#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
DoD-1	DoD	Jonathan Shu	Critical	1	General	General	General	DoD non-concurs with any revision of NIST SP 800-73 that offers no alternative to the "pairing code" concept as written.	DoD proposes a viable alternative that mitigates risks while providing Federal Agencies flexibility to meet their own business needs. The alternative to "pairing code" is "PIN" as long as the PIV issuer implements a separate contactless PIN counter to minimize exposure to other risks." See comment DoD #15 for details on separate PIN counter.	As discussed with OMB, agencies wishing to enable the optional VCI feature without pairing (it is to be disabled by default) will need to require compensating controls to ensure PII (i.e. name, email address and organization) will not be skimmed from the PIV card when in close proximity when the card is outside of its protective sleeve. PIN counter is addressed by resolution to comment OT-2.
DoD-2	DoD	Jonathan Shu	Admin	1	v	150	Revision History	This section states Revision History is "Deprecated some data elements in the CHUID (Buffer Length, DUNS, and Organizational Identifier) and legacy data elements in all X.509 Certificates (MSCUID)." However, throughout the document the stated changes are not apparent.	DoD recommends updating Tables 9 through 39, change "Optional" to "Deprecated" for each deprecated data element.	Resolved by OT-19.
DoD-3	DoD	Jonathan Shu	Substantive	1	1 and 2	375-381	1.3	Implementation Timeframe: This section states, "With the exception of the requirement for the PIV Card Application to enforce the minimum length requirements for the PINS Federal departments and agencies must implement these recommendations no later than 12 months after the effective date of FIPS 201-2." The required implementation date of 12 months is too aggressive. DoD will have trouble issuing CAC/PIVs with new mandatory features within 12 months of the final standards, due to resource limitations, acquisition cycles, and required testing processes to ensure that cards with new capabilities continue to operate seamlessly.	DoD strongly recommends agencies are provided a 24-month window to incorporate new mandatory features.	Resolved by SCA-1 and by DoD-7 from the disposition of comments on the May 2013 draft of SP 800-73-4 at http://csrc.nist.gov/publications/drafts/800-73-4/sp800_73-4_2013_draft_comments_and_dispositions.pdf.
DoD-4	DoD	Jonathan Shu	Substantive	1	5	486	3.1.2	Currently, the document outlines a minimum of 14 characters for the credential series number. DoD continues to believe that this should be 16 characters in order to provide a larger pool of unique numbers. Organizations with larger numbers of cardholders like DoD are concerned that collisions will occur much sooner with 14 characters versus 16 characters.	DoD recommends adding the credential series and the individual credential Issue to the FASC-N identifier providing the minimum length of 16 characters.	Resolved by DoD-9 from the disposition of comments on the May 2013 draft of SP 800-73-4 at http://csrc.nist.gov/publications/drafts/800-73-4/sp800_73-4_2013_draft_comments_and_dispositions.pdf.
DoD-5	DoD	Jonathan Shu	Critical	1	7 14-15 23	547-549 804, table 2 965	3.1.3 3.5 Table 7	DoD feels that access over SM of the X.509 Certificate for PIV Authentication must be equivalent to contact operations. This will ensure deployed infrastructure can continue be interoperable and support existing use cases (i.e., smart card network logon, web authentication, and secure mail) on Microsoft OS platform without major reengineering.	DoD recommends the PIV Authentication public certificate is available over the contact interface, Secure Messaging (SM) or Virtual Contact Interface (VCI) as free read to mirror today's processes on the contact interface.	Resolved by DoD-1.
DoD-6	DoD	Jonathan Shu	Substantive	1	7	576-585	3.1.4	Permitting the asymmetric CAK to be generated off card enables a vulnerability that multiple cards can be created and used for physical access by different individuals using different cards.	DoD recommends a requirement be added that the CAK must be generated on-card and be non-exportable. Alternately, if NIST determines that off-card generation should be permitted, DoD strongly recommends that the CAK be uniquely generated for each card and the off card key required be destroyed (i.e., no key escrow capabilities).	Resolved by DoD-10 from the disposition of comments on the May 2013 draft of SP 800-73-4 http://csrc.nist.gov/publications/drafts/800-73-4/sp800_73-4_2013_draft_comments_and_dispositions.pdf.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
DoD-7	DoD	Jonathan Shu	Critical	1	8 14-15 23	601-602 804, table 2 965	3.2.1 3.5 Table 7	DoD feels that access over SM of the X.509 Certificate for Digital Signature must be equivalent to contact operations. This will ensure deployed infrastructure can continue be interoperable and support existing use cases (i.e., smart card network logon, web authentication, and secure mail) on Microsoft OS platforms without major reengineering.	DoD recommends the digital signature public certificate is available over the contact interface, Secure Messaging (SM) or Virtual Contact Interface (VCI) as free read to mirror current processes/capabilities over the contact interface.	Resolved by DoD-1.
DoD-8	DoD	Jonathan Shu	Critical	1	8 14-15 23	610-611 804, table 2 965	3.2.2 3.5 Table 7	DoD feels that access over SM of the X.509 Certificate for Key Management must be equivalent to contact operations. This will ensure deployed infrastructure can continue be interoperable and support existing use cases (i.e., smart card network logon, web authentication, and secure mail) on Microsoft OS platforms without major reengineering.	DoD recommends the key management public certificate is available over the contact interface, Secure Messaging (SM) or Virtual Contact Interface (VCI) as free read to mirror current processes/capabilities over the contact interface.	Resolved by DoD-1.
DoD-9	DoD	Jonathan Shu	Critical	1	8	626	3.2.1	DoD feels NIST should allow Federal agencies the flexibility to implement PIN caching in the manner they feel best meets their business needs and willingness to accept risk. We understand the requirement within FIPS 201 for the PIN access control rule; however, we do not understand the need for NIST to venture outside that specific requirement. The responsibility to manage any risk associated with government owned workstations, PKE websites, and business processes that use digital signatures is the responsibility of each Federal agency. DoD requests NIST allow the Department to exercise those authorities.	At the end of section 3.2.1, add the following: "Although a PIN must always be provided to the card, this provision is not intended to preclude PIN caching by the application software."	Resolved by DoD-11 from the disposition of comments on the May 2013 draft of SP 800-73-4, available at http://csrc.nist.gov/publications/drafts/800-73-4/sp800_73-4_2013_draft_comments_and_dispositions.pdf.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
DoD-10	DoD	Jonathan Shu	Critical	1	9		3.3.2	As an accompanying feature to DoD comment #1 and #15 ("pairing code" alternative as PIN and secondary PIN counter on contactless interface), DoD believes the discovery object should include a mechanism for relying parties/systems to know whether a pairing code or the alternative is used for any particular PIV.	DoD recommends NIST specify the unused bits of the Discovery Object as a required component to indicate if the "pairing code" alternative is used. Suggested addition to DMDC Proposed NIST 800 73-4 2nd Public Draft Update for Paring Code Alternative Definition of the Discovery Object tag 0x5F2F (Table 1., Page 9, Lines 623 – 632) should be modified in support of the pairing code alternative and contactless PIN blocking mitigation should be as follows. + Tag 0x5F2F encodes the PIN Usage Policy as follows: First byte: Bit 7 indicates whether the PIV Card Application PIN satisfies the PIV Access Control Rules (ACRs) for command execution4 and data object access. * Bit 7 shall always be set to 1. * Bit 6 indicates whether the Global PIN satisfies the PIV ACRs for command execution and PIV data object access. * Bit 5 indicates whether the pairing code is implemented. * Bit 4 Indicates that PIV Card Application PIN and Global PIN satisfy pairing code ACRs. * Bit 3 Indicates that vendor specific contactless PIN blocking mitigation is implemented. * Bits 8 and 2 through 1 of the first byte shall be set to zero.	Resolved by adding discovery of Pairing Code and VCI in the PIN Usage Policy as follows: Bit 7 is set to 1 to indicate that the mandatory PIV Card Application PIN satisfies the PIV Access Control Rules (ACRs) for command execution and data object access. Bit 6 indicates whether the optional Global PIN satisfies the PIV ACRs for command execution and PIV data object access. Bit 5 indicates whether the optional OCC satisfies the PIV ACRs for command execution and PIV data object access Bit 4 indicates whether the optional VCI is implemented. Bit 3 is set to zero if the pairing code is required to establish a VCI and is set to one if a VCI is established without pairing code Bits 8, 2, and 1 of the first byte shall be set to zero. Table 1 shall be updated accordingly.
DoD-11	DoD	Jonathan Shu	Substantive	1	10-11		3.3.3	DoD agrees with the protection of the Key History Object using the Security Object. The Key History Object as defined requires a commitment to a URL during the issuance of a card. DoD does not support inclusion of the access method (i.e., HTTP) and DNS Name as part of the Key History Object since these can change.	DoD recommends NIST outlines provisions to protect the rest of the information including the SHA-256 hash of the OffCardKeyHistoryFile and the structure of the OffCardKeyHistoryFile.	Declined. Such a change would not be compatible with SP 800-73-3. Also, since HTTP is the only access mechanism that may be specified, it cannot change.
DoD-12	DoD	Jonathan Shu	Critical	1	12 14-15 23	720-721 804, table 2 965	3.3.3 3.5 Table 7	DoD feels that access over SM of the Key History Object must be equivalent to contact operations. This will ensure deployed infrastructure can continue be interoperable and support existing use cases (i.e., smart card network logon, web authentication, and secure mail) on Microsoft OS platforms without major reengineering.	DoD recommends the key history object is available over the contact interface, Secure Messaging (SM) or Virtual Contact Interface (VCI) as free read to mirror current processes/capabilities over the contact interface.	Resolved by DoD-1.
DoD-13	DoD	Jonathan Shu	Critical	1	12 14-15 23	725-726 804, table 2 965	3.3.4 3.5 Table 7	DoD feels that access over SM of the Retired X.509 Certificates for Key Management must be equivalent to contact operations. This will ensure deployed infrastructure can continue be interoperable and support existing use cases (i.e., smart card network logon, web authentication, and secure mail) on Microsoft OS platforms without major reengineering.	DoD recommends retired X.509 certificates for key management are available over the contact interface, Secure Messaging (SM) or Virtual Contact Interface (VCI) as free read to mirror current processes/capabilities over the contact interface.	Resolved by DoD-1.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
DoD-14	DoD	Jonathan Shu	Critical	1	14 14 18 23	627-674 804 865 965	3.3.2 Table 2, Footnote 11 5.1, Table 4 Table 7, Footnote 18	See comment #1, the security condition for use must permit PIN to establish VCI.	DoD recommends changing VCI entries to SM.	Resolved by DoD-1.
DoD-15	DoD	Jonathan Shu	Critical	1	18	865	5.1, Following Table 4	See comment #1: DoD proposed alternative to "pairing code" (i.e., second PIN counter on contactless interface) would not require PIN Block (where PIN Block affects both contact and contactless interfaces) due to invalid PIN entry over SM.	DoD recommends the following language be added to this section "Separate PIN block invalid entry counters may be implemented for the contact and contactless interfaces. If separate invalid entry counters or an equivalent mechanism are implemented, a blocked PIN condition on the contactless interface shall not cause the contact interface PIN to be blocked. Both the contact and contactless PINs shall be blocked when the contact PIN invalid entry counter is expired. A successful PIN entry on either the contact or contactless Interface shall reset both contact and contactless PIN invalid entry counters. A PIN blocked contactless interface may be unblocked by a successful PIN entry on the contact interface. Issuers may optionally decrement the contactless PIN invalid entry counter for invalid Paring Code entry and block both Pairing Code and PIN entry on the contactless interface due to an expired contactless invalid entry counter."	Resolved by OT-2.
DoD-16	DoD	Jonathan Shu	Critical	2	7	451, Note 1	3	See comment #1: VCI may be established by presentation of a valid PIN.	DoD recommends updating Note 1 to "For SM, OCC, PIN and pairing code alone can be submitted via secure messaging (SM) over the contactless interface."	Resolved by DoD-1.
