speified are overly burdensome to agencies.	consolidate Roles.
2	Cybertrust	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 ad a glossary and or prepend information to differentiate the roles.
3	Cybertrust	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.	
4	Cybertrust	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.	
5	Cybertrust	Russel Weiser	T	Section 4.1.3.1	Clarify the meaning of OVDs	
6	Cybertrust	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)	
7	Cybertrust	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	
8	Cybertrust	Russel Weiser	G	Section 4.1.4	I see no use in allowing multiple topologies. Select one and stick with it.	
9	Cybertrust	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.	
10	Cybertrust	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?	
11	Cybertrust	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.
12	Cybertrust	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.	

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

Submitted by: _____

Date: _____

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
13	Cybertrust	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	
14	Cybertrust	Russel Weiser	T	Section 4.4.1	Same issue as in 11 and 12 above.	
15	Cybertrust	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
16	Cybertrust	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
17	Cybertrust	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.
18	Cybertrust	Russel Weiser	E	5.2.4.1	Seems that the last paragraph should actually be the 1st in this section.	
19	Cybertrust	Russel Weiser	T	5.2.4.3	Should include "where a position sensitivity level is increased **or decreased**"	
20	Cybertrust	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