Submitted by: Northrop Grumman. POC: Kenneth Aull (703-345-8861, ken.aull@ngc.com)
Date: 21 Dec 04

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	Northrop Grumman	ken.aull@ngc.com	General	Replacement for PIV-2	Existing smartcard implementations provide space and functionality for an Identity Certificate. This functionality can be used to provide a simple transition strategy for FIPS-201	Define a FIPS-201 Standard for the Federal Identity Certificate (PKI) to be included in each PIV. Specifically, the Certificate SubjectName should be standardized to sign all the key information about the holder of the PIV, such as name, FASC-N, Unique ID, Vetting level, and Sponsor. Revocation of the certificate cancels all of the above including biometrics (see further comments). Example: cn=name,ou=FASC-N, ou=CHUID, ou=level,ou=sponsor,ou=gov,c=us. Non-Repudiation should not be asserted in the Identity Certificate since it is not the personal, PIN protected digital signature of the individual. The PIV should support client authentication in order to support privacy-protected recovery of reference biometrics.
2	Northrop Grumman	ken.aull@ngc.com	General	Replacement for PIV-2	PIN should not be used to protect the Identity Certificate, which is public information. The card should be allowed to do a digital signature to prove that the private key is contained on the card, and to provide private access to reference biometrics.	The Identity Certificate should be able to be used for digital signature to prove to a Registration Station that it is a valid PIV without the use of a PIN. This is a minor modification to existing and planned issuing stations, they need to set the protection flag to support open use of signing of the Identity certificate only. Inserting the card into a qualified registration station (proven through PKI) should allow the request of reference biometrics, since the real biometrics are also being collected at a qualified registration station. Note that the OID of a certificate for a qualified registration station can be proven via the Federal Bridge.
3	Northrop Grumman	ken.aull@ngc.com	General	Replacement for PIV-2	Bind biometrics cryptographic hashes and URI pointers into the Identity Certificate to inform the registration station where to locate the biometrics, and how to check against alteration in place or in transit.	Use RFC 3039 to provide the standard extension for biometrics for use in X.509v3 certificates. This mechanism can also be used to sign general 'biometrics', as a well as well-formed XML assertion of security level, clearance, person type for use in helping the relying party to determine which additional capabilities should be assigned to a person registering into the local physical and logical system. The recommendation is to include an RFC 3039 for each biometric on the card (optional), as well as for at least 8-fingers in FBI-standard wavelet form at the Sponsor's FIPS-201 website.
4	Northrop Grumman	ken.aull@ngc.com	General	Replacement for PIV-2	PIV issuers should provide RFC 3039 hashed biometric access for PIV that they have issued, to support biometric assertion of card ownership to relying parties	PIV issuers should place compressed biometrics on-card, OR off-card, FBI-standard wavelets in a secure SSLv3 strong encryption, strong authentication protected database. The issuer has a choice of biometric location, or can use both locations. On-Line databases shall require a cryptographic signature to a real-time challenge using SSLv3 in order to obtain only the biometrics/XML assertions belonging to the one card holder that is presenting his card at a qualified registration station, proven crytographically via Federal Bridge OID. General access using a HSM is only allowed to the issuing CA in order to obtain the reference biometrics in order to compute the cryptographic hash to be included in the identity certificate under the URIs presented during certificate creation, in accordance with RFC 3039.