DoD-17	DoD	Jonathan Shu	Critical	2	7	451, Note 2	3	See comment #1: The security condition for Use must permit PIN to establish VCI.	DoD recommends updating Note 2 to "The term virtual contact interface is used in this document as shorthand for a security condition in which secure messaging is used AND the security status indicator associated with the PIN or pairing code is TRUE."	Resolved by DoD-1. Also, the sentence will be updated, accordingly.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
FE-1		Federal Employee	G					"NIST is interested in receiving feedback on whether the new skimming protection measure shall be included on all PIV Cards that implement the VCI, or if it departments and agencies that issue the cards shall have the ability to disable this security control if there are specific use cases that conflict with pairing code function and alternate mitigating controls are available and identified."	None. Continue to make the pairing code mandatory for PIV Cards that support the virtual contact interface. If the skimming protection is disabled then any card reader within range of a PIV Card will be able to retrieve private information (e.g., name and email address) from the card by simply establishing secure messaging and then reading the data, as there would be no access control restrictions that would protect access to the data. As noted in SP 800-116, "[a] contactless PIV Card reader with a sensitive antenna can be concealed in a briefcase, and is capable of reading ISO/IEC 14443 contactless smart cards like the PIV Card at a distance of at least 25 cm." This means that if skimming protection were disabled a stalker could use a card reader hidden in a briefcase to obtain the name and email address of a Federal employee or contractor as she was walking down the sidewalk or was sitting in a bar after work without her knowledge. The information read from the card could likely be used in an online search to obtain more information about the cardholder. If the stalker had violent tendencies then the stalker's ability to obtain this information about the cardholder could put her safety at risk.	Noted. As discussed with OMB, agencies that "wishing to enable the optional VCI feature without pairing (it is to be disabled by default) will need to require compensating controls to ensure PII (i.e. name, email address and organization) will not be skimmed from the PIV card when in close proximity when the card is outside of its protective sleeve." An informative note will be added for implementers to point out that the VCI method 'secure messaging coupled with pairing code' is designed to protect against skimming attacks.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
FE-2		Federal Employee	G					Suppose you were sitting in a bar after work having a drink. Someone approaches you and he asks you for your name and email address. There's something about him that makes you feel uncomfortable. He seems a bit creepy. Would you tell him you name and email address? Would you encourage your daughter to do so if she were in that position? If not, then please do not force people to provide this information in circumstances such as this by making the information available for skimming from the identity cards that they are required to carry with them when they go to work.		Noted. See resloution to FE-1.
FE-3		Federal Employee	G					WebMD (http://www.webmd.com/women/features/how-to-protect-yourself-from-a-stalker) encourages women, in order to protect against being stalked by relative strangers to "Have a policy of never giving your email address to a stranger - not even the cute guy you meet at a bar." The National Institute of Justice (http://www.nij.gov/topics/crime/stalking/Pages/welcome.aspx) notes that stalking, even cyberstalking, is a "serious crime."	Follow the advice of WebMD and the National Institute of Justice, and do not allow PIV Cards to expose personal information that would put people's safety at risk.	Noted. See resolution to FE-1.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
FE-4		Federal Employee	G					"NIST is interested in receiving feedback on whether the new skimming protection measure shall be included on all PIV Cards that implement the VCI, or if it departments and agencies that issue the cards shall have the ability to disable this security control if there are specific use cases that conflict with pairing code function and alternate mitigating controls are available and identified."	None. Continue to make the pairing code mandatory for PIV Cards that support the virtual contact interface. Skimming protection is absolutely essential. Information about the cardholder, such as name and email address, must not be readable over the contactless interface without cardholder consent. Departments and agencies must not be permitted to distribute cards that make this information freely available. Simply requiring the establishment of secure messaging would still be making the information freely available, as the secure messaging protocol in the draft only protects against passive eavesdropping and so does not provide any access controls. If the cards make information such as name and email address freely available over the contactless interface, there are no "alternate mitigating controls" that can adequately protect the cardholder.	Noted. See resolution to comment FE-1.
FE-5		Federal Employee	G					HSPD-12 says that "it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)."	None. Continue to make the pairing code mandatory for PIV Cards that support the virtual contact interface. Per HSPD-12, the Government-wide standard must protect personal privacy. It is not acceptable under HSPD-12 to establish a standard that allows for the creation of forms of identification that do not protect personal privacy, even if the departments or agencies issuing the cards claim to have "alternate mitigating controls."	Noted. See resolution to comment FE-1.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
FE-6		Federal Employee	G					OMB Memorandum M-03-22 defines Information in identifiable form (now know as personally identifiable information) as: information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).[2] [2] Information in identifiable form is defined in section 208(d) of the Act as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." Information "permitting the physical or online contacting of a specific individual" (see section 208(b)(1)(A)(ii)(II)) is the same as "information in identifiable form." SP 800-122 also notes that name and email address are considered to be personally identifiable information.	Do not allow the pairing code to be disabled. A Federal employee who is sitting in a bar or walking down a sidewalk expects to be able to remain anonymous. That cannot happen if anyone nearby with a skimming device can read personally identifying information about that individual from the PIV Card.	Noted. See resolution to comment FE-1.
FE-7		Federal Employee	G					According to the document "Proposed Changes to SP 800-73," certificates on the PIV Card were originally PIN protected, even over the contact interface, and were only made freely available over the contact interface in order to "promote compatibility of PIV Cards with COTS smart card logon mechanisms and common applications." The document did, however, note that even making this information available over the contact interface would have some impact on privacy. Isn't this an acknowledgement from NIST that the certificates contain data that needs to be protected in order to protect personal privacy?		Noted. See resolution to comment FE-1.
FE-8		Federal Employee	G					OMB Memorandum M-05-24 states the following with respect to the specification of the PIV Card: Part 2: Government-wide Uniformity and Interoperability – Detailed specifications to support technical interoperability among departments and agencies, including card elements, system interfaces, and security controls required to securely store and retrieve data from the card.	None. Continue to make the pairing code mandatory for PIV Cards that support the virtual contact interface. Allowing some departments and agencies to disable this security control would be contrary to the M-05-24 call for "uniformity and interoperability." M-05-24 also calls for the specification (SP 800-73) to dictate the "security controls required to … retrieve data from the card." SP 800-73-4 needs to specify a uniform set of security controls required to retrieve data from the card that protect personal privacy.	Noted. See resolution to comment FE-1.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
FE-9		Federal Employee	G					"if it departments and agencies that issue the cards shall have the ability to disable this security control if there are specific use cases that conflict with pairing code function and alternate mitigating controls are available and identified."	None. Continue to make the pairing code mandatory for PIV Cards that support the virtual contact interface. While some commenters on the initial draft of SP 800-73-4 did not like the pairing code, none identified use cases that conflict with pairing code function, because there are none.	Noted. See resolution to comment FE-1.
FE-10		Federal Employee	G					FIPS 201-2 states that "Once secure messaging has been established, a virtual contact interface may be established." This clearly means that secure messaging and virtual contact interface are not synonymous and that an additional action must be taken once secure messaging has been established in order to establish a virtual contact interface. Since the pairing code is the only additional action specified in the draft of SP 800-73-4, disabling the pairing code would mean that once secure messaging was established a virtual contact interface would also be established without any further action. This would be a violation of FIPS 201-2.		Noted. See resolution to comment FE-1.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
FE-11		Federal Employee	G					"if it departments and agencies that issue the cards shall have the ability to disable this security control if there are specific use cases that conflict with pairing code function and alternate mitigating controls are available and identified." Who would decide whether "there are specific use cases that conflict with pairing code function"? Who would decide whether an "alternate mitigating control" was sufficient? If the people at an agency responsible for issuing PIV Cards believe there is no need to protect personal privacy, would these same people be able to decide to disable the security control by declaring that they had identified an alternative mitigating control (doing nothing)? If not, who would have the authority to stop them from doing this and putting all of the cardholders in their agency at risk?	If NIST decides to give departments and agencies the option to disable skimming protection then NIST must provide details about what a department or agency would be required to do to demonstrate that (1) it has specific use cases that conflict with pairing code function and (2) it has identified alternate mitigating controls. The specification must indicate who will evaluate whether the need is real and the mitigating controls are adequate, and explain what enforcement mechanisms will be in place to ensure that a department or agency cannot disable the security controls without receiving the approval of this (external to the department or agency) authority. NIST must then provide an opportunity for public comment on these processes before SP 800-73-4 goes final. Draft NISTIR 7977 claims that NIST follows the principles of "Transparency" and "Openness" as part of the standards and guidelines development processes. Making a major change this like, that would have a real and personal impact on every Federal employee and contractor, without allowing those impacted to review and comment on the change would be neither open nor transparent.	Noted. See resolution to comment FE-1
GSA-1	GSA	Chi Hickey	T	1	14	801	3.5	Footnote 10 is not very clear. It states: "As a consequence of this requirement, any keys that have to be generated on card cannot be made available over the contactless interface (including the virtual contact interface) in a dual chip implementation." In accord with §3.1.4, CAK can be on or off card. It should be clear that any key generated on card can not be copied.	"As a consequence of this requirement, any keys that **have been** generated on card cannot be made available over the contactless interface (including the virtual contact interface) in a dual chip implementation." Hence off-card injected CAK and its cert can be identical on both chips.	Resolved by adding a second sentence to the end of footnote 10 that says: "In addition, the asymmetric CAK needs to be generated off-card and loaded onto both chips for dual chip implementations."
GSA-2	GSA	Chi Hickey	T	1			3.1.2, Appx A Table 9	Both still reference TIG SCEPACS v2.2	Remove references and fully document CHUID/FASC-N in SP800-73-4. Still do not have clarity on 14 9's, zeros, etc. We should supply end-to-end CHUID and FASC-N language for 73-4. We only supplied FASC-N last time.	Addition of full CHUID/FASC-N details will be considered in next revision. See GSA-7.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
GSA-3	GSA	Chi Hickey	T	1	5	469-470	3.1.1	States: "Unused optional data elements shall be absent." This should be the rule for all data elements in all buffers defined in the PIV datamodel.	Insert at end of §3 the following text: All buffers defined in the PIV data model have tagged items that are optional data elements. Unused optional data elements shall be absent (meaning there should not be a tag present with zero length) unless explicitly specified for the container.	Declined. The language is specific to the Card Capability Container since the CCC is the only data object that allows fields to be present but to contain no value field. So, no other data objects could include data elements that are present but unused.
GSA-4	GSA	Chi Hickey	T	1	6	512-513	3.1.2	Cardholder UUID is in a free read container over the contactless interface.	Move the Cardholder UUID to the Printed Information Buffer. This appropriately protects it as PII data.	Declined. The Cardholder UUID is a randomly generated number. It needs to be available as free read over the contactless interface in order to support access control re-provisioning and/or access decision in physical access control systems. See also Federal Register Notice at https://www.federalregister.gov/articles/2013/09/05/2013-21491/announcing-approval-of-federal-information-processing-standard-fips-publication-201-2-personal
GSA-5	GSA	Chi Hickey	E	1	7	567	3.1.5	Reference to SP 800-76 is not bracketed.	Change to [SP800-76].	Accept.
GSA-6	GSA	Chi Hickey	T	1	8	596-597	3.1	States: "The following two data elements are mandatory if the cardholder has a government-issued email account at the time of credential issuance." This should be broadened to cover any issuer.	The text should be: "The following two data elements are mandatory if the cardholder has an **affiliated email address for their organization** at the time of credential issuance." This avoids "If PIV Then" logic in applications.	Declined. This requirement comes from Section 4.2 of FIPS 201-2 and cannot be changed in SP 800-73-4. Also note that the scope of this document is HSPD-12 / FIPS 201-2 (PIV), which is specific to USG only.
GSA-7	GSA	Chi Hickey	G	1					Ensure that PIV-I is not out of scope in any element of this specification because the government is a relying party of PIV-I.	Out-of-scope. The scope of this document is HSPD-12 / FIPS 201-2, in form of the PIV card, which is USG specific. PIV-I is out of scope. It would therefore not be appropriate to include the specifications for PIV-I. As noted in footnote 14 in Part 1, however, SP 800-73-4 has been written in such a way that facilitates its use in the development of data models, such as PIV-I, that are based on the PIV data model as specified in the FCIO NFI document.
