#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
DoD-1	DoD	Jonathan Shu	Critical	1	General	General	General	Asymmetric Card Authentication Key (aCAK): This document continues the theme from Draft FIPS 201-2 of making the aCAK mandatory for federal PIVs. The aCAK does not require user authentication so the capability exists for an arbitrary value to be signed without a user's knowledge. This certificate is intended for physical access control reader trust and transactions rather than people oriented transactions. Poorly public key enabled (PKE) applications or systems could be fooled into accepting these device transactions. Since this document requires the CAK, DoD believes the draft SP 800-73-4 does not prescribe enough standards-based protections against the ability to exploit card transactions with the aCAK.	DoD strongly recommends protections be put in place to make sure aCAK cannot be used for PKE website/unclassified network logon individual authentication or digital signing transactions. An example could be for NIST to pursue and promote an update to RFCs 5280 and 6818 to add a new "card authentication" key usage.	Declined. The profile for the Card Authentication certificate is already designed to help prevent the certificate's acceptance in environments in which it should not be accepted. The suggestion of adding a new bit to the keyUsage extension could not be accomplished through the IETF, as suggested, as the extension is defined in X.509, and past experience indicates that any attempt to add a new bit to the extension would be unsuccessful. The change would also not be backward compatible with the large base of currently deployed PIV Cards with Card Authentication keys.
DoD-2	DoD	Jonathan Shu	Critical	Gen	General	General	General	Secure Messaging: DoD and NIST have worked for over the last 4 years within the national standards community to create a standards-based, interoperability way to secure communicate with smart cards contactlessly. The result of that effort is ANSI 504 and opacity ZKM implementation. It is unclear why this document's secure messaging criteria has deviated from ANSI 504 by requiring a populated GUID with UUIDs, distribution points be within CVC, and few other provisions. These changes are unwarranted and complicate implementation in such a way that threatens interoperability between U.S. Federal government and commercial/private entities using the national standard (i.e., ANSI).	DoD strongly recommends NIST eliminates any provisions that stray from ANSI 504 Diffie-Hellman protocol within this document.	Noted. 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).

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
DoD-3	DoD	Jonathan Shu	Critical	1 and 2	General	General	General	Pairing code: This document introduces a new concept associated with secure messaging called "pairing code" that will add significant complexity and costs to agencies' PIV implementations. There is no mention of the actual risk the feature is attempting to mitigate or a comparison of alternative techniques that could be used to resolve the same issue. In the current fiscal climate, such major enhancements must come with tradeoffs so that agencies can select the best approach to meet their needs in conjunction with the level of risks they are willing to accept. NIST needs to set the requirements for security (with a justifiable rationale) and not solutions. DoD feels solutions are not standards.	Without a real conversation about risk, benefits, and alternatives for PIV issuers/relying parties (who actually own risk), DoD nonconcurs with any revision to SP 800-73 that contains a mandatory requirement for the "pairing code" concept as currently written.	Noted. Implementation of the pairing code is optional. However, data objects and keys that may only be accessed (used) over the contact or virtual contact interfaces cannot be made accessible over the contactless interface from cards that do not implement both secure messaging and the pairing code. See also OT-28 and SCA-12.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
DoD-4	DoD	Jonathan Shu	Critical	1 and 2	General	General	General	Pairing code: The concept of "pairing code" is scattered throughout parts 1 and 2 of this document without providing the following: A. An outline of the specific risk the new concept of "pairing code" is seeking to mitigate. For the last 10 years, transactions have occurred with PIVs without this new feature. Federal agencies were provided the flexibility to use other techniques (e.g., cardholder PINs and electromagnetic sleeves) to migrate any perceived risks. B. Enough sound detail about the new concept so that it can be implemented consistently across PIV issuers. It is unclear if this concept is a number physically provided by the cardholder, electronic number created by the issuer (but provided by the card), or a cryptographic process. This ambiguity has significant impact on relying parties and client applications that appear to be required to use the non-descript pairing code in processing PIV transactions over the contactless interface.	DoD strongly recommends NIST eliminate the concept of pairing code or make it optional with other similar capabilities like opacity ZKM plus aCAK and mutual authentication (i.e., Opacity full secrecy).	Resolved by DoD-3. Implementation of the pairing code is only required in order to enable new functionality of the card (e.g., reading the PIV Authentication certificate and using the PIV Authentication key over the contactless interface). Agencies that do not require this new functionality do not need to implement the pairing code. Sections 2.4.3 and 3.2.1 of Part 2 clearly explain that the pairing code is an 8 digit value that is transmitted to the card using the VERIFY command (just as with the PIV Card Application PIN and the Global PIN), and that the result of the correct pairing code being provided is to set the security status of key reference '98' to TRUE, and thus it should already be clear that the pairing code is not a “cryptographic process.” In addition, text has been added to Part 1 (e.g., Section 5.1.3) that provides additional information about the use of the pairing code. See also: G-17 and GSA-3.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
