Proposed Changes to SP 800-73

NIST is planning to amend SP 800-73 to synchronize biometric data model with SP 800-76, Biometric Data Specification for Personal Identity Verification, and enhance the utility of the PIV card for logical access. The following table provides all the Errata made to-date on this specification. Note that the Errata is not incorporated in the document to avoid the need for developers to seek out differences.

Changes to the biometric data container and PKI certificate access control rules will ease the development and implementation of PIV standards. Specifically, the modifications to SP 800-73 will permit retrieval of certificates through the card's contact interface without entering a PIN. These modifications do not impact the access control rules for private keys, or the information accessible through the contactless interface.

PIN access to certificates is a departure from current best practices because certificates are generally available without access control. SP 800-73 restricted access to these certificates to protect cardholder identities included in PIV certificates. However, these cardholder identities can be obtained from other sources on or in the PIV card without a PIN, and PIN access for certificates negatively impacts compatibility with smart card based authentication mechanisms and applications.

NIST believes PIV smart card logon is essential to protecting logical access to Federally controlled information systems. The most common smart card based authentication mechanism assumes that certificates are available without presentation of a PIN. Similarly, common applications, such as secure mail, assume that digital signature and key management certificates are available without presentation of a PIN. The proposed amendments to SP 800-73, permitting retrieval of certificates through the card's contact interface without entering a PIN, promote compatibility of PIV cards with COTS smart card logon mechanisms and common applications with minimal negative impact on privacy.

Date	Section, Page	Change
9/29/05	1.8.5, Pg 6	Correct the reference to "Appendix C.2" to "Appendix C"
9/29/05	5.5, Pg. 26, Table 12, First cell of the forth row	Correct the Algorithm ID for the Card Application Administration Key from: '06' To: '00'
9/29/05	5.6, Pg. 26, Table 13, Third cell of the forth row, 7.2.3, Pg 39, Response Syntax Table, First cell of the first row	Correct the meaning of the status word "63CX" from: "Verification failed, X indicates the number of further allowed retries" to: "Verification failed, X indicates the number of further allowed retries or resets"
9/29/05	6.3.1, Pg. 32	Correct "bytesToBeVerified" to "algorithmInput"
9/29/05	6.3.1, Pg. 32	Correct "CryptoResult" to "algorithmOutput"
9/29/05	6.4.1, Pg. 33	Remove the return code PIV_OFFSET_BEYOND_END_OF_DATA_CONTENT as the OFFSET argument no longer appears in the signature of the entry point.

Date	Section, Page	Change
9/29/05	Table 15, Pg. 35	Correct the Security Condition for Use for RESET RETRY COUNTER from “PIV Card Application Adminstrator and Card Holder Biometric” to “PIN Unblocking Key”.
9/29/05	Table 15, Pg. 35	Correct the Security Condition for Use for PUT DATA from “Data Dependent. See Table 1.” to “PIV Card Application Administrator”.
9/29/05	7.1.1, Pg. 36	Correct all occurrences of “a right truncated version” to “the right truncated version”
9/29/05	Appendix A	Correct the maximum size of all X.509 certificate objects to 1856
9/29/05	Table 25, Pg. 51	Correct the key reference from ‘9A’ to ‘9E’
2/6/06	Table 1, Pg. 5	Remove Fingerprint Buffer 2 from the table.
2/6/06	Table 1, Pg. 5	Replace “PIV Authentication Key Buffer” with “PIV Authentication Certificate Buffer”.
2/6/06	Table 1, Pg. 5	Change the PIV Authentication Key Buffer access rule to “Read Always”.
2/6/06	Table 1, Pg. 5	Replace “Digital Signature Key Buffer” with “Digital Signature Certificate Buffer”.
2/6/06	Table 1, Pg. 5	Change the Digital Signature Key Buffer access rule to “Read Always”.
2/6/06	Table 1, Pg. 5	Replace “Key Management Key Buffer” with “Key Management Certificate Buffer”.
2/6/06	Table 1, Pg. 5	Change the Key Management Key Buffer access rule to “Read Always”.
2/6/06	1.8.4, Pg. 5	Replace “headers” with “header”.
2/6/06	4.1, Pg. 22	Add a note indicating Card Holder Fingerprint I and II will be recorded in one container.
2/6/06	Table 6, Pg. 22	Replace “Card Holder Fingerprint I” with “Card Holder Fingerprints”.
2/6/06	Table 6, Pg. 22	Remove Card Holder Fingerprint II.
2/6/06	5.5, Pg. 26	Add a second sentence to the first paragraph — Key references are only assigned to private and secret (symmetric) keys.
2/6/06	5.5, Table 12, Pg. 26	Change the title of Table 12 / Column 4 from “Authenticatable Entity” to “Security Condition for Use”
2/6/06	5.5, Table 12, Pg. 26	Replace “Authenticatable Entity” for Card Holder Global PIN from “Card Holder” to “Always”.
2/6/06	5.5, Table 12, Pg. 26	Replace “Authenticatable Entity” for Card Holder PIV Card Application PIN from “Card Holder” to “Always”.
2/6/06	5.5, Table 12, Pg. 26	Replace “Authenticatable Entity” for PIV Authentication Key from “PIV Card Application Provider” to “Card Holder PIN”.
2/6/06	5.5, Table 12, Pg. 26	Replace “Authenticatable Entity” for PIV Card Application Administration Key from “PIV Card Application Administrator” to “Always”.
2/6/06	5.5, Table 12, Pg. 26	Replace “Authenticatable Entity” for PIV Card Application Digital Signature Key from “PIV Card Application Administrator” to “Card Holder PIN - Always”.

Date	Section, Page	Change
2/6/06	5.5, Table 12, Pg. 26	Replace “Authenticatable Entity” for PIV Card Application Key Management Key from “PIV Card Application Administrator” to “Card Holder PIN”.
2/6/06	Appendix A, Pg. 45	Replace “Card Holder Fingerprint I” with “Card Holder Fingerprints” in the Buffer Description table.
2/6/06	Appendix A, Pg. 45	Remove Card Holder Fingerprint II from the Buffer Description table.
2/6/06	Appendix A, Pg. 46	Change Card Holder Fingerprint I size to maximum 4k bytes.
2/6/06	Appendix A, Pg. 46	Replace the table heading “Card Holder Fingerprint I” with “Card Holder Fingerprints”
2/6/06	Appendix A, Pg. 46	Remove Card Holder Fingerprint II table.