GSA-8	GSA	Chi Hickey	T	1	9-10	628-670	3.3.2	The text is very precise, but difficult to read. Table 1 is very confusing using text only.	Recommend simplifying the text by using the recommended table and explanatory text in Tab "649 Table 1 Alternative". Also sugggest using an RFU Bit in the first byte to designate virtual card interface is implemented.	Resolved by edits in Section 3.3.2.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
GSA-9	GSA	Chi Hickey	T	1	11	681-682	3.3.3	States: "...the PIV Card Application contains any retired key management private keys, but may be present even if no such keys are present in the PIV Card Application." Which opens an unnecessary confusion for the relying party if the buffer is present but empty.	Recommend removing the optionality with the following language: "...the PIV Card Application contains any retired key management private keys, but **shall not be present if** no such keys are present in the PIV Card Application."	Declined. This change may not be backward compatible with issuers that may already include the Key History Object on all PIV Cards.
GSA-10	GSA	Chi Hickey	T	1	11	697-698	3.3.3	States: "The offCardCertURL field may be present if the keysWithOffCardCerts value is zero but the keysWithOnCardCerts value is greater than zero." Which opens an unnecessary confusion for the relying party if the URL is present but points to nothing.	Recommend removing the optionality with the following language: "The offCardCertURL field **shall not be** present if the keysWithOffCardCerts value is zero."	Declined. This change may not be backward compatible with issuers that may already include the URL in the Key History Object whenever the card includes retired key management keys. In addition, in many cases it will be faster to read the certificates from the URL or from a locally cached copy of the file obtained via the URL, so it may be beneficial to include the URL even if all certificates are stored within the PIV Card Application. Note that the URL would never point to nothing. See NIST IR 7676 at http://csrc.nist.gov/publications/nistir/ir7676/nistir-7676.pdf
GSA-11	GSA	Chi Hickey	T	1	11	716	3.3.3	States: "Private keys do not have to be stored within the PIV Card Application in the order of their age." Which makes it more difficult to select the key needed for the relying party.	Recommend removing the optionality with the following language: "Private keys **must be** stored within the PIV Card Application in **descending** order of their age."	Declined. This change would not be backward compatible with existing implementations. In addition, applications would not use the age of the key as the basis for selecting a retired key management key. See NIST IR 7676 "Maintaining and Using Key History on Personal Identity Verification (PIV) Cards" at http://csrc.nist.gov/publications/nistir/ir7676/nistir-7676.pdf
GSA-12	GSA	Chi Hickey	T	1	12	744-764	3.3.7	Proving the provenance of the CVC in this manner opens significant optionality that will be difficult for relying parties. Especially with regard to lines 761-764 that state this is a "temporary measure" and "will be deprecated in a future version"	A permanent solution is needed immediately that solves high speed transactions for turnstile applications. Provenance of the CVC should be tied to the CMS' self generated ECC keypair and CVC with a hash of the CVC in the Security Object. Immediately, the CVC is tied to the CMS' content-signing certificate.	Declined. See DoD-18 from the disposition of comments of the May 2013 Draft for concerns about the implementation of the proposed approach. (See http://csrc.nist.gov/publications/drafts/800-73-4/sp800_73-4_2013_draft_comments_and_dispositions.pdf)

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
GSA-13	GSA	Chi Hickey	T	1	18	854-857	5., and Footnote 13	This whole paragraph opens pandora's box for relying party options. This specification must be universal for all issuers. The federal enterprise relies on PIV-I, as such, this document should fully specify it. "A customized Part 1 data model exists in the PIV-Interoperable…"	See #2. This specification should be universal for all issuers, avoiding "If ISSUER Then…" logic in all possible ways. Let PKI Policy for issuance determine requirements around customization in using PIV technology. The paragraph could be construed to indicate PIV-I issuers need not follow Part 1, which would be catastrophic.	Resolved by GSA-7.
GSA-14	GSA	Chi Hickey	T	1	20-21	890-918, 930-944	5.1.2, 5.1.3, 5.4, 5.5	Secure messaging and VCI as described is insufficient for high speed transactions. Use of a Pairing Code that can be easily cached and distributed defeats the value of the VCI.	A permanent solution is needed immediately that solves high speed transactions for turnstile applications. A stronger means of registering a card to an application is required. Even though not mandatory in FIPS 201-2, VCI is a critical to many mobile device solutions with NFC. Mobility is an extremely high priority use case. VCI should be made mandatory.	Resolved by SCA-3. Noted. SP 800-73 does not cover 'registration'. Declined. As noted, support for secure messaging and the virual contact interface is optional in FIPS 201-2, and so cannot be made mandatory in SP 800-73-4.
GSA-15	GSA	Chi Hickey	T	1	25	968-970	Appx A, Table 8	CCC is not deprecated.	Recommend adding "CCC will be deprecated and eliminated in a future version of SP 800-73.	Declined. NIST has been advised that the CCC is still used by at least one agency and so needs to remain mandatory.
GSA-16	GSA	Deb Gallagher	Critical	1	General	General	General	GSA non-concurs with any revision of NIST SP 800-73 that offers no alternative to the “pairing code” concept as written.	GSA proposes a viable alternative that mitigates risks while providing Federal Agencies flexibility to meet their own business needs. The alternative to "pairing code" is "PIN" as long as the PIV issuer implements a separate contactless PIN counter to minimize exposure to other risks."	Resolved by resolution to comment DoD-1.
G-1	Gemalto	Y.PIN	T	2	8	469-473	3,1,1	This paragraph conflicts with the following paragraph 474-478 in that the security status will be reset no matter if selecting or deselecting. This is also good security practice of applet implementations.	behavior shall be identical to 474-478	Declined. The text in first paragraph (lines 445-449 in the version without tracked changes) has remained unchanged since the initial version of SP 800-73 (April 2005). It is also consistent with Section 2.4.2, which states that application security status indicators are set to FALSE when the currently select application changes from one application to another, but does not impose a requirement to set to application security status indicators to FALSE if the currently selected application remains unchanged (even if the SELECT command is called).

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
G-2	Gemalto	Y.PIN	T	2	8	474-478	3,1,1	More clarification is needed for global security status regarding global security setting, e.g. OCC and global PIN. Shall these global security statuses be invalidate or is the intent that any card application can reuse these authentication statuses set by the previous card application?	Clarify disposition of global security status indicators, e.g. OCC and PIN, when selecting an card application.	Declined. The referenced lines (which are lines 450-454 in the version without tracked changes) state that when the currently selected card application changes from the PIV Card Application to another application "all of the PIV Card Application security status indicators in the PIV Card Application shall be set to FALSE." Section 2.4.2 (lines 381-386) states that the security status indicator associated with OCC is an application security status indicator. Section 2.4.2 also states that the Global PIN is a global security status indicator (lines 386-387) and that global security status indicators do not change when the currently selected application changes from one application to another (lines 378-380).
G-3	Gemalto	Y.PIN	T	2	11	548-552	3,2,1	Introducing a new status SW 6A81 for access condition not met is redundant with the existing SW 6982. In addition, the SW 6A81 is already used for "function not supported." Requiring SW 6A81 to be used only in the case for VCI is impractical and overly burdensome for both the implementation of the card application and caller of the card application.	Use the same SW as everywhere: '6982'	Resolved by OT-25.
G-4	Gemalto	Y.PIN	T	2	12	604-609	3,2,1	Is tag '97' still usable in P2 of the Verify command? It seems that it is but all references have been deleted in the Verify description, except in the Note (line 606). Requiring both the primary and secondary verification for the reference '96' will degrade performance resulting in poor usabibility experience. In addition, the caller could pass the secondary print while passing reference '96' to verify the primary, yet the card application would return success because the secondary matched. It is the responsibility of the caller to the card application to manage specifically what finger to verify in the match so that it can then take the appropriate action if the match doesn't succeed.	Revert back and use 96/97 as before.	Accept to revert back to '96' and '97' as first draft.
G-5	Gemalto	Y.PIN	T	2	12	604-609	3,2,1	As current written, it's not clear what the state of the retry coutner in the event the fingerprint does not match the primary and then goes match the secondary. For instantace, the retry counter is decremented when primary match doesn't succeed and then decremented again when it does not match the secondary.	Clarify disposition of retry coutner during the fingerprint match sequences.	Resolved by G-4.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
G-6	Gemalto	Y.PIN	T	2	15	713 & 680-682	3,2,3	Allow to unblock the global PIN (if supported) with same PUK. When there are other card applications, coresident with the PIV card application, they would use the global PIN. When the global PIN is blocked, there is not way to unblock the global PIN.	Allow global PIN unblcok with the same PUK.	Noted. Global PIN management is out of scope for the PIV Card Application.
G-7	Gemalto	Y.PIN	T	2	15	713 & footnote after 684	3,2,3	There is not a method to unblock OCC.	For unblock, add codes '00', '96', and '97' for primary and secondary fingerpring to the Reset Retry Counter card command.	Resolved by HID-13 and G-6.
G-8	Gemalto	Y.PIN	T	2	14	672	3,2,2	There is not a method to update OCC.	Use the Change Reference Data to update the OCC.	Declined. There is more involved than use of the Change Reference Data to change OCC reference data. It would include updating the BIT Group template and Secure Object -- all of which requires a card management operation, rather than a user-based action. Note also that INCITS 504 specifies use of PUT DATA to change OCC reference data.
G-9	Gemalto	Y.PIN	T	2	21		4.1	The document does not decribe these values or how to update them. Therefore, it is not possible to determine how to update this information to open the secure channel.	Provide information on how to update the information, perhaps defining a container.	Declined. The values used in the key-establishment protocol on Page 21 are described in the following subsections. Information on how to update static information (e.g., the Card Verifiable Certificate) not specified since card management is out of scope.
G-10	Gemalto	Y.PIN	T	2	21	839	4.1	In step H3 of the flow diagram, both the GUID and Cicc* is returned. The Cicc could be returned instead since it contains the GUID and since the GUID is no longer being encrypted.	Either use Cicc or re-establish encryption of the GUID.	Resolved by HID-22.
G-11	Gemalto	Y.PIN	E	2	27	934	4,1,5	Not clear how the signature the computed.	Clarify the signature contained in the Cicc* is computed using the Cicc values.	Resolved by HID-22.
G-12	Gemalto	Y.PIN	E	2	22	846-848	4.1	Section 4.1 does not explain the intermediate CVC. There's no information on how to store or retrieve this intermedieate CVC. Is this stored on the card or client application data? Why is there a dedicated Table 16 that appears the same as Table 15?	Clarify the usage of the intermediate CVC.	Declined. While Tables 15 and 16 are very similar, they are not the same. Information about how to store and retrieve the Intermediate CVC is specified in Part 1 (see Section 3.3.7 and Table 42).

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
G-13	Gemalto	Y.PIN	T	2	30	981-988	4.2	The document appears to allow a clear text command to be sent during a secure channel session without breaking the current session. This ability goes against secure channel protocol practice. Typically, as soon as the card receives an unencrypted command, the secure channel is closed and the command is rejected. For most of secure channel protocols, once a secure channel session is open, all commands shall satisfy the security level of this secure channel session, otherwise the secure channel is broken and closed.	Suggest following the typical secure channel protocol and have the channel closed and command rejected when receiving an unecrypted command.	Declined. If the result of sending a command (GET DATA CAK Certificate) without using secure messaging once session keys had been established were to destroy the session keys and reject the command, then the reader could obtain its desired result by simply sending the same command twice. When the first command is received "the secure channel is closed and the command is rejected," but when the same command is sent again it would be processed. So, there would be no security benefit in requiring the command to be rejected and the session keys to be destroyed. If the access control rules allow the command to be performed without secure messaging, there is no compelling reason to reject the command just because secure session keys have been established.
G-14	Gemalto	Y.PIN	T	2	34	1083	4,2,4	Figure 2, Figure 3 and Figure 4 add a single byte '00' at the end of the command. It seems this byte is used only by the communication protocol (Le). This byte is optional in T=1 and T=CL protocols. In T=0, this byte is not supported and can cause issues (discrepency between Lc and data field length).	Revert back to previous version that does not included protocol bytes.	Declined. Section 10.4 of ISO/IEC 7816-4 requires this '00' byte (which it refers to as the "new Le field") to be present.