DoD-5	DoD	Jonathan Shu	Critical	Gen	General	General	General	Theme of Replacing FASCN with card or person UUID for federal issuers: This document continues the effort from NIST to blanket the standard with UUIDs that were initially intended to broaden the federal standards to be able to be used by non-Federal issuers. We believe the document has gone overboard in integrating too many capabilities that only address non-federal issuers within a federal government standard. The introduction of UUIDs appears to duplicate capabilities already inherent in the FASCN and signal a migration away from it for federal PIV issuers. We feel this choice by NIST creates a significant gap in capabilities for federal issuers and relying parties. Currently, the FASCN provides relying parties the ability to identify the card Issuer, uniquely identify the card, and uniquely identify the card holder. The card or cardholder UUIDs only provide a unique number and do not notify the relying party who the issuer is within one simple transaction. We feel this is a significant flaw with trying to accommodate non-federal issues with a standards for federal PIV issuers. A one size fits all solution does not work efficiently.	DoD Strongly recommend the document continues to require and support the use of FASCN for federal PIV issuers.	Noted. FIPS 201-2 requires the FASC-N to be populated on all PIV Cards, so there is no attempt to replace the FASC-N. The Card UUID was made mandatory in FIPS 201-2 in addition to the FASC-N based on several comments that were submitted on the March 2011 Draft FIPS 201-2. See, for example, DoD-41, which stated that "[t]he UUID must be mandatory for interoperability between PIV and PIV-I ecosystems." Similarly, several comments were received on the July 2012 Draft FIPS 201-2 requesting a mandatory cardholder UUID. While NIST declined to mandate the inclusion of a cardholder UUID, it was agreed that NIST would specify an optional cardholder UUID in Draft SP 800-73-4.
DoD-6	DoD	Jonathan Shu	Admin	1	2		1.3	PUK acronym is not provided.	PIN Unblocking Key should be spelled out the first time.	Accepted. PUK will be spelled out on its first use.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
DoD-7	DoD	Jonathan Shu	Critical	1	1 and 2	362-365	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, paring code, and PUK, 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 be provided a 24-month window to incorporate new mandatory feature.	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.
DoD-8	DoD	Jonathan Shu	Substantive	1	5 and 6	464-532	3.1.2	This document uses the terms "Card Holder Unique Identifier (CHUID)" and "Cardholder Unique Identification Number" (or as it appears cardholder UUID) to refer to two different items. These terms are too similar and it makes it difficult to understand which capability is required where.	DoD recommends using a different term to describe the cardholder UUID than "Cardholder Unique Identification Number."	Resolved by replacing “Cardholder Unique Identification Number” with “Cardholder UUID.”

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
DoD-9	DoD	Jonathan Shu	Substantive	1	5	479	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 number of cardholders like DoD are concerned that collisions will occur much sooner with 14 than 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.	Declined. This would be a non-backward compatible change with respect to existing relying parties that make access control decisions based on a 14-digit FASC-N identifier. The 14-digit FASC-N identifier allows each site to issue up to 1 million PIV Cards before needing to be assigned a new system code and provides 10 thousand system codes per agency code. This should be sufficient for even a large agency. In addition, DoD, as with other large departments, consists of many agencies, and so has been assigned a large number of agency codes in SP 800-87.
DoD-10	DoD	Jonathan Shu	Critical	1	7	549	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 strongly 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).	Declined. In response to a comment submitted on the July 2012 Draft FIPS 201-2 (DHS TWIC-11), FIPS 201-2 permits the asymmetric CAK to be generated off card. Section 3.1.4 of SP 800-73-4 states that “If an asymmetric CAK is generated off-card, the result of each key generation shall be injected into at most one PIV Card.” Section 6.1.2 of the X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework [COMMON] states that “Anyone who generates a private signing key for a subscriber shall not retain any copy of the key after delivery of the private key to the subscriber.”
