Comments on draft FIPS 201

Submitted by: Sharon Boeyen - Entrust Inc. _________

Date: December 7, 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
1	Entrust Inc.	Sharon Boeyen	G	Section 8, page v	Third paragraph introduces concept of accredited issuers but does not clarify whether these are card issuers, certificate/credential issuers or both.	Add text to section 8 clarifying the relationship between accredited "issuers" and associated card management systems and CAs.
2	Entrust Inc.	Sharon Boeyen	G	Section 2.2 page 5	PIV Issuing Authority definition implies a single issuer when in fact there may be a certificate issuer and a separate card issuer. While it is likely that the "Issuing Authority" is the entity that issues the smartcard based PKI credential, this should be clarified in the text, even if the fact that this authority may get services from elsewhere (e.g. a CA) is irrelevant to the end entity. Because there may be re-issuannce of a PKI credential without re-issuance of a physical card (e.g. an OID or email address change), it is important the roles of each authority be clearly stated in the specification. If the terms are each defined in this section, that would set the context for the remainder of the paper and some of the following comments (e.g. number 3) may become irrelevant.	Clarify the definition of the issuing authority and relate that entity to other authorities from which it may receive services (e.g. a CA). Also add text that outlines when a card is re-issued versus conditions for re-issuance or renewal of certificates on the card.

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
3	Entrust Inc.	Sharon Boeyen	G	Section 2.2.2 page 7	The first sentence discusses issuing or re-issuing identity credentials, but is unclear whether this pertains to issuance of the card or of the credentials, including certificates, that are stored on the card. This confusion carries through to other sections of the paper as well. However, if clarified here, the remaining instances are at least scoped within a specified context.	Add clarifying text to explain the meaning of "credentials" in this sentence. Also clarify the relationship of such credentials with both the card and certificates stored on the card
4	Entrust Inc.	Sharon Boeyen	G	Section 3.3 page 12 and page 13	PIV Card Issuance and Management Subsystem is a confusing name for a subsystem that includes Key Management and CA functions. A broader term should be used for this subsystem.	Suggest renaming to "PIV Management Subsystem"
5	Entrust Inc.	Sharon Boeyen	G	Section 3.3 page 12 and page 13	Component names within the PIV Card Issuance and Management subsystem do not clearly identify the components, but rather name a subset of the particular functions carried out by the components	Suggest renaming "Card Issuance" component to "Card Management" and suggest renaming "Key Mgt" component to "PKI Management".

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
6	Entrust Inc.	Sharon Boeyen	T	Section 3.3 page 13	The role of the registration repository and its relationship to a CA database is not explained, however there is an information flow shown in figure 3-1 from the registration repository to the key management component.	Add text that explains the role of the registration repository with respect to the key mgt component. Specifically, this repository contains data that needs to be included in the certificates issued by the CA. However the paper should make it clear that this registration repository is separate from the internal database a CA maintains about its certificate subjects.
7	Entrust Inc.	Sharon Boeyen	T	Section 3.4 page 16	The "PKI credential issuance" bullet discusses logical credentials. However there are logical credentials that are not part of PKI credentials (such as PINs)	Suggest replacing "generation of logical credentials" with "generation of PK certificates".
8	Entrust Inc.	Sharon Boeyen	G	Section 3.4 page 16	The activity described for the "PIV card maintenance" step deals with card maintenance as well as maintenance activities in the lifecycles of data on the cards, such as certificates.	Suggest renaimg the bullet from "PIV card maintenance" to PIV maintenance".

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
9	Entrust Inc.	Sharon Boeyen	T	Section 3.4 page 16	The PIV card termination step states that keys shall be destroyed as part of this step.	If the user is being issued a new card, then some of their keys (other than the authentication key) can be moved to a new card for the user. The text should be revised to clarify whether card termination includes situations such as that described here or not. If so, then the text should be clarified to indicate that the authentication key is destroyed but that other keys may be rolled over onto a new card for the user.
10	Entrust Inc.	Sharon Boeyen	T	Section 4.2.2 page 26	The "Issuing Authority" signs the CHUID. However, it is unclear who the Issuing Authority actually is. See comment against section 8 that suggests clarification of the definition of the issuing authority.	Either the definition of the issuing authority should be clarified as recommended in comment 2 above, or the text in section 4.2.2 should be modifed to clarify which entity is actually signing the CHUID.