G-15	Gemalto	Y.PIN	T	2	37	1154	4.3	The statement that "an error occurs in secure messaging" is too vague. For example, is it a bad cipher/decipher, a bad MAC, incorrect TLV (misusing, inconsistency, additional tags, missing tag, command in clear…)?	Clarify what errors could occur at this point.	Resolved by adding a footnote stating that an error is any SW1 SW2 combo except '61 XX' or '90 00'.
G-16	Gemalto	Y.PIN	T	2	37	1158	4.3	The select and deselect will discard the session keys for security reasons.	Add deselection of the PIV application	Resolved by G-15 from the disposition of comments on the May 2013 draft of SP 800-73-4, which notes that the session key are global in scope.
G&D-1	G&D	Jatin Deshpande	t	1	20		5.1.3	This section defines that the Pairing Code cannot be changed by the cardholder. However, it would be good to allow the change for the user for different reasons: - The Pairing Code is a 8 byte random number which is not easy to memorize for the most users. The risk of blocking the Pairing Code due to wrong entries is high. - If the Pairing Code is compromized (e.g. due to leakage of the cache) the user should be able to change the Pairing Code.	Following sentenced should be changed: "The results of each random pairing code generation shall be loaded onto at most one PIV Card and cannot be changed by the cardholder." to: "The results of each random pairing code generation shall be loaded onto at most one PIV Card and can be changed by the cardholder afterwards by an individual code."	Declined. There is no expectation for the cardholder to memorize the pairing code (see Section 5.1.3 in Part 1) and the pairing code cannot be blocked (See Section 3.2.1 in Part 2, including footnote 5). See also SCA-4.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
G&D-2	G&D	Jatin Deshpande	t	1	20		5.1.3	The pairing code was changed to optional in this revised draft (3.3.2), however, for VCI it seems to be still mandatory (acc. to footnote on page 14 and 5.1.3). The pairing code shall not be mandatory since VCI might be used for other use cases beyond mobile devices where a pairing code is hardly applicable or impractical: E.g. Transport, Automation, Industrial Facilities, Logistics.	The Pairing Code shall be considered as optional for VCI. The federal agencies should be able to decide if the Pairing Code shall be used for VCI. Following sentence should be changed: "If the PIV Card supports the virtual contact interface then it shall implement support for the pairing code." to "If the PIV Card supports VCI then optinally it may require a pairing code verfication to establish this VCI."	Resolved by resolution to comment DoD-1.
G&D-3	G&D	Jatin Deshpande	t	1	20		5.1.3	It might be very useful to allow the deactivation of the Pairing Code for VCI etablishment. E.g. if an administrator has to test or check PIV cards on a set of mobile devices. Typically this is done by an administrator team in a lab. The risk of security attacks does not really exist because the tests are performed in a lab. On the other hand it would be very cumbersome to always pair a device with a card for each test.	It should be possible to deactive the Pairing Code on a PIV card. This could be realized by adding a DEACTIVE PIN command into the PIV Card Application APDU interface specification. Before this sentence: "PIV Card Issuers may choose to provide the pairing code value to the cardholder in another manner, such as printing it on a slip of paper, rather than printing it on the back of the card." Following shall be added: "The Pairing Code can be deactived on the PIV card by the cardholder. This Pairing Code required the validation of the Pairing Code."	Declined. Any tests of the PIV Card that would require establishment of a VCI would likely also require entry of the cardholder's PIN value, so the requirement to enter a pairing code in addition to PIN in these circumstances would not be very cumbersome.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
G&D-4	G&D	Jatin Deshpande	t	1	21		5.5	The pairing code shall be an optional requirement for establishing the VCI. See also comment #2	The following section: "Once secure messaging has been established over the contactless interface, a VCI may be established by the presentation of the pairing code to the PIV Card using secure messaging. Any command sent to the card using secure messaging while the security status indicator associated with the pairing code is TRUE is considered to be sent over the VCI." should be changed to: "A VCI is established once a secure messaging channel has been created over the contactless interface. This VCI may require the presentation of the pairing code to the PIV Card using this secure messaging channel. If a pairing code is required a command sent to the card through the secure messaging is only consisdered to be send over VCI if the security status indicator associated with the pairing code is TRUE. The usage of a pairing code might be required depending on the configured PIV card access conditions."	Resolved by DoD-1. Affected text will be updated.
G&D-5	G&D	Jatin Deshpande	t	2	7		Note 2	The pairing code shall be an optional requirement for establishing the VCI. See also comment #2	Following sentence: "The term VCI is used in this document as a shorthand for a security condition in which secure messaging is used AND the security status indicator associated with the pairing code is TRUE." (copied from Part 1)" Should be changed to: "The term VCI is used in this document as a shorthand for a security condition in which secure messaging is used. Depending on the PIV card access conditions this might also require that the security status indicator associated with the pairing code is TRUE." (copied from Part 1)"	Resolved by resolution to comment DoD-1. Affected text will be updated.
G&D-6	G&D	Jatin Deshpande	t	2	14		3.2.3	It should be possible to reset the retry counter for the pairing code. See also comment 8	It should be described that the retries of Pairing Code entries are limited by a retry counter. This retry counter can be reset with the PUK by using the RESET RETRY COUNTER.	Declined. There is no retry counter associated with the pairing code. See also G&D-8.
G&D-7	G&D	Jatin Deshpande	t	2	14		3.2.3	For the PIN different retry counters shall exist: One counter for contactbased interface and one counter for contactless interface. The risk of PIN retries via CL interface is much higher on the CB interface and this shouldn't block the PIV Card usage on the CB interface. A reset of the retry counters shall only be possible via contactbased interface.	Following should be added: The PIV Card has to manage a retry counter for the contactbased interface and one retry counter for the contactless interface. These retry counters shall be decremented independly from each other. RESET RETRY COUNTER resets both retry counters.	Resolved by OT-2.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
G&D-8	G&D	Jatin Deshpande	t	2	11		3.2.1	Having no retry counter for the pairing code makes the pairing code concept useless. An attacker could easily figure out the pairing code by dictionary attacks via CL interface.	A retry counter for the pairing code shall be added and following setence removed: "There is no retry counter associated with the pairing code, and so the authentication method cannot be blocked for that key reference."	Declined. The primary purpose of the pairing code is to protect the personal information on the PIV Card from being read using a skimming device. As there are 108 possible pairing code values and the pairing code is chosen at random, even if the skimming device could try 1000 pairing codes per second, it would take an average of 13.9 hours to figure out the pairing code by a brute-force attack, and in practice a skimming device would be able to try far fewer than 1000 pairing codes per second. So, figuring out the pairing code by a dictionary attack would not be easy. If the attacker had access to the PIV Card for a sufficient amount of time to perform such a brute force attack, the attacker would almost certainly be able to obtain the personal information from the PIV Card by simply inserting it into a contact card reader.
G&D-9	G&D	Jatin Deshpande	t	2				A command DEACTIVE PIN / ACTIVATE PIN shall be added to this specification which allows to temporarily disable the Pairing code. See also comment #3		Resolved by G&D-3.
G&D-10	G&D	Jatin Deshpande	t	2	13		3.2.2	It should be possible to also change the value of the pairing code with CHANGE REFERENCE DATA. See also comment 1.		Declined. See G&D-8. If the pairing code could be user selected then it would be far more vulnerable to dictionary attacks. It would also lead to confusion if the pairing code value were printed on the back of the card (as permitted by Section 5.1.3 of Part 1).
G&D-11	G&D	Jatin Deshpande	t	1	20		5.1.3	The case that several PIV cards need to be paired with a Mobile Device is not considered by this specification. It might happen that several employees share one mobile device (e.g. common department phone for traveling purpose). In this case several pairing codes has to be cached in the device. Moreover they have to be mapped to different PIV cards. This mapping could be implemented by using e.g. the Card UUID.	This section should mention that several PIV cards may be paired with a device. Moreover, it should describe how these multiple Pairing Codes for the different PIV cards shall be managed by a device. E.g. by using the Card UUID.	Declined. As noted, the system that is caching pairing code values may maintain pairs of Card UUIDs (or FASC-Ns) and pairing code values.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
G&D-12	G&D	Jatin Deshpande	t	1	20		5.1.3	This sections describes it is recommend that a client application caches the pairing code in order to avoid user promts all the time. However, it is not described that this client application should provide the user the option to remove a pairing code from the cache. But in terms of security it would be quite essential to define such a requirement (not only a recommendation). E.g. if this device is provided to another employee it must be garanteed that this paring code is deleted from the device.	We recommend to define in this section following requirement: "If the client application caches the pairing code it is required to provide the user an option to delete this pairing code from the device".	Declined. Just an a client application may cache copies of the X.509 certificates from the PIV Card without being required to provide the user an option to delete the certificates from the device there is no requirement to provide the user an option to delete the pairing code from the device.
G&D-13	G&D	Jatin Deshpande	t	2	5		2.4.3	8 digits for the pairing code is very long and difficult for users to memorize. We recommend to introduce a retry counter for the paring code in terms of security (see comment #8). By introducing this retry counter a paring code with 4 digits should be enough.	We recommend to change the length of the pairing code from 8 digits to 4 digits.	Resolved by G&D-1 and G&D-8.
HID-1	HID	Francois-Eric Guyomarc'h	Te	1	3	419-420	2.2	PIX is not incremented across different standard versions, using this information would provide an easy and fast way for the caller to identify the level of standard supported by the PIV application	Use minor version to document the standard version supported by PIV application	Declined. The version update may not be backwards compatible with fielded readers and systems.
HID-2	HID	Francois-Eric Guyomarc'h	Te	1	8	605-607, note 5	3.2.1	NISTIR7863 provides recomendations for acceptable PIN caching methods for the PIN Always rule, it should be clarified whether these recomended methods also applies to the OCC Always rule	Add a note that PIN caching methods defined in NISTIR7863 also applies to OCC methods and/or update NISTIR7863 to add recommendations for OCC Always rule	Noted. Footnote 1 in Draft NISTIR 7863 states: "FIPS 201-2 introduces the option for PIV Cards to implement on-card fingerprint biometric comparison in addition to the PIN, as a mechanism to authenticate the cardholder to the card, however, the recommendations in this document only apply to the PIN."
HID-3	HID	Francois-Eric Guyomarc'h	Te	1	12	738-744	3.3.6	It is ambiguous as to whether The Security Object enforces integrity of the Biometric template In contrast this is clearly specified for Key History, line 722.	Add a sentence, that the security object enforces integrity of the Biometric Template	Resolved by adding the following sentence to section 3.3.6: "The Security Object enforces integrity of the BIT Group Template according to the issuer." Similar text will be added to section 3.1.1 and 3.3.8.
HID-4	HID	Francois-Eric Guyomarc'h	Ed	1	12	756	3.3.7	The [COMMON] reference is not listed in the reference documents.	Add [COMMON] in the list of references.	Accept.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
HID-5	HID	Francois-Eric Guyomarc'h	Te	1	13	767	3.3.8	It is unspecified whether The Security Object enforces integrity of the Pairing code reference data container In contrast this is clearly specified for Key History, line 722.	Add a sentence, that the security object enforces integrity of the Pairing code reference container	Resolved by HID-3.
HID-6	HID	Francois-Eric Guyomarc'h	Ed	1	14	801-803	3.5	The access control conditions could be more clearly specified and aligned across different sections	It would clarify to update Table 2 to have two columns: 'Access Rule for Read on Contact interface' and 'Access Rule for Read on Contactless interface' and use the industry standard 'NEVER' ACR to indicate the container is not accessible across that interface. This would also be consistent with Table 4 For example: ACR Contact ACR Contactless Card Capability Container Always Never CHUID Always Always	Accept. Note, however, that an access rule of 'Never' will not appear in the table since all containers may be read over the contactless interface if secure messaging is used and the security status indicator associated with the pairing code is TRUE (i.e., the virtual contact interface).