DoD-11	DoD	Jonathan Shu	Substantive	1	8		3.2.1	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, as long as the software enforces explicit user action. Guidance for caching PINs can be found in [reference to the NIST information paper].	DoD recommends the SP mirrors NIST's 2012 information paper on PIV PIN caching that provides flexibility for PIN caching and support of alternative acknowledgement measures, such as pop-ups asking if the user intends to sign.	Resolved by adding a footnote that refers to NISTIR 7863.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
DoD-12	DoD	Jonathan Shu	substantive	1	8	660 and 864	3.3.2	These sections mandate the creation of a discovery object containing a URL to the CVC signer's certificate if the card supports secure messaging. This introduces an unnecessary, online validation mechanism . By requiring access to this URL to validate the CVC, the discovery object itself becomes a security related object requiring cryptographic protection and an additional validation step. Without this URL, there would be no reason to include the discovery object in the CHUID security object.	DoD recommends NIST specify that the CVC be signed with the card issuer credential, and verified with the certificate contained in the CHUID asymmetric signature. Remove the requirement for a URL to the signer of the CVC in the discovery object.	Resolved by removing the URL from the Discovery Object and by creating a new data object that will contain the certificate needed to verify the signature on the CVC. See also DoD-13.
DoD-13	DoD	Jonathan Shu	Substantive	1	10	863	3.3.2	This section states "The Security Object enforces integrity of the Discovery Object." Requiring the Security Object to include the Discovery Object component introduces significant complexities into the card issuance process without commensurate security benefit. Since this object contains addressing elements, similarly as the CCC does, its integrity should be protected in a like fashion.	DoD recommends deleting the requirement that the Security Object enforces integrity of the Discovery Object.	Declined. The Discovery Object was first introduced in SP 800-73-2 (September 2008). SP 800-73-2, SP 800-73-3, and SP 800-73-4 all say “At a minimum, unsigned data objects, such as the Printed Information data object, shall be included in the Security Object if present.” Both the Discovery Object and the Card Capability Container (CCC) are unsigned data objects, and so there has been a requirement since SP 800-73-2 for both of these data objects to be included in the Security Object.
DoD-14	DoD	Jonathan Shu	Substantive	1	11		3.3.3	This section states "The Security Object enforces integrity of the Key History Object." Requiring the Security Object to include the Key History Object component introduces significant complexities into the card issuance process without commensurate security benefit. Since this object contains addressing elements, similarly as the CCC does, its integrity should be protected in a like fashion.	Recommend deleting the requirement that the Security Object enforces integrity of the Key History Object.	Declined. See DoD-13. As the Key History Object is an unsigned data object, it is required to be included in the Security Object, if present, just as with the CCC.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
DoD-15	DoD	Jonathan Shu	Substantive	1	8	579	3.1.7	Including the Discovery Object, Key History Object and 20 Retired X.509 Certificate For Key Management Objects in the calculation of the Security Object would require the Security Object to be recalculated and digitally signed any time a change to one of those data objects is made (i.e. changing the URL in the Discovery Object or associating additional Retired Key Management Keys to the Card). While enabling post-issuance applications to change the contents of those two data objects may be desirable, permitting post issuance changes to the Security Object is less desirable to DoD due to the nature of the other information for which the Security Object enforces integrity. DoD recommends treating these objects similar to other post-issuance changeable objects (i.e. the email address in the active Key Management Cert.)	DoD recommends deleting the requirement that the Security Object enforces integrity of the Discovery Object and Key History Object.	Resolved by DoD-14.