5	Northrop Grumman	ken.aull@ngc.com	General	Replacement for PIV-2	NIST should establish a reference Registration API in order to support major smartcard standards such as GSC-IS 2.1, VM and File Cards. Additionally, when available, the API for SP 800-73 should be supported. The API should support digital signature using the Federal Identity Certificate, and recovery of reference biometrics, if the RFC 3039 indicates the presence of on-card biometrics	A reference API, certified by NIST, should be contributed by manufacturers that wish to participate in FIPS-201. Upon inserting a PIV into a registration station using the standardized API, the card type shall be determined, and the appropriate stack provides methods for exercising the digital signature and biometric recovery which are supported in each independent stack. Since the stack for digital signature and biometric recovery is a small part of the full smartcard API, such a reference API should be available three months before Agencies are expected to use the API to validate compliant PIV using stacks that have been submitted and verified by NIST for incorporation into the reference API. All major cards in use by the Federal Government shall be supported at the discretion of the vendors, including SP 800-73 when available. This provides a smooth and discontinuity free evolution of smartcard technologies, while supporting existing implementations with minimal or no disruption.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editorial, 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
6	Northrop Grumman	ken.aull@ngc.com	Technical	version 1.0, Section 4.4.6, Page 37	RFC 3852 should not be used for protecting biometrics in storage. There is no method for revoking a signed biometric, in support of identity theft, change of biometrics (e.g. weight gain), loss of employment, etc.	RFC 3039 is recommended as the preferred method of providing biometric data protection on and off card. The RFC provides for unlimited URI points and hashes to biometrics, using existing Identity certificates. The use of the identity certificate then provides CRL/OCSP revocation of faulty, fradulent or expired biometrics. Biometrics are essentially cancelled when the identity is revoked. RFC 3039 3.2.4 Biometric Information This section defines an extension for storage of biometric information. Biometric information is stored in the form of a hash of a biometric template. The purpose of this extension is to provide means for authentication of biometric information. The biometric information that corresponds to the stored hash is not stored in this extension, but the extension MAY include an URI pointing to a location where this information can be obtained. If included, this URI does not imply that this is the only way to access this information. It is RECOMMENDED that biometric information in this extension is
7	Northrop Grumman	ken.aull@ngc.com	Technical	Version 1.0, Section 6.1.3, Page 52	Signature check on the biometric should always (not optionally) involve a CRL/OCSP check of the identity certificate (see comment 1 above), which would check the biometric hash signed into the certificate. Date check should also always be required.	1). The cardholder grants access to the identity certificate by inserting the PIV into the reader. The PIN allows the on-board signed hashed (by the RFC 3039 extension)biometric to be read from the card. 2). The date of the identity certificate is validated. 3). The revocation status of the identity certificate is checked through the Federal Bridge 4). The biometric reference is read from the card, and the signed hash is checked. 5). The cardholder is prompted to submit a live sample. 6). If the biometrics match, the person owns the identity certificate and the card. 7). All CHUID elements are already in the identity certificate, including FASC-N, Agency code, DUNS, Position Sensitivity, and can be used for physical access. Note. By including CHUID in the certificate subject name, CHUID functionality is identical in the physical and logical worlds. In one case identity is proved by the private key, in the other, it is proved biometrically.
8	Northrop Grumman	ken.aull@ngc.com	Technical	Version 1.0, Section 6.1.2, Page 52	The Identity certificate should contain the CHUID contents in a public certificate. Authentication is greatly simplified, being the same in the physical and logical world	1). The Identity certificate is read from the card. 2). The expiration date of the certificate is checked. 3). The trusted signature is checked through the Federal Bridge 4). The certificate is evaluated for revocation 5). FASC-N, Agency code, DUNS, or Position Sensitivity are used to determine access. In the alternative case, the identity certificate is passed through a unidirectional cryptographic transform.....
9	Northrop Grumman	ken.aull@ngc.com	Technical	Version 1.0, Section 4.4.5, Page 35	Use of RFC 3039 allows for multiple biometrics. This allows a facial representation suitable for on-card storage, and off-board storage, signed by the identity certificate.	Provide an Optional off-board facial photograph suitable for life-size comparison. This would be an RFC 3039 pointer to signed biometric data. This data can be safely stored since it is anonymous, and digitally signed by the identity certificate. Revocation of the identity certificate cancels the biometric data.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editorial, 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
10	Northrop Grumman	ken.aull@ngc.com	Technical	Version 1.0, Section 4.1.6, Page 24	No PIN should be required for the release of biometric data. An example is the Electronic passport, which does not require a PIN to release biometric data. The privacy of the individual is not protected by such a requirement.	Place biometric data in the public area of the PIV. This greatly simplifies the processing of biometric data, and allows it to be retained at high volume transit points in accordance with RFC 3039. Permission to use the biometric should be granted by the card holder by "insertion into a card reader". Use of a PIN should not be required to support digital signature using the Identity Certificate.