HID-7	HID	Francois-Eric Guyomarc'h	Te	1	14	Table 2	3.5	It is understood that OCC is an alternative for PIN however The cardholder Fingerprints, Cardholder Facial image and Iris can't be read after OCC authentication even though they can be read after PIN presentation. Allowing OCC for these containers would opens up possible authentication use cases using multiple biometrics for instance OCC authentication of card holder followed by another PIV Bio authentication, Facial Image verification or Iris for instance. (granted Fingerprint is less relevant since it is same biometric factor)	Update the ACR column to allow reading all PIN protected containers after successful OCC authentication.	Declined. Section 4.2.3.3 of FIPS 201-2 states that: "The PIV biometric data, except for fingerprint templates for on-card comparison, that is stored on the card • shall be readable through the contact interface and after the presentation of a valid PIN; and • may optionally be readable through the virtual contact interface and after the presentation of a valid PIN." Allowing the PIV biometric data to be readable after successful OCC authentication (without requiring PIN authentication) would not be compliant with FIPS 201-2.
HID-8	HID	Francois-Eric Guyomarc'h	Te	2	5	395-396	2.4.3	Min PIN length is enforced by PIV application but nothing is stated for the padding.	Add a sentence that PIV application must also enforce padding with FF	Resolved by adding to the sentence at the end: "as well as the other formatting requirements as specified in this section."
HID-9	HID	Francois-Eric Guyomarc'h	Te	2	9	466-473	3.1.1	It is ambiguous as to wether the tag AC shall include all supported algorithms of the different PIV keys or if the AC tag is only meant to be used for the SM keys algorithms	Clarify whether response to select shall include all supported algorithms by all PIV keys or only Secure Messaging Key	Noted. It is not a requirement that other algorithms are listed in the AC tag, but it is allowed.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
HID-10	HID	Francois-Eric Guyomarc'h	Te	2	9	Table 5	3.1.1	If the intent of the AC Tag is to return all supported cyptographic algorithms (see Comment 8) It is unspecified how the caller can identify which key is bound to which algorithm.	Clarify how the caller can identify which key is bound to which algorithm returned by the select. Consider re-using object identifier tag value to reference the relevant keys as specified in Part 1, table 4	SP 800-157: Resolved by HID-9. Note: The AC tag is not designed to provide the binding between algorithm and keys. This is done through the PIV data model. See also Appendix C of Part 1.
HID-11	HID	Francois-Eric Guyomarc'h	Te	2	9	471-472	3.1.1	It is allowed that 2 different cipher suites may be returned in tag AC even though Part 1 only specifies one secure messaging key	Replace 'Tag 0xAC shall be present and indicate algorithm identifier 0x27 **and/or** 0x2E when the PIV Card Application supports secure messaging' by 'Tag 0xAC shall be present and indicate algorithm identifier 0x27 **or** 0x2E when the PIV Card Application supports secure messaging' Alternatively allow indicating as part of the response to select the identifier of the key that Cipher Suite refers to.(See Comment 11)	Resolved by OT-22.
HID-12	HID	Francois-Eric Guyomarc'h	Te	2	11	521-526	3.2.1	The standard provides two options to handle malformed PIN entries, either decrement the reference counter or not.This choice will provide a different user experience depending on choice of either behaviour by a PIV application: On several malformed PIN presentations either the card will be locked or not.	NIST shall elect one and only one option to provide a unified user experience and a common behaviour amongst PIV applications, preference goes over the most secure option(decrement reset retry counter) to avoid giving any hint to the attacker of the correctness of provided PIN format.	Declined. See XTec-4. SP 800-73-4 needs to allow the option to return '6A 80' in the case of malformed PIN entries in order to maintain backwards compatibility with SP 800-73-2 and SP 800-73-3.
HID-13	HID	Francois-Eric Guyomarc'h	Te	2	14	577-579	3.2.3	Reset Retry counter does not allow to unblock the OCC Method. FIPS 201(section 6.2.2) requires that OCC-AUTH block after a consecutive number of attempts so a method to unblock the OCC authenticator must exists	Allow OCCs references 96 and 97 to be used in RESET RETRY Command	Declined. Footnote 9 in Section 3.2.3 of Part 2 states that "The PIV Card Application may be implemented to reset the retry counter associated with OCC data when new OCC data is loaded onto the card." See also resolution to OT-57 from the first draft at http://csrc.nist.gov/publications/drafts/800-73-4/sp800_73-4_2013_draft_comments_and_dispositions.pdf.
HID-14	HID	Francois-Eric Guyomarc'h	Te	2	Table 9	678-679	3.3.1	PUT DATA is permitted on the BIT template even though neither 800-76 or 800-73 defines an interoperable format on card data (ie enrollment data) BIT will traditionally be stored at same time as minutiae template so it is questioned in what use case the PUT DATA of the BIT container will be useful if the enrollment data APDU is not standardized	Consider definition of an interopable command for biometric enrollment of OCC data(as defined in early drafts of 800-76) Consider disallowing update of the BIT container in PUT DATA.	Declined. Card management is out of scope. Disallowing update of the BIT Group template data object would be inappropriate as SP 800-73 permits all other data objects to be updated using the PUT DATA command.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
HID-15	HID	Francois-Eric Guyomarc'h	Te	2	22	Step H2	4.1.1	This steps requires full public key validation which is a time consuming process and may adverse the performance of the protocol. This is an important factor especially for PACS Use Cases It is understood from the 'NSA Suite B Implementer's Guide to NIST SP 800-56A July 28, 2009', Section B.3 that: *SP 800-56A specifies two routines to perform public-key validation: ECC Full Public* *Key Validation and ECC Partial Public Key Validation. The difference between the two routines is a check to ensure that the point has the correct order.* ***This check is unnecessary for prime-order curves, such as the curves used in Suite B. As long as the implementation under testing only claims to support the Suite B subset of NIST curves,*** *the partial validation routine will be sufficient to satisfy FIPS 140 CAVP testing of both* full and partial public-key validation capabilities.	Consider allowing partial public key validation rather than full validation given that curves are prime order curves.	Accept.
HID-16	HID	Francois-Eric Guyomarc'h	Te	2	26	753-754	4.1.5	Same as Comment 15	Consider allowing partial public key validation rather than full validation given that curves are prime order curves.	Accept.
HID-17	HID	Francois-Eric Guyomarc'h	Te	2	28	763-764	4.1.5	Same as Comment 15	Consider allowing partial public key validation rather than full validation given that curves are prime order curves.	Accept.
HID-18	HID	Francois-Eric Guyomarc'h	Te	2	30	795-797	4.2	The behaviour is unspecified if only bit 3 or bit 4 of CLA is set	Clarify if a specific status code shall be returned by PIV application if only 1 bit is specified or if secure messaging shall not be used in that case	Noted. Since PIV card application does not support variations in secure messaging, if bits 3 and 4 are not set, the card may return '68 82', secure messaging not supported, 6E 00, class not supported or similar. See Section 4.2.7 for error handling in secure messaging.
HID-19	HID	Francois-Eric Guyomarc'h	Te	2	30	815-819 and Table 2, p 7	4.2	The standard restricts the command that can be protected by secure messaging/VCI to 'non-card-management' commands but CHANGE REFERENCE DATA Other 'card managment' commands may carry sensitive data and would benefit from secure messaging/VCI security in particular we think that the RESET RETRY use case may be relevant : : It could be done offline where the PUK is entered by a user, and hence would benefit from SM protection. Note: It does not contradict FIPS 201-2 policy that states 'Any operation that may be performed over the contact interface of the PIV Card may also be performed over the virtual contact interface'.	Allow RESET RETRY COUNTER to be also optionally protected using secure messaging/VCI	Declined. See OT-6. PIN resets must be performed in conformance with Section 2.9.3 of FIPS 201-2, which requires a CMS-based mutual authenticated session (protocol) for remote reset. Providing the PUK to the cardholder to submit to the card would not be compliant with FIPS 201-2.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
HID-20	HID	Francois-Eric Guyomarc'h	Te	2	7	Note 1	3	OCC is accepted out of VCI (SM only) which is different for PIN, having this kind of exceptions makes the PIV application more complex as it has deals with different cases. In most use cases a credential needs to be read from the card after OCC authentication so will require establishment of a VCI anyway and so we do not save on performances or usability	OCC is a replacment for PIN so OCC shall require VCI as well.	Resolved by OT-13 from the disposition of comments on the May 2013 draft of SP 800-73-4. (see http://csrc.nist.gov/publications/drafts/800-73-4/sp800_73-4_2013_draft_comments_and_dispositions.pdf)
HID-21	HID	Francois-Eric Guyomarc'h	Te	2	9	Table 3	3.1.1	Tag 5F50 is unspecified	Remove unspecified tag or reference relevant standard that defines the specification of this tag.	Declined. Tag '5F50' has appeared as an optional data element in the Application Property Template with the same description since the original version of SP 800-73 (April 2005).
HID-22	HID	Francois-Eric Guyomarc'h	Te	2	21		4.1	Encrypted GUID has been removed from the standard, hence there is no point keeping the Ciic*. It can be replaced by Cicc and then the GUID needs not to be returned separately. These simplifications will optimize the algorithm and performances of the protocol	Step C1: Replace Cicc*by Cicc in the algorithm. Step C11: Remove the GUID from the reponse Step C11: Replace Cicc* by Cicc step H5: remove the step	Accept.
HID-23	HID	Francois-Eric Guyomarc'h	Te	3	4	263-269	3	The specified mechanism to identify which interface to use in not optimal as it requires to read a full certificate. Using a tag in the response to Select would be more efficient and decouples from the definition of the data model.	Add a tag in Response to select to identify the currently selected media interface. Suggest to reuse ANSI504 definition of physical interface byte tag '91'.	Declined. Adding a new parameter to the pivSelectCardApplication function would not be backward compatible with existing applications. Requiring the PIV Card to include tag '91' in the Application Property Template so that it would be returned in the applicationProperties parameter of the pivSelectCardApplication function would impose an unnecessary new requirement on PIV Cards. If the application does not have a need to read the X.509 Certificate for PIV Authentication, there are many other alternatives. The application could try to read one of the optional data objects that it will need in order to function (e.g., X.509 Certificate for Digital Signature). While these data objects are optional, this would not be an issue if the application could not perform its intended function if the object were not present. Another option would be to read the Card Capability Container, which is much smaller than the X.509 Certificate for PIV Authentication. In many cases, however, especially cases in which speed is particularly important, the application will already have another mechanism for determining whether it is communicating with the PIV Card over the card's contact or contactless interface and so will not need to rely on PIV Middleware functionality in order to obtain this information.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
HID-24	HID	Francois-Eric Guyomarc'h	Ed	3	9	Table 3	3.2.3	Reference Data format is unspecified	Add in the comment a reference to other applicable part of the standard that defines the content of the reference data for PIN, Pairing Code and OCC Data	Resolved by replacing “E.g., the PIN value” with “value of the PIV Card Application PIN, Global PIN, or pairing code as described in Section 2.4.3, Part 2, or OCC data as described in Section 5.5.2 of [SP800-76]” and by adding SP 800-76-2 to the References section.
HID-25	HID	C. Chan	T	2	32	837	4.2.2	Regarding encryption counter, NIST SP800-73-4 conflicts with GPC 2.2_D SCP03. In GP, it specifies to increment the encryption encounter regardless of whether encryption is used or not in each command & response. Should align with GPC 2.2_D SCP03.	Change from "The encryption counter shall be incremented by one after each creation of an IV to encrypt command data, and it shall be reset to its initial value after each successful completion of the key establishment protocol." to "The encryption counter shall be incremented by one after each creation of an IV to encrypt command data for each command (i.e. for each pair of command and response APDU) within a secure messaging session, and it shall be reset to its initial value after each successful completion of the key establishment protocol. No encryption shall be applied to a command where there is no command data field. In this case, the encryption counter shall still be incremented."	Resolved by changing the following sentence: The encryption counter shall be incremented by one after each creation of an IV to encrypt command data, and it shall be reset to its initial value after each successful completion of the key establishment protocol. To: The initial value of the encryption counter upon successful completion of the key establishment protocol shall be '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01'. The encryption counter shall be incremented by one after each APDU sent over secure messaging (except for the GET RESPONSE command and APDUs with a CLA of '1C'), and it shall be reset to its initial value after each successful completion of the key establishment protocol. The 16-byte IV shall be created by encrypting the encryption counter with SKENC using AES in the electronic codebook (ECB) mode of operation.