DoD-16	DoD	Jonathan Shu	Critical	1 and 2	12 25	751-753 711-721	3.4.1 (item 3) 4.1.5	This section states, "3. If the PIV Card supports secure messaging, then the same 16-byte binary representation of the UUID value shall be used as the Subject Identifier in the card verifiable certificate (CVC), as specified in Part 2, Section 4.1.5." Adding the UUID to the CVC deviates from ANSI 504 standard protocol features without outlining the expected benefit or risk it provides.	DoD strongly recommends deleting this sentence because it adds a distinct enough value to stray from the national standard that DoD and NIST has worked to complete with industry over the last 4-5 years.	Declined. Subject Identifier is not defined in ANSI 504. It was left up to the application profile developers of ANSI 504 to decide its value. The protocol requires Subject Identifier to contain GUID. GUID is defined as UUID in PIV.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
DoD-17	DoD	Jonathan Shu	Critical	1	17	Table 4	5.1	Confusion on what VCI and SM actually mean: This table includes a column entities "Security Condition for Use" that covers the contactless interface. Terms like virtual contactless interface (VCI) and secure messaging (SM) are used to describe functions. However, it is unclear what the difference would be for these items because in other sections of the document, it appears the secure messaging is needed to use the VCI to perform various functions. A good example is that access to PINs require VCI and biometrics SM. This does not make sense because we feel the PIN should be protected when sent contactlessly from the card.	DoD strongly recommends NIST cleans up the use of VCI and SM throughout the document to be consistent and eliminate any confusion.	Resolved by adding the following to the end of footnote 7 in Part 1: “The term virtual contact interface 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.” In addition, the following sentence will be added after the first sentence in Section 5.5 of Part 1: “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.”
DoD-18	DoD	Jonathan Shu	Critical	1	19		5.1.2	DoD has significant concerns with the requirements for the content and construction of the CVC as outlined in this document. Currently, DoD creates and digitally signs all PIV objects prior to encoding. This document appears to mandate that other actions take place on the card (i.e., ECC key generation, CVC creation, and CVC signing) before other PIV objects (particularly the discovery object and the security object) can be completed. Several back and forth transactions with DoD's certificate signer would be necessary that do not exist today. This very prescriptive requirement will force major changes and complicate the efficiencies DoD has established in our card issuance process.	DoD strongly recommends NIST remove CVC information from the other PIV objects like the Discovery Objects and Security Objects. This will provide PIV issuers more flexibility and allow them to construct the CVC without major modification to existing PIV issuance architectures.	Resolved by DoD-12.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
DoD-19	DoD	Jonathan Shu	Substantive	1	19	863	5.1.2	If the content signing certificate used to sign the CVC is the same as the content signing certificate that was used to sign the CHUID, making the content signing available via a URL is an unnecessary and burdensome element to manage and maintain. Also, checking the discovery object and hitting an external URL to obtain the same signing public key that is available on the card in the CHUID container will introduce unnecessary latency into the secure messaging operation.	DoD recommends NIST make the publication of the content signing cert via a URL contained in the discovery object optional if the certificate used to sign the CVC is the same as the one required to be included in the CHUID container as per FIPS 201 and section 3.1.2 of SP 800-73-4.	Resolved by DoD-12.
DoD-20	DoD	Jonathan Shu	Critical	1	20	891-895	5.5	Before PIN protected information can be sent over the contactless interface, this section requires a pairing code transaction be executed after the ANSI 501, Diffie-Hellman secure channel is created with the contactless interface of the card and a system. The pairing code is used after a Secure Messaging session has been established which already has "data confidentiality and integrity" protection. Pairing code does not serve to establish a persistent trust relationship between a card and a terminal but must be entered each time a terminal is encountered. From a usability standpoint, requiring the user to remember and enter multiple PINs will be confusing and inevitably lead to more blocked cards. The specification does not provide a key reference for a pairing code unblocking key; resetting the retry counter; whether changing the reference data is allowed for the pairing code; nor prescribing the impact of entering too many unsuccessful pairing verification attempts.	DoD strongly recommends this specification more closely mirror ANSI 504 and either remove pairing code or make this feature optional rather than required. Risks are owned by federal agencies and they should have the flexibility to mitigate them with the techniques they deem necessary.	Declined. Access control rules for data objects and keys are not addressed by ANSI 504. So, including a requirement for a pairing code as an access control condition is not a failure to “more closely mirror ANSI 504.” See also SCA-12. Noted. DoD is not required to implement the virtual contact interface, and may continue to require operations that are currently restricted to the contact interface to be performed over the the contact interface. Section 3.2.1 of Part 2 has been modified to indicate that there is no retry counter associated with the pairing code and so its use cannot be blocked as a result of successive unsuccessful attempts. In order to mitigate the risk of brute force attacks there is now a requirement that the pairing code be an 8-digit number created at random by the issuer. Part 1 now includes a new Section 5.1.3, which addresses usability issues with respect to the pairing code. See also GSA-3.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
DoD-21	DoD	Jonathan Shu	Admin	1	27	950	Appendix A, Table 18	Tag 0x5F2F is incorrectly listed as 3 bytes.	Change max bytes for PIN usage policy to 2.	Accept.