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
11	Entrust Inc.	Sharon Boeyen	E	Section 4.1.5 page 23 & Section 4.3 page 27	Section 4.1.5 provides an outline of the keys and certificates that are mandatory (3rd bullet in first list) and optional (2nd list). Section 4.3 repeats these in a single list and then goes on to describe each in a separate and lengthier bullet list. However, the list in 4.1.5 doesn't use the same names for the keys (e.g. PIV authentication key, etc) making it confusing to correlate the keys from section 4.1.5 with those described in 4.3..	Use the same names for the keys in section 4.1.5 that are used in section 4.3.
12	Entrust Inc.	Sharon Boeyen	T	Section 4.3 page 29	There is a requirement that the FASC-N for the card be stored in the subject alternative name extension of the of the certificate for the PIV authentication key. However the reason for this requirement is not explained and the FASC-N is already stored elsewhere on the card.	Either explain why this is needed, or remove the requirement. If it remains a requirement, the syntax must be specified for the nameform. Also, there is nothing explaining how the CA would obtain this data. Is it supplied in a certificate request message or must the CA obtain it from the registration database (if it is stored there).
13	Entrust Inc.	Sharon Boeyen	G	Section 5.1.1 page 40	The FIPS does not specify the type schema or interfaces for the registration repository, however there is an information flow indicated from that repository to the CA.	Text should be added explaining what data flows from this repository to the CA and how that flow occurs.

Submitted by: Sharon Boeyen - Entrust Inc. _________
Date: December 7, 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
14	Entrust Inc.	Sharon Boeyen	T	Section 5.1.2 page 40	This section states that both cards and certificates can be revoked. The last sentence of the first paragraph states that the CAs shall maintain status servers and responders needed for PIV card and certificate status checking. However, CAs deal only with certificate revocation, not with card revocation.	Rewrite this section clarifying that CAs shall provide these services ONLY for certificate revocation. If there is to be a similar service for card revocations, involving some sort of lists and/or status servers, this new service needs to be fully defined.
15	Entrust Inc.	Sharon Boeyen	T	Section 5.1.2 page 40	The last sentence of the 2nd paragraph states that "A current, unexpired PIV authentication certificate on a card is proof that the card was issued and is not revoked. That is not true because the authentication certificate could be unexpired but be revoked (without the card having been revoked). Also there is some time lapse (even if only seconds) between the time a card is reported missing and the authentication certificate is revoked with that status replicated to all necessary servers.	Revise this sentence along the following lines: "The presence of a valid, unexpired and unrevoked certificate on a card is an indication that the card was issued and is not revoked.
16	Entrust Inc.	Sharon Boeyen	G	Section 5.2.2 page 42	Similar to earlier comments above - the relationship of the "issuing authority" to the CA and card management system is unclear. Also, there is nothing stated about the issuer of the certificate used to verify the signature of the issuing authority (e.g. on the biometrics).	Explain the relationship, if any and also add text about the issuer of the issuing authority's certificate. Is this certificate required to be issued by the same CA that issues certificates to card holders? Must it at least be a CA that is connected to the US Federal Bridge CA?

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
17	Entrust Inc.	Sharon Boeyen	T	Section 5.2.2 page 43	The last paragraph of this section suggests that PKI certificate identification information may possibly be enrolled and registered with the PIV backend database system. It is unclear whether this is the same "registration repository" mentioned in earlier sections of the document. The information retained by the CA in its internal database, about its certificate subjects should NOT need to be stored in another database. This is unnecessary duplication and leads to synchronization problems.	Delete "and possibly PKI certificate identification information" from the sentence.
18	Entrust Inc.	Sharon Boeyen	T	Section 5.2.3.2 page 44	The fifth bullet lists the FASC-N as a mandatory element in the subject alternative names extension of PIV authentication certificates. As with earlier related comments, the reason for this requirement is not explained, especially given that the FASC-N is already stored elsewhere on the card.	Either explain why this is needed, or remove the requirement. If it remains a requirement, the syntax must be specified for the nameform. Also, there is nothing explaining how the CA would obtain this data. Is it supplied in a certificate request message or must the CA obtain it from the registration database (if it is stored there).

Submitted by: Sharon Boeyen - Entrust Inc. _________
Date: December 7, 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
19	Entrust Inc.	Sharon Boeyen	T	Section 5.2.4 pages 46 and 47	Although there are two different terms "renewal" and "re-issuance" the difference between these two is not apparent. The only difference appears to be that with renewal a new facial image is collected. For instance, the first sentence of 5.2.4.1 states that a cardholder applies for "renewal" when a valid card expires. However the first sentence in the second paragraph of 5.2.4.2 states that a cardholder shall apply for re-issuance when the PIV card is expired. Also, neither subsection discusses the relationship with expiration dates of certificates.	Clarify which of the two processes a cardholder is to apply for upon expiry of their card. Also indicate whether it is normal procedure for the card to expire first, or for cardholders to apply for renewal/reissuance prior to their card's expiry. Add text to this section about the lifetimes of certificates. There is one small paragraph in 5.2.4.1 but nothing in 5.2.4.2. Somewhere there should be an explanation of the lifecycle of these certificates and indications of when/why they would need to be rolled over. At present this is provided only for the PIV authentication certificate and its explanation is very brief.
20	Entrust Inc.	Sharon Boeyen	T	Section 5.2.5 page 48	In the penultimate bullet, it states that agencies 'may' revoke certificates corresponding to the optional digital signature and key management keys. Given the reasons for PIV card termination, it is unclear why this is a 'may' instead of a 'shall'.	Either explain the circumstances under which it would be logical for an agency not to revoke these certificates, or change the "may" to a "shall".