IG-1	InfoGard	SWeymann	G	2	44	1090	A.5.2.1	In existing validations, use of ECC CDH required the CAVP Component Validation List ECC CDH Shared Secret certificate. Assuming that NPIVP will require a CAVP Key Agreement Scheme SP 800-56A validation if the Secure Messaging option is supported, that validation is inclusive of the ECC CDH primitive. It should not be necessary for vendors to separately test the CVL ECC CDH primitive if the module has the appropriate complete EC DH key agreement scheme (KAS) validation. The current SP 800-73-4 draft does not address this point one way or ther other, but vendors preparing for compliance are already asking. This comment is intended to avoid future confusion.	Please include a statement in Part 2 covering this topic - Section A.5.2.1 may be the best choice. "All other procedures required to complete the key agreement are performed by the cardholder’s client application and its associated cryptographic module. Cards that support ECC CDH with the PIV KMK shall obtain CAVP CVL ECC CDH or KAS EC DH validation."	Noted. This comment will be considered as part of SP 800-78-4 since cryptographic algorithm validation testing requirements are specified in Section 7 of SP 800-78-4,

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
IG-2	InfoGard	SWeymann	T	2	43	1048	A.5.1	The function of GENERAL AUTHENTICATE with the PIV KMK with an RSA key is the SP 800-56B Section 7.1.2 RSADP operation. This operation continues to be a source of misunderstanding by CMVP reviewers in the PIV card FIPS 140-2 validations, who in the recent past required this to be described as establishing a key into the module. The purpose of the operation is key decryption; it is NOT to establish a key into the module. Please identify this operation specifically as SP 800-56B Section 7.1.2 RSADP in A.5.1 or a subsection.	At approximately line 1059: "The role of the on-card KMK private RSA transport key is to decrypt the sender's symmetric key on behalf of the cardholder and provide it to the client application cryptographic module. This operation is the RSA decryption primitive (RSADP) as specified in SP 800-56B Section 7.1.2. The RSADP operation may be used in the Approved mode provided the implementation has a CAVP validated RSADP or RSA signature implementation." [Note that the primitive described by RSADP is part of the RSA signature process. CAVP validation of RSADP is now available but it should not be necessary to separately test if RSA signature is validated.]	Resolved by IG-1.
IG-3	InfoGard	SWeymann	T	2	37	954	4.3	In similar protocols, session keys are destroyed on closure of the channel. This is a more conservative way to manage the keys, and is inclusive of the 2nd and 3rd bullets in the current draft. Also, if there is a simple error, such as an integrity failure (which could be just a transmission problem), does that really warrant key destruction?	The session keys established after successful execution of the key establishment protocol in Section 4.1 shall be zeroized in the following circumstances: + the card is reset; + the secure channel is closed for any reason, including unrecoverable secure messaging errors or a client request for new session keys (use of GENERAL AUTHENTICATE with PIV Secure Messaging key).	Declined. There is no mechanism defined to "close" a channel. No recovery mechanism exists to 'recover' from a transmission error by smart cards.
IG-4	InfoGard	SWeymann	T	2	21	708	4	FIPS 201 Section 2.9.2 is referenced but doesn't exist.	[FIPS201 Section 2.5.4]	Declined. While PIV Card Post Issuance Update Requirements were specified in Section 2.5.4 in the March 2011 Draft of FIPS 201-2, they are specified in Section 2.9.2 in the final (August 2013) version of FIPS 201-2. There is no Section 2.5.4 in FIPS 201-2.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
IG-5	InfoGard	SWeymann	T	2	6	403	2.4.3	Card enforcement of PIN policy is a good idea on the surface, but precludes use of systems with centralized PIN policy; this specification PIN policy is hard-wired onto the card, making it potentially incompatible with Global PINs for other applets. Also, the use of decimal only means that 6 digits must be used, and with that minimum, the retry count MUST be > 10 in order for cards to meet 140-2 reqiurements for authentication to the card. AS3.26 requires 1 in 100,000; the 6 decimal characters is the lowest possible value to meet AS03.25 at 1 in 1,000,000, and a counter is the only way to limit attempts in a one minute period to under 10. The decimal only limitation is presumably due to physical access control PIN entry scenarios, which InfoGard believes are rare in practice. In logical access scenarios, other characters can be used. At the system level, the minimum strength must be enforced. At the card level, this translates to a reduction in the strength of authentication in situations where physical access does not use a PIN pad. Use of physical with a PIN pad is not common, so requiring cards to enforce the character set and size weakens most systems for an unusual scenario.	Consider specifying use of a "template" or similar mechanism to allow an agency to set a policy that can be controlled by a centralized mechanism, but can be enforced by the card, and allows stronger PINs if the user has no access to anything that requires decimal only due to PIN pad use. For example, a PIN policy value might have an 8 character code where each character of the template indicates what characters are allowed for the PIN. If the decimal only limitation is retained and must be enforced by the card, then this specification should also require a 10 retry minimum; otherwise, the card cannot pass FIPS 140-2 AS03.26.	Declined. Section 4.3.1 of FIPS 201-2 states that “For PIN-based cardholder activation, the cardholder shall supply a numeric PIN.” So, both the PIV Card Application PIN and the Global PIN must be restricted to decimal digits. Since the PIN may be 6, 7, or 8 digits in length, there are actually 111,000,000 different possible PIN values, so the probability that a single random attempt will succeed is 1 in 111,000,000, far less than 1 in 1,000,000. This also means that the card does not need to limit the number of allowable retries to 10 in order to satisfy AS03.26 from the derived test requirements for FIPS 140-2. Even 1000 random attempts over the course of a minute would have a cumulative probability of success of less than 1 in 100,000.
IG-6	InfoGard	SWeymann	T	1	20	904	5.1.3	"... pairing code shall consist of eight decimal digits … "… loaded onto at most one PIV Card". Why is it necessary to limit the characters to decimal digits? This paragraph implies coordination across issuers: two different issuers are not permitted to issue the same number; how will they coordinate? With decimal only codes, the unique code space is 10^8 (100 million). Assuming ~10 million PIV card users, and potentially card reissuance, this could be problematic.	"If implemented, the pairing code shall consist of eight alphanumeric printable characters and it shall be generated at random by the PIV Card Issuer." Alternatively, if there is a strong reason for decimal only PIN, an issuer prefix could use the first character, with the remaining 7 characters decimal.	Declined. While it is unlikely that the pairing code would be needed in physical access control scenarios (see IG-5 and SCA-5), the possibility that it will be used in such scenarios cannot be entirely ruled out, so the pairing code needs to be limited to decimal digits in order to work with PACS PIN pads. The text on line 904 does not imply coordination across issues. It states that “The results of each random pairing code generation shall be loaded onto at most one PIV Card.” There was no intention to suggest a requirement to verify that “each random pairing code generation” created a pairing code value that is different from all previously generated pairing code values. If the text were changed as proposed, however, it would allow a PIV Card Issuer to randomly generate a single pairing code value and then load that same value onto every PIV Card that it issues. Random “collisions” (which are to be expected according to the birthday paradox) are acceptable, intentionally loading the same pairing code value onto multiple cards is not.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
OT-1	OT	C. Goyet	T	1	18		Table 4	If OCC can be verified over the contactless with just a SM, an attacker who does not know a card's pairing code could lock the card by establishing secure messaging and sending a few VERIFY commands with incorrect OCC values.	Change contactless security condition to use key reference value 96 and 97 from SM to VCI or use the protection mechanism described in the next comment.	Resolved by OT-2.
OT-2	OT	C. Goyet	T	1	18		Table 4	The mandatory Pairing code is raising a lot of resistance amongst the industry. Could a solution be to use the existing PIN instead of the pairing code, and add a protection mechanism to prevents an attacker from locking the card by establishing secure messaging and sending a few VERIFY or CHANGE REFERENCE DATA commands with incorrect PIN values. A simple solution easy to implement without involving the use of separate PIN Try Counters for contact and contactless, has already been successfully deployed in other smart card projects. It consists of defining an intermediate threshold value for the Pin Try Counter (PTC) and specify that when the PTC goes below that intermediate threshold (e.g. 3), all associated related commands (VERIFY, CHANGE REFERENCE DATA and RESET RETRY COUNTER) are no longer authorized over the contactless and would return status '6983' (Authentication method blocked). A successful execution of the command over the contact interface resets the associated retry counter to its nominal value (e.g. 10), thus recovering the contactless use of the command. This recovery is done by the card holder itself without requiring IT help desk intervention.	To protect PIN or OCC lockout over contactless (due to invalid PIN/OCC entry using SM), we recommend to define an intermediate threshold value for the Pin Try Counter (PTC) associated to the PIN/OCC security status and specify that when the PTC goes below that intermediate threshold (e.g. 3), all associated related commands (VERIFY, CHANGE REFERENCE DATA and RESET RETRY COUNTER) are no longer authorized over the contactless and would return status '6983' (Authentication method blocked). A successful execution of the command over the contact interface resets the associated retry counter to its nominal value (e.g. 10), thus recovering the contactless use of the command. This recovery is done by the card holder itself without requiring help desk intervention. This solution is preferred to the use of two separate PIN Try Counters, one for contact and one for contactless, as it prevents the values of the two counters to add up to increase the overall number of possible failed attempts. Besides the same threshold could apply for all reference data (PIN, Global PIN, OCC) verify using the VERIFY APDU command for cards that do not implement the pairing code required for VCI.	Resolved by defining an intermediate threshold value for the PINs and OCC retry counters. Note: Protecting the PIN from being blocked is a secondary benefit of the pairing code, but not its primary purpose. The primary purpose of the pairing code is to protect personal privacy, as mandated by HSPD-12. PIN protection of personal data on PIV Cards was considered as an alternative to the pairing code, but PIN protection would not be compatible with COTS smart card logon mechanisms and common applications.
OT-3	OT	C. Goyet	T	1	18		Table 4	Thank you for splitting Table 4 in two tables as suggested by OT-15 comment to first draft. However the second table is missing its heading and the current heading of table 4 need to be adjusted to reflect the change.	Add heading "Table 5" called PIV Card Application Key references" and change title of table 4 to "PIV card Application Reference data".	Resolved by creating 4a and 4b tables to distinguish.
OT-4	OT	C. Goyet	T	1	18		Table 4	In addition the first table should have the heading of the first column changed to read "Reference Data ID" and the second table "Key ID".	Change in table 4 the heading of the first column changed to read "Reference Data ID" and the second table "Key ID".	Resolved by changing table 4b, first column as follows. "Key Reference Value" to "Key Reference Value (i.e., Key ID)."

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
OT-5	OT	C. Goyet	T	1	18		Table 4	It is our understanding since the very first version of FIPS 201 that the PIV card application has always been considered by NIST as an application that could coexist with other applications running on the same chip. This understanding was confirmed last month by NIST response to OT-12 comment on first draft of SP800-73-4 that states: "the PIV card application is one application of possibly many and should not set global security requirements." If we all agree that the PIV card application should not set global security requirements, the key id value chosen for the Secure Messaging Key should not be taken from the range allocated by ISO to Global key IDs. Key ID value '03' should therefore not be used. Like key ids for primary and secondary fingers for OCC, the value should be taken from the range allocated by ISO for Application key references.	Use for the PIV secure messaging key a key id value reserved for PIV Card Application key references, i.e. within the range under the control of the NIST namespace. Number '80' and '81' are currently available and won't conflict with Reference Data with same ID value as Reference Data are listed in a separate table and used with the VERIFY instead of the GENERAL AUTHENTICATE command.	Resolved by OT-16 from the disposition of comments on the May 2013 draft of SP 800-73-4, which states: "The PIV Secure Messaging is intended to be a global key".