11	Northrop Grumman	ken.aull@ngc.com	Technical	Version 1.0, Section 4.1.6.1, Page 24	Biometric data should not be used for card activation. This is because card activation can occur in untrusted environments.	Biometric data should only be used to authenticate the ownership of the card to a relying party, and only in an environment where spoofing is difficult. Example, in a public gateway, attended by a guard, a biometric, plus the card should provide a reliably authentication of the ownership of the card. At an unattended location, presentation of a biometric, and card is insufficient.
12	Northrop Grumman	ken.aull@ngc.com	Technical	Version 1.0, Section 4.2, Page 25	CHUID should not use RFC 3852 signatures. These signatures provide no ability to revoke an asymmetric signature.	Critical CHUID information such as the Unique ID, expiration date, Sensitivity should be signed into the basic Identity certificate. This allows the sponsoring organization to cancel a mistake. For this reason, the revocation status of any card should always be checked, and it should not be optional. An explicit format and content of the Identity Certificate and its subject name should be established, containing the FASC-N, CHUID, and trust level.
13	Northrop Grumman	ken.aull@ngc.com	Technical	Version 1.0, Section 5.2.1.1, Page 41	Insider attack to modify biometrics is a real risk. This should be prevented.	The establishment of an identity should be encoded in an Identity digital certificate, and RFC 3039 should be used to prevent subsequent undetectable modification of submitted biometrics, and to provide a reliable source of verification biometrics. A subsequent submittal of a different identity with the same biometrics should result in the revocation of the original identity certificate, and the reissuance of a new identity certificate that maintains all previous alias.
14	Northrop Grumman	ken.aull@ngc.com	Technical		PIV Sponsors should be required to set up biometrics webserver that can only be accessed by the Specific PIV that links the user and the biometrics	The URI used in RFC 3039 need a distributed distribution point. Each sponsor agency should vend the biometrics to the relying party if the specific PIV is used
15	Northrop Grumman	ken.aull@ngc.com	Technical		The Registration Use case should allow a transition from existing smartcards to SP 800-73 cards	Existing smartcards, using a standardized Identity certificate, should be acceptable to any registration station. As SP 800-73 cards become available, and have been certified, it is expected that the smartcards will standardize on SP 800-73. The specific functions should be, recognize smartcard type, and then support digital signature using the Identity Certificate.
16		ken.aull@ngc.com	Technical	Section 4.1.4, Figure 4.2	The magnetic stripe, as depicted in Section 4.1.4, Figure 4-2: BACK OF THE CARD (STANDARD FORMAT) was located on the “wrong” side of the card. The placement of the magnetic stripe depicted in the FIPS PUB 201 figure should be in compliance with ISO 7811 regarding placement of the magnetic stripe on a smart card.	Make magnetic strip place conform to ISO 7811

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	Northrop Grumman	ken.aull@ngc.com	Technical	Section 4.1.4, Figure 4.2	If the magnetic stripe is relocated to the right hand side of the card, the optional 3 of 9 Linear Bar Code would have to move to the left side of the card.	Switch Magnetic strip with Barcode placement (see recommendation above).
18	Northrop Grumman	ken.aull@ngc.com	Technical	Section 4.1.4, Figure 4.2	The optional 3 of 9 Linear Bar Code, depicted on the long edge of the card can not be accommodated if the card has a magnetic stripe and the Point Sizes specified for the text are adhered to. The reason is that there is not enough room on the card.	Use smaller Point size
19	Northrop Grumman	ken.aull@ngc.com	Technical	Section 4.1.4, Figure 4.2	The Point Size (10pt Arial) that is specified for the Agency Card Serial Number and Issuer Identification Number is too large if the optional Physical Characteristics fields are to be included on the card. Using a Point Size of 6pt Arial seems to works well.	Use Point size of 6pt Arial
20	Northrop Grumman	ken.aull@ngc.com	Technical	Section 4.1.4, Figure 4.2	The use of 5pt Arial text on the back of the card not only makes reading it difficult due to size, but also results in less than ideal printing resolution by most mid-range smart card printers.	Use larger Point size of 6 or greater
21	Northrop Grumman	ken.aull@ngc.com	Technical	Section 4.1.4, Figure 4.2	Critical Security information is obscured when the PIV is plugged into a standard card reader.	To allow a security officer to observe the PIV while inserted in a reader during normal operation as a digital token, the expiry date, and the Duty Status Should be moved from the obscured area. Nothing of critical value should be printed in this area.