DoD-22	DoD	Jonathan Shu	Substantive	1	32	993	Appendix A	Why is the IsX509 for retired certificate being set to 0 which normally means false when the certificates will be x509?	It is our belief that if the encryption key certificate is a x509 certificate the IsX509 value should be 1.	Declined. Draft SP 800-73-4 requires the IsX509 bit of CertInfo to be 0 in every certificate data object, not just the retired certificates. This requirement has remained unchanged since SP 800-73, which was published in April 2005. Changing the requirement now would be non-backward compatible without any counterbalancing benefit.
E-1	Entrust	SB	G	1	7	561	3.1.7	The ICAO Document that is referenced [MRTD] has been superseded and is no longer available	Update referenced document [MRTD] to " *ICAO 9303 Machine Readable Travel Documents Part 3: Machine Readable Official Travel Documents, Volume 2: Specifications for Electronically Enabled MRtds with Biometric Identification Capability " 2008.* The document is available at: http://www.icao.int/publications/pages/publication.aspx?docnum=9303 Section IV is "PKI for machine readable travel documents offering ICC read only access". Also the Appendix that is likely the correct specific references to replace those in 3.1.7 is Appendix 3 (Normative) to Section IV - Document Security Object	Accept. SP 800-73-4 will be pointing to the 2008 ICAO Document and reference Appendix A/A3.1/A3.2 instead of C, where applicable.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
E-2	Entrust	SB	T	1	19	861	5.1.2	It seems rather confusing to issue a card-verifiable certificate for the card's public key for secure messaging, but an X.509 certificate to verify the signature on that CVC. A relying party would need to mix the validation processes for two separate PKI technologies in order to verify the key	Consider also a CV certificate to verify the signature on the current CVC, along the lines adopted by the EU for the Terminal Authentication Protocol used in their eMRTD Extended Access Control, as documented BSI TR 03110 found at: https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03110.html	Declined. SP 800-73-4 needs to specify a mechanism for validating CVCs that is interoperable for all PIV and PIV-I cards. Use of the existing X.509-based Federal PKI to distribute CVC trust anchors avoids the need to establish a new, but similar, CVC-based PKI infrastructure. In the case of physical access control systems, it is believed that in most cases the relying party will simply verify the signature on the CVC received from a card using a key that it has previously obtained in a trusted manner. The X.509 infrastructure will only be used by card registration systems in exception cases when a new CVC signing key is encountered – the new key would then be verified and pushed out to the relying party systems.
E-3	Entrust	SM	T	2	26	737	4.1.8	The command syntax specifies that Le should be absent. However, since the response to the command defined at line 739 does contain a data field, Le should normally have been provided in the command. Otherwise, the PIV Card will return only status 61xx and require another message exchange.	Le's value should be specified as "length of expected response" or an explanation given for why it is preferable to exclude it.	Resolved by specifying Le's value as '00'.
E-4	Entrust	SM	T	2	44	1104	A.6	As explained in Entrust Comment #3, an Le value should be sent in the GENERAL AUTHENTICATE command in the example.	Add an Le byte to the command.	Accept

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
E-5	Entrust	SM	T	2	20	678	4	The phrase "that may be subsequently used to protect the communication channel between the two parties" suggests that even after the secure messaging key establishment has been performed, commands not protected by secure messaging can be interspersed with commands that are protected. Is this the intent? Has consideration been given to requiring use of secure messaging once key establishment has been completed? This would provide greater protection in some man-in-the-middle scenarios. It may then be desireable to allow all commands except SELECT to be sent with secure messaging (instead of only those commands specified at page 27 line 768). The commands accessible over the VCI could still be restricted.		Declined. It is up to the client application to determine whether to use secure messaging with each command that it sends to the card. Requiring that once secure messaging has been established, the card must reject any command that is sent without secure messaging would be non-standard. Other than the SELECT command, Draft SP 800-73-4 already allows all commands that may be performed within the PIV Card Application, except RESET RETRY COUNTER, PUT DATA, and GENERATE ASYMMETRIC KEY PAIR, to be performed using the secure messaging protocol specified in the document. The commands (other than SELECT) that cannot be performed over the secure messaging protocol specified in SP 800-73-4 are card management operations, which would need to be performed in a manner that satisfies the requirements of Section 2.9.4 (PIV Card Post Issuance Update Requirements) of FIPS 201-2.