OT-6	OT	C. Goyet	T	1	18		Table 4	FIPS 201-2 states very clearly in section 4.2.2 Cryptographic Specifications, 4th paragraph that ""Any operation that may be performed over the contact interface of the PIV Card may also be performed over the virtual contact interface.". FIPS 201-2 does not make any restriction to non card management commands only. Since the security condition for use of the 9B key in contact is set to "Always" in Table 4, the security condition for use of the 9B key in contactless shall be set to "VIC" to allow a mutual authentication with key 9B to be performed over the contactless after a VCI was established, as allowed by FIPS 201-2. This is the security condition for USE of the 9B key, not for use of commands protected by the mutual authentication controlled by the 9B key. So this is NOT a request to replace a mutual authentication requirement with a VCI requirement as previously understood by NIST in response to OT-17 comment on first draft. The mutual authentication over contactless should be allowed on top of the VCI to comply with FIPS 201-2 section 4.2.2.	Set contactless security condition for use of the 9B key to "VCI" instead of "Never".	Declined. The purpose of the virtual contact interface is to permit operations performed by the cardholder to be performed over the contactless interface of the card. Operations involving the PIV Card Application Administration key (the '9B' key) are performed by the PIV Card Application Administrator, not the cardholder.
OT-7	OT	C. Goyet	T	1	18		Table 4	The same rational applies to the security condition for use of the PIN unblocking key '81'	Set contactless security condition for use of the PIN Unblocking Reference data '81' to "VCI" instead of "Never".	Resolved by OT-6.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
OT-8	OT	C. Goyet	T	1	23		Table 7	How is the container minimum capacity (bytes) computed? Since this is a minimum value, shouldn't it be set to the minimum that would allow a card to pass qualification i.e. that would allow storage of "mandatory data elements only"? Such definition would open the market to lower cost chips with less memory. The minimum capacity could also be understood as the minimum capacity that allows storage of all mandatory and optional date elements up to their maximum size. In either case, the sizes listed in this table need to be adjusted to reflect the changes in this version of SP800-73. For instance the minimum size for printed information is 190 bytes but if you add all the possible elements in table 14 you get a total of 219 bytes of data and a total of 235 bytes for the container including the tags and length. That won't fit into a 190 byte container.	Define the container minimum capacity as the minimum capacity required for a card to be validated when only mandatory data elements are stored. Update the container minimum capacity values listed accordingly.	Noted. The minimum capacity includes all optional data elements of each data object so that card stock can be created that can handle optional data elements that are personalized or left out. Container sizes will be verified and corrected where applicable.
OT-9	OT	C. Goyet	T	1	27		Table 14	Prior to the first draft of SP800-73-4, the Agency card serial number contained in the Printed Information container was defined as 10 bytes max in Text. (See table 13 from SP800-73-3 part 1). SP 800-73-4 draft defines it as 20 byte max with the same encoding type (Text = ASCII). That means that the Agency Card Serial Number has been extended from 10 to 20 digits in this version of SP800-73. This creates an issue during graphical personalization of the PIV cards as the size and font of zone 1B defined in FIPS 201-2 cannot accommodate 20 characters. If a 20 character Agency Serial Number is stored in the Printed Information data object, should that number be truncated when printed in zone 1B or is the printing allowed to extend beyond the limit of zone 1B as defined by FIPS 201-2?	Please specify that the Agency Card Serial number may not fit into FIPS 201-2 Zone 1B, and it is the agency discretion to truncate it or not.	Declined. Section 3.3.1 of Part 1 states that "All FIPS 201 mandatory information printed on the card is duplicated on the chip in [the Printed Information] data object." So, the number printed in Zone 1B of the PIV Card is the Agency Card Serial Number, and that same number shall be stored in the Agency Card Serial Number field of the Printed Information data object, if the Printed Information data object is present. If the commenter is correct that the serial number printed in Zone 1B will always be less than 20 characters (due to space limitations) then there would never be a need to truncate this number when duplicating it in the Agency Card Serial Number field of the Printed Information data object.
OT-10	OT	C. Goyet	T	1	12	740	3.3.6	It is said that the BITG shall be absent if OCC does not satisfy the PIV ACRs for command execution and data object access. However for cards that supports OCC, the BITG is a group template and is built dynamically by the card using the BIT available. If the Agency does not want to use OCC, and therefore OCC has not been personalized, there are no BIT and a GET DATA for BITG would return 7F 61 03 02 01 00 to comply with the definition of the BITG. So the data object is present but indicates that there is no BIT, which is different from an absent BITG.	Allow a BITG to be either absent or if present to indicate that there are no BIT by returning the value 7F 61 03 02 01 00. Recommend to use the discovery objet instead of the BITG to find out if OCC satisfy the PIV ACRs.	Accept.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
OT-11	OT	C. Goyet	T	1	7	547-549	3.1.3	The X.590 Certificate for PIV Authentication access over SM operations must be equivalent to contact operations or existing deployed infrastructure will be inoperable.	The PIV Authentication private key is available over the contact interface or Virtual Contact Interface. The PIV Authentication certificate is available over the contact interface, Secure Messaging (SM) or Virtual Contact Interface (VCI).	Resloved by resolution to comment # DoD-5 and DoD-1.
OT-12	OT	C. Goyet	T	1	8	601-602	3.2.1	The X.590 Certificate for Digital Signature access over SM operations must be equivalent to contact operations or existing deployed infrastructure will be inoperable.	The digital signature private key is available over the contact interface or Virtual Contact Interface. The digital signature certificate is available over the contact interface, Secure Messaging (SM) or Virtual Contact Interface (VCI).	Resolved by DoD-7 and DoD-1.
OT-13	OT	C. Goyet	T	1	8	610-611	3.2.2	The X.590 Certificate for Key Management access over SM operations must be equivalent to contact operations or existing deployed infrastructure will be inoperable.	The key management private key is available over the contact interface or Virtual Contact Interface. The key management certificate is available over the contact interface, Secure Messaging (SM) or Virtual Contact Interface (VCI).	Resolved by DoD-8 and DoD-1.
OT-14	OT	C. Goyet	T	1	12	720-721	3.3.3	The Key History Object access over SM operations must be equivalent to contact operations or existing deployed infrastructure will be inoperable.	The Key History object is only available over the contact interface, Secure Messaging (SM) or Virtual Contact Interface (VCI).	Resolved by DoD-12 and DoD-1.
OT-15	OT	C. Goyet	T	1	12	725-726	3.3.4	The Retired X.509 Certificates for Key Management access over SM operations must be equivalent to contact operations or existing deployed infrastructure will be inoperable.	Retired X.509 Certificates for Key Management private keys are only available over the contact interface or VCI. Retired X.509 Certificates for Key Management certificates are available over the contact interface, Secure Messaging (SM) or Virtual Contact Interface (VCI).	Resolved by DoD-13 and DoD-1.
OT-16	OT	C. Goyet	T	1	14-15	804, Table 2	3.5	Contact interface mode must include SM for all containers whit an Access Rule for Read that is "Always"	Update each row of Table 2 with interface mode "Contact and Secure Messaging" where the Access Rule for Read is "Always"	Resolved by DoD-1.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
OT-17	OT	C. Goyet	T	1	14	804, Table 2, Footnote 11	3.5	Define interface mode "Contact and Secure Messaging"	Add to Footnote 11: Contact and Secure Messaging means the container is accessible through the contact interface, secure messaging, and the Virtual Contact Interface.	Resolved by OT-16.
OT-18	OT	C. Goyet	T	1	9	627-674	3.3.2	References to feature as Paring Code is ambiguous	Change References from "Paring Code" to VCI	Declined. There is nothing ambiguous about the pairing code. Changing “pairing code” to “VCI” would be inappropriate, as the PIN Usage Policy provides information about reference data. The pairing code is a form of reference data. The VCI is a virtual interface that may be established through use of the pairing code. There will be a a reference to Pairing Code section 5.1.3.
OT-19	OT	C. Goyet	T	1	v	150	I. Revision History	Revision History States: "Depreciated some data elements in the CHUID (Buffer Length, DUNS and Organizational Identifier) and legacy data elements in all X.509 Certificates (MSCUID)" However throughout the document the stated changes are not apparent.	Update Tables 9 through 39; change "Optional" to "Depreciated" for each depreciated data element.	Declined. The deprecated data elements remain optional. Immediately following each of the referenced tables there is a note providing information about the data elements that are being deprecated.
OT-20	OT	C. Goyet	T	1	23	965	Appendix A, Table 7	Insure alignment with Table 2 changes. Contact interface mode must include SM for all containers whit an Access Rule for Read that is "Always"	Update each row of Table 2 with interface mode "Contact and Secure Messaging" where the Access Rule for Read is "Always"	Resolved by OT-16.
OT-21	OT	C. Goyet	T	1	23	965, Table 7, Footnote 18	Appendix A, Table 7	Define interface mode "Contact and Secure Messaging"	Add to Footnote 18: Contact and Secure Messaging means the container is accessible through the contact interface, secure messaging, and the Virtual Contact Interface.	Resolved by OT-16.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
OT-22	OT	C. Goyet	T	2	9	473	3.1.1	In your response to OT-32 comment on first draft, you've clarified the use of tag AC by saying:" The presence of algorithm identifier '27' or '2E' indicates that the corresponding cipher suite is supported by the PIV Card Application for secure messaging and that the PIV Card Application possesses a PIV Secure Messaging key of the appropriate size for the specified cipher suite." In this second draft, on line 473 it is said: "Tag 0xAC shall be present and indicate algorithm identifier 0x27 and/or 0x2E when the PIV Card Application supports secure messaging." By using "and/or" do you imply that a card could potentially support both simultaneously, i.e. be personalized with two PIV Secure Messaging Keys, one for algorithm identifier 0x27 and one for algorithm identifier 0x2E? If that is the case, don't we need to have two different key ID values in table 4 of SP800-73-4 part 1? Having two different keys value sharing the same key ID does not seem to comply with ISO 7816 standards.	Clarify whether a personalized PIV card can support both '27' and '2E' and if so, how to differentiate both PIS Secure Messaging keys if they share the same key ID.	Resolved by replacing "and/or" with "or" and by adding "but not both."
OT-23	OT	C. Goyet	T	2	12	547	3.2.1	Allowing '96' to mean '96' or '97' would prevent the application to perform two finger verifications, i.e. the verification of both the primary finger and the secondary finger, as a successful verification of the secondary finger would be enough to return a 9000 status for both verify with 96 and verify with 97 commands. As reported in NIST MINEX II, a two-finger-verification can increase accuracy of the matching, and may be needed in some cases.	Remove the possibility for fingerprint enrolled under id 97 to be successfully verified as if it was the fingerprint with id 96.	Resolved by G-4.
OT-24	OT	C. Goyet	T	2	12	547	3.2.1	The solution proposed to verify authentication data, against not only the reference data identified by the P2 parameter (e.g. '96') but also another reference data not indentified in the P2 parameter (e.g. '97'), is NOT ISO COMPLIANT!!! According to ISO 7816-4 the VERIFICATION shall be done only against the reference data specified in the P2 parameter, unless that value is '00'. But you cannot use '00' with INS '20' as it has already been allocated to the Global PIN by SP800-73 part 1.	The recommended way to perform a 1 to 2 OCC Verification compliant with ISO is to use the ISO 7816-4 VERIFY APDU with odd INS (i.e. '21') instead of even INS '20', and to put in the command data filed the Biometric Data Template ('7f2e') as defined in the latest edition of ISO 19794-2. The '7F2E' data object could contain only one sub data object, the finger minutia data with tag '81' and whose content is the sequence of minutia described in section 5.5.2 of SP800-76.	Resolved by G-4.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
OT-25	OT	C. Goyet	T	2	11	512	3.2.1	We agree that if the key reference is '96' or '98' and the VERIFY command is submitted over the contactless interface without secure messaging, then the card command shall fail. However we recommend that in this case the PIV Card Application returns the status word '6982' (Security Status Not satisfied) instead of '6A 81' (Function not supported). Because in this case the function is supported, but no SM was previously established, and the SM is a security status.	Change returned status from '6A 81' (Function not supported) to '6982' (Security Status Not satisfied) in this case, or more generally allow both status to be returned like you've allowed both '6A 80' or '63 CX' when data was not correctly formatted.	Resolved to have 2 status words: o If card supports SM and SM is not established then return 69 82 o If card does nt support SM then return 6A 81. Similar changes have been made in Change Reference Data command.