E-6	Entrust	SM	T	2				Has any consideration been given to the addition of a command for key import? Key import is required to support the escrow of encyption keys.		Resolved by G-12.
ES-1	Electrosoft Services	Jason Mohler	T	2	11	507	3.2.1	When key references 00 and 80 are used with the verify command over the contactless interface, with or without SM, the card will return 6A 81 in both instances. It would be helpful to return different status words for instances where key references 00 and 80 are sent with the verify command over the contactless interface with or without SM. Returning separate and distinct status words for these two scenarios will afford developers and implementers better insight into error conditions associated with the verify command.	Return different status words for instances where key references 00 and 80 are sent with the verify command over the contactless interface with ('69 85' conditions for use not satisfied) and without SM ('6A 81' Function not supported). An applicable return code will need to be added to the pivLogIntoCardApplication in part three as well.	Declined. Separate status words would not afford developers better insight into error conditions, as an application should not have to rely on the status words returned by a command to know the current security status of the pair code. Furthermore, there are far too many different scenarios that could result in a command not executing successfully to assign different status words to each scenario.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
G-1	Gemalto	Y.PIN	ed	1	4		3,1,1	need reference for GSC-IS (version number, etc etc)		Noted. A reference to GSC-IS already appears in the References section (Appendix E).
G-2	Gemalto	Y.PIN	ed	1	7		3,1,6	is it possible to describe which image format is used? (jpeg, jpg2000, …)?	Suggest jpeg.	Resolved by adding a reference to SP 800-76.
G-3	Gemalto	Y.PIN	ed	1	12		3,3,9	What is the specification reference for iris image (file format, matching algorithm, ..)? Without this information, the card will not be able to perform the OCC feature for the iris image.		Resolved by adding a reference to SP 800-76. SP 800-73-4 does not permit on-card biometric comparison (OCC) using the iris image.
G-4	Gemalto	Y.PIN	te	1	15	last sentence	4,1,1	a data object not initialized shall be set with a zero length value. This statement needs to be replaced with the suggested changed to be inline with existing standards (e.g. ISO) with regard to lifecycle state of data objects.	Define a life cycle state for data objects that follows the object life cycle state as defined by ISO (OPERATIONAL ACTIVATED, OPERATIONAL DEACTIVATED, CREATED) CREATED: object is created, but the data are not yet populated or data have been deleted ACTIVATED: object is created and data populated DEACTIVATED: when the object is not fully populated (a put data chaining used to populated the object is aborted) this could also applies to other objects like keys.	Resolved by changing the referenced sentence to: Before the card is issued, data objects that are created but not used shall be set to zero-length value.
G-5	Gemalto	Y.PIN	te	1	17	last sentence	table 4	It's not clear how these access conditions apply to actions that can be performed with those objects. For example, looking at the PIV Card Application PIN and the Always condition for contact, then it's not clear if that condition applies to unblocking the PIN and change reference data.	Specify the access conditions for each action that could peformed on each object (put data, get data gen key pair, general authenticate).	Resolved by adding the following reference to Table 2 of Part 2 to the end of Line 830 in Part 1: “Table 2 of Part 2 specifies the security conditions for each command.”

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
G-6	Gemalto	Y.PIN	te	1	17		table 4	The middleware and reader need confidentiality in exchanging commands with the card.	Support optionnally SM (SCP03 using global keys/OPACITY using local keys) in contact/contactless for any command that does not mandate SM or VCI	Declined. Symmetric key based SM protocol was not used since it is not likely to be interoperable across Federal government agencies. Also, adding more options without apparent benefits makes product testing and system implementations much more complex.
G-7	Gemalto	Y.PIN	te	2	5	second paragraph	2,4,3	The document is not sufficiently precise when talk about pin/puk length. For instance, in line 406 the bytes sent to the card command interface may only be 0x00-0xFE yet in line 397 the document states the bytes sent to the card command interface include 0xFF. These statements conflict.	Distinguish pin length with padding and pin length without padding. For instance, use the wording "pin length with padding" and "pin length without padding."	Noted. Section 2.4.3 in Part 2 states: "The pairing code shall be exactly 8 bytes in length and the PIV Card Application PIN shall be between 6 and 8 bytes in length. If the actual length of PIV Card Application PIN is less than 8 bytes it shall be padded to 8 bytes with 'FF' when presented to the card command interface". (PIV Card Application PIN / pairing code) Section 2.4.3 in Part 2 also states: "The PUK shall be 8 bytes in length, and may be any 8-byte binary value. That is the bytes comprising the PUK may have any value in the range 0x00 – 0xFF." (PIN Unblocking key) The PIV Card application PIN may be padded. The pairing code PUK may not be padded. Line 397, which refers to sending a padding PIV Card Application PIN to the card command interface, does not apply to the PUK.
G-8	Gemalto	Y.PIN	te	2	12		3,2,1	It's common practice in industry for the user interface to display the number PIN attempts remaining when a PIN attempt failed. This provides the user additional feedback to manage their future PIN attempts. Another is to verify the reset/retry counter for verification purposes in validating the pre-presonalization from vendors.	add the support of iso command verify pin with lc=0 and the card returns the retry counter of the pin with neither reseting the security status nor decrementing the retry counter	Noted. Support for this option has been included since SP 800-73 (April 2005). See footnote 5 in Draft SP 800-73-4 Part 2 (footnote 7 in Revised Draft SP 800-73-4 Part 2).

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
G-9	Gemalto	Y.PIN	te	2	11	9th paragraph	3,2,1	in part 2: in verify command, if format defined in 2.4.3 is not satisfied, the command shall fail, the sw is 6A80 and the security status and counter are unchanged. This is different from industry practice where the retry counter is decremented when the command fails no matter the reason.	proposal: In verify command, if the pin length with padding is not 8, ok to reject the command but the counter is not decremented because this is an APDU format issue. In the remaining scenarios that follow, the counter is decremented because it falls in the "pin check" category that includes format issues. If the pin length without padding is not between 6 or 8 for pin/global pin or if the puk length without padding is not 8, the command shall be rejected, but the retry counter shall be decrement and the security status shall be reset for security reason. Same remark if the pin/global pin value is not composed of 30-39 digits. it shall be seen by the card as a bad pin presentation so the security status shall be reset and the retry counter shall be decremented.	Resolved by changing the 9th paragraph (10th paragraph in the Revised Draft) to the following text: If the key reference is '00' or '80" and the authentication data in the command data field does not satisfy the criteria in Section 2.4.3 then the card command shall fail and the PIV Card Application shall return either status word '6A 80' or '63 CX'. If status word '6A 80' is returned, the security status and the retry counter of the key reference shall remain unchanged(6). If status word '63 CX' is returned, the security status of the key reference shall be set to FALSE and the retry counter associated with the key reference shall be decremented by one. Footnote 6: It is recommended that in this case the authentication data not be compared to the on-card reference data. Also modify paragraph 11 (now paragraph 12) as follows: If the key reference is '00', '80', or '96' and the authentication data in the command data field is properly formatted (see previous two paragraphs) and does not match reference data associated with the key reference, then the card command shall fail. If the card command fails, the PIV Card Application shall return the status word '63 CX', the security status of the key reference shall be set to FALSE, and the retry counter associated with the key reference shall be decremented by one.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
G-10	Gemalto	Y.PIN	te	2	13	5th paragraph	3,2,2	in part 2: if either the current reference data or the new reference data format is not correct, the command is rejected and security status and retry counter are unchanged	in CRD command, if the format of the new pin value is not correct, the command shall be rejected and the security status and retry counter shall remain unchanged, but if the current pin value is not in correct format (length/value), the command shall be rejected and the security status shall be reset and the retry counter shall be decrement. This is to be in sync with the previous comment #9 regarding the PIN format and counter.	Resolved by allowing either '63 CX' or '6A 80' in the case that the authentication data is incorrectly formatted.
G-11	Gemalto	Y.PIN	te	2	14	3rd paragraph	3,2,3	Similar to comments #9 and 10. As written, a bad format for current PUK shall reset security status and decrement retry counter.	Only the padded PUK length shall be verified without decrementing the retry counter and without reseting the security status. The new PIN value format shall be checked without decrementing the RETRY COUNTER.	Resolved by OT-40, which removes any formatting requirement for the PUK and by allowing either '63 CX' or '6A 80' to be returned for the cases in which the PUK is incorrect and the new PIN is incorrectly formatted.
G-12	Gemalto	Y.PIN	te	2	17		3,3,1	There is an industry need for a non-proprietary methods for a CMS to manage keys on the card.	Define the put data command to manage keys (symm or asymm) to update the key value. It is an issue for CMS to support proprietary solution that are card manufacturer dependend.	Declined. Any attempt to specify a standard for loading keys onto the PIV Card would be not be backwards compatible with some PIV Cards.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
G-13	Gemalto	Y.PIN	te	2	27	3rd paragraph	4,2,3	If secure messaging is applied first and then the result is split and sent in chaining the APDU command is impractical for on-card memory resources and performance, it can cause some memory trouble as big internal buffer shall be used to store the complete datafield. The technique as specified conflicts with GlobalPlatform's support for secure messaging where each APDU is encrypted seperately to avoid these problems.	Define the minimum chaining length that could be used with secure messaging. Compute the secure message for only one command at a time and not for the complete payload. If you prefer not to follow GlobalPlatform's lead, then define the minimum length that shall be supported by the card for chaining with secure messaging.	Declined. While GlobalPlatform proprietary secure messaging may compute secure messaging separately for each APDU, ANSI 504 specifies a requirement to "compute secure messaging on the entire message before command fragmentation for data transportation." This is consistent with ISO/IEC 7816-4, which permits secure messaging to be applied before fragmentation. There is no need to specify a minimum length that shall be supported for commands sent with secure messaging, as the length of a command data field that may be sent under secure messaging is already limited. Section 4.2 of Part 2 notes that only GET DATA, VERIFY, CHANGE REFERENCE DATA, and GENERAL AUTHENTICATE may be performed using the secure messaging mechanism defined in SP 800-73-4. Of these only VERIFY and GENERAL AUTHENTICATE permit the use of command chaining. The length of the VERIFY data field is limited by the number of minutiae sent to the card (see Section 5.6.2.1 of SP 800-76-2) and the length of the GENERAL AUTHENTICATE data field is similarly limited (see Appendices A.3 and A.6 of Part 2). Note that Card Management APDUs do not use this secure messaging protocol and therefore could use GP. There is also no need to specify a minimum length that shall be supported for response chaining, and there is no requirement for cards to use a big internal buffer, as the data may be transmitted from the card as it is generated. There is no requirement for the card to encrypt and compute a MAC over the entire command payload before beginning transmission of the response.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
G-14	Gemalto	Y.PIN	te	2	29	3rd paragraph	4,2,2	The status word is not specified if the padding indicator is incorrect. In addition, it's unclear if the status indicator must be reset.	Clarify the card behavior if the padding indicator is different from 01 or 02. Perhaps this would be 6988. Clarify the disposition of the status indicator in these situations.	Declined. Section 4.2.7, Error Handling, specifies errors that could take place during secure messaging.
G-15	Gemalto	Y.PIN	te	2	27		4,3	Missing a circumstance.	The PIV application is reselected or another application is selected.	Declined. The PIV Secure Messaging key and the session keys established as a result of performing the key establishment protocol in Section 4.1 of Part 2 are global in scope and so there is no requirement to destroy the session keys when the PIV application is reselected or another application is selected.
G-16	Gemalto	Y.PIN	te	2	30	figure 2	4,2,3	In the case of chaining, it's not clear if the chaining bit of the class byte is masked.	Clarify if the chaining bit is masked or not.	Declined. While the comment does not explain what it means for the chaining bit to be "masked," both Figure 2 and Step 2 in Section 4.2.3 specify that a CLA byte of '0C' shall be used for the computation of the C-MAC. Furthermore, the second sentence of the first paragraph of Section 4.2.3 says "In the case that fragmentation is required for data transmission, the command shall be constructed without fragmentation for the purposes of computing the MAC, and the CLA byte used in the computation of the MAC shall be '0C'."
G-17	Gemalto	Y.PIN	te	general	general			The definition of the pairing code is incomplete.	Clarify the usage of the pairing code, user experience, and use cases. For instance, will the pairing code need to be entered each time or could the middleware cache the pairing code? Is there a try counter associated to the pairing code?	Resolved by adding a new Section 5.1.3 to Part 1 which addresses information about user experience and caching and by modifying Section 3.2.1 of Part 2 to remove the retry counter for the pairing code.