OT-26	OT	C. Goyet	T	2	13	562	3.2.2	We understand that card management commands like personalization commands are outside the scope of SP800-73. But the statement in line 562, "If any other key reference value is specified the PIV Card Application shall return the status word '6A 81'" , prevent the use of the CHANGE REFERENCE DATA for card management purposes like OCC enrollment, or Global PUK modification to name just a few. Our recommendation would be to define expected status ONLY for commands used in the context of SP800-73, and not define mandatory status that could hamper card management commands.	Remove sentence "If any other key reference value is specified the PIV Card Application shall return the status word '6A 81'" or clarify the scope of such statement to avoid conflict with card management commands.	Declined. The restriction only applies to the PIV Card Application. See also G-8. Note: The PIV Card Application data model is fixed. See http://www.idmanagement.gov/homeland-security-presidential-directive-12/faqs#t50n134 (last FAQ).
OT-27	OT	C. Goyet	T	2	14	602	3.2.2	The statement "the PIV Card Application shall return the status word '6A 81'" "prevents some card management commands to be used. Same rational as previous comment.	Remove sentence "Any other key references in P2 shall not be permitted and the PIV Card Application shall return the status word '6A 81"or clarify the scope of such statement to avoid conflict with card management commands.	Resolved by resolution to comment # OT-26.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
OT-28	OT	C. Goyet	T	2	16	647	3.2.4	The statement "If key reference '03' is specified in P2 then algorithm identifiers in P1 other than '27' and '2E' shall not be permitted and the PIV Card Application shall return the status word '6A 86'." prevents some card management commands to be used. Same rational as previous comment.	Remove mandatory check on status word that could hamper card management commands.	Resolved by OT-59 from the disposition of comments on the May 2013 draft of SP 800-73-4, which states: "Declined. If the referenced sentence were deleted, then this would leave open the possibility that an attacker could have the PIV Card perform the ECC CDH primitive with the '03' key and have the result of the primitive operation exported from the card. An attacker could use this capability to derive the session keys that were generated for a secure session and then decrypt all of the traffic that was transmitted over that session. This may also leave the PIV Card and legitimate client applications communicating with the PIV Card open to other attacks as well."
OT-29	OT	C. Goyet	T	2	32	851	4.2.2	It says "If padding is used, the first byte of the value field of tag '87' shall be '01'; otherwise, the first byte shall be '02'." However figure 1 defines a mandatory padding with '80' followed by optional zeros, so in this case the padding is always used and the padding indicator should always have the value '01'. This is compliant with ANSI 504 that states in section 9.1.1 that the cryptogram padding indicator PI value is always '01'. This is also in line with most applications (MRTD, IDL, etc) as making the padding mandatory allows to simplify the secure messaing by removing options and checks to process on both sides.	Remove mention of padding indicator = '02' as this case never happen if the data is encrypted as per figure 1.	Resolved by removing padding indicator = '02'.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
SCA-1	SCA			1	2	370	1.3	Departments must implement these recommendations no later than 12 months after the effective date of FIPS 201-2. Since SP800-73-4 is not yet final, this should be extended.	Departments must implement these recommendations no later than 12 months after the effective dates of SP800-73-4 and SP 800-85-3 and availability of vendor test/validation tools.	Declined. The effective date text in Section 1.3 was written to align with the effective date text in FIPS 201-2, which was developed in coordination with OMB. New requirements in SP 800-73-4 that must be implemented to satisfy the requirements of FIPS 201-2 need to be implemented by the date specified in FIPS 201-2. All new requirements in SP 800-73-4 have already been specified (as optional) in SP 800-73-3, so implementation of these requirements does not have to wait for completion of SP 800-73-4 or SP 800-85-3, and vendor test/validation tools are already available. Features that are new in SP 800-73-4 are optional to implement, and so the 12 month requirement does not apply to them.
SCA-2	SCA		T	1	7	562-564	3.1.4	"An Asymmetric CAK may be generated on-card, or off-card. If an asymmetrc CAK is generated off-card, the result of each key generation shall be injected in at most one PIV card." A number of issuers are issuing PIV and PIV-I cards with two separate chips. One chip is used for contact interface, a second chip is used for contactless inteface operations. (These are primarily PACS related.) Clarification is needed to avoid two different and unique values for the same card and card holder.	NIST should revisit how dual chip cards will conform to this requirement. Both chips must have the same FASC-N and UUID.	Noted. Section 3.5 of Part 1 states: “For dual chip implementations, for any container that can be accessed over both the contact interface and the contactless interface (including the virtual contact interface) the data object shall be copied into the corresponding containers on both chips.10 10 As a consequence of this requirement, and keys that have to be generated on card cannot be made available over the contactless interface (including the virtual contact interface) in a dual chip implementation” So, in a dual chip card, the same X.509 Certificate for Card Authentication (and the same Card Authentication private key) would have to be loaded onto both chips on the card.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
SCA-3	SCA		T	1	21	940	5.5	Once secure messaging has been established over the contactless interface, a VCI may be established by the presentation of the pairing code to the PIV Card using secure messaging. There are use cases where this approach would seriously affect usability (e.g., with Microsoft platforms, with transit applications). Pairing code will require creating significant new infrastructure. Card platforms must be interoperable across as many systems as possible.	We recommend an alternate method: that Secure Messaging (SM) and PIN establish VCI and Card Activation. The act of removing the card from the sleeve is an act of explicit consent to release card data. Accepting this, SM and PIN to establish VCI and Card Activation is an alternate to the mandatory use of a Pairing code.	Resolved by DoD-1. Note: The only authentication mechanisms defined in FIPS 201-2 that would require the use of the VCI if performed over the contactless interface are off-card biometric comparison (BIO and BIO-A) and authentication using the PIV Authentication certificate (PKI-AUTH), both of which require the PIN to be submitted to the card, so it is very unlikely that a transit application would make use of the VCI. NIST also consulted with Microsoft to verify that Microsoft platforms could support use of the pairing code to establish a VCI, including caching the pairing code in order to avoid usability problems.
SCA-4	SCA		T					Pairing code is cached in devices; if device is compromised, pairing codes are compromised and could require cards to be re-issued.	Need method for the user to change pairing code.	Declined. See G&D-8 and 10. If an attacker were able to get unauthorized access to a file that associated pairing code values with card identifiers (e.g., (Card UUID, pairing code) pairs), it is likely that this attacker would also obtain other information about the cardholders from the same device and so would be able to associate personal information about the cardholder (e.g., name and email address) with the card identifier (e.g., Card UUID) without the need to read this information on the card, in which case changing the pairing code would not serve to protect the privacy of the cardholder.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
SCA-5	SCA		T	1	18	865	5.1, Following Table 4	PIN lockout due to invalid PIN entry using SM SM may be perceived as additional use risk	Add an optional PIN invalid entry counter for the contact and contactless interfaces so that a blocked PIN condition on the contactless interface will not cause the contact interface PIN to be blocked. In addition, we concur with DMDC comment stating: "A PIN blocked contactless interface may be unblocked by a successful PIN entry on the contact interface. To protect PIN lockout over contactless (due to invalid PIN entry using SM), we recommend to define an intermediate threshold value for the PIN Try Counter (PTC) and specify that when the PTC goes below that intermediate threshold (e.g. 3), all associated PIN related commands (VERIFY, CHANGE REFERENCE DATA and RESET RETRY COUNTER) are no longer authorized over the contactless and would return status '6983' (Authentication method blocked). A successful execution of the command over the contact interface resets the associated retry counter to its nominal value (e.g. 10), thus recovering the contactless use of the command. This recovery is done by the card holder itself without requiring help desk intervention (i.e. PUK). This solution is preferred to the use of two separate PIN Try Counters, one for contact and one for contactless, as it prevents the values of the two counters to add up to increase the overall number of possible failed attempts. "	Resolved by OT-2.
SCA-6	SCA		T	1	14	804 Table two	3.5 Table 2	FIPS 201-2 Pg 41 state: Once secure messaging has been established, a virtual contact interface may be established. Requirements for the virtual contact interface are specified in [SP 800-73]. Any operation that may be performed over the contact interface of the PIV Card may also be performed over the virtual contact interface. SM is established automatically without PIN. Table 2 does not refect this. Always access rule is only shown as Contact	Update each line in Table 2 that say Access Rule "Always" and "Contact" to "Contact and SM "	Resolved by comment OT-20, OT-21, OT-16 and DoD-1.
SCA-7	SCA		T	1	14	Table 2 Foot note 11	3.5 Table 2	Footnote 11Contact interface mode means the container is accessible through contact and virtual contact interfaces only. Contact and contactless interface mode means the container can be accessed from any interface. This does not include SM. Add SM	Suggested text: Contact and Secure Messaging means the container may be accessed via either contact interface, Secure Messaging, or Virtual Contact Interface.	Resolved by comment OT-20, OT-21, OT-16 and DoD-1.
SCA-8	SCA		T	1	23	965	Appendix A, Table 7	Harmonize with changes in Table Two	Update each row of Table 7 that say Access Rule "Always" and "Contact" to "Contact and SM "	Resolved by comment OT-20, OT-21, OT-16 and DoD-1.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
SCA-9	SCA		T	1	23	footnote 18	Appendix A, Table 7	Harmonize with Footnote 11, Table 2	Suggested text: Contact and Secure Messaging means the container may be accessed via either contact interface, Secure Messaging, or Virtual Contact Interface.	Resolved by comment OT-20, OT-21, OT-16 and DoD-1.
SCA-10	SCA		G	1				ANSI 504 standards should be used, without presistent binding, to establish card authentication and secure messaging.	ANSI 504 standards should be used, without presistent binding, to establish card authentication and secure messaging.	Noted. See resolution to DoD-2 of first Draft, which states: "OPACITY ZKM is utilized to the maximum extent possible. Note that ANSI 504 Part 1 does not specify requirements for Subject Identifier. It is expected to be defined by an application developer. NIST continues to work on and support National standards, including ANSI 504. The changes that were made to develop the protocol that appears in Draft SP 800-73-4 were necessary in order to satisfy U.S. Government requirements for cryptographic algorithms (e.g., SP 800-56A)."
Xtec-1	XTec, Incorporated	DBC	Technical	1	1	368	1.3	This document states that departments and agencies must implement the recommendations in SP 800-73-4 no later than 12 months after the effective date of FIPS 201-2. The date should be 12 months after the date of the final version of SP 800-73-4.	Change the date to 12 months after the date of the final version of SP 800-73-4.	Resolved by SCA-1.
Xtec-2	XTec, Incorporated	DBC	Technical	1	13	777	3.4.1	This states that the UUID “should” be version 1, 4, or 5, as specified in RFC4122, Section 4.1.3. But in describing the Cardholder UUID in Section 3.4.2, it uses the verb “shall”. Shouldn’t both the Card UUID and Cardholder UUID use the verb “shall”?	Change "The UUID should be version" to "The UUID shall be version"	Accept.
Xtec-3	XTec, Incorporated	DBC	Technical	1	18	865	5.1	If the Pairing Code’s use over the contact interface serves no purpose (as specified in footnote 14), Table 4 should specify that the Security Condition for Use over the Contact Interface is “Never” and not “Always”	Change the Security Condition for Use over the Contact Interface for "Pairing Code" to “Never”	Declined. There is no compelling reason to require PIV Card Applications to block use of the VERIFY command with the pairing code over the contact interface.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
Xtec-4	XTec, Incorporated	DBC	Technical	2	11	522	3.2.1	If the authentication data in the command data field does not satisfy the criteria in Section 2.4.3, either status word 6A80 or 63CX can be returned (it's left to the applet implementer to decide which status word value to return). Instead of allowing either status word 6A80 or 63CX to be returned, only status word 6A80 should be returned. Returning status word 6A80 when the authentication data in the command data field does not satisfy the criteria in Section 2.4.3 makes the Verify command status word consistent with the status word value returned for the "Change Reference Data" command and the "Reset Retry Counter" command	Only allow status word 6A80 to be returned if the authentication data in the command data field does not satisfy the criteria in Section 2.4.3	Declined. See HID-12. See also G-10 and OT-56 in the disposition of comments on the May 2013 draft of SP 800-73-4 at http://csrc.nist.gov/publications/drafts/800-73-4/sp800_73-4_2013_draft_comments_and_dispositions.pdf
Xtec-5	XTec, Incorporated	DBC	Technical	2	16	650	3.2.4	"GENERAL AUTHENTICATE" is misspelled	Change "GENERAL AUTHENTICATICATE" to "GENERAL AUTHENTICATE"	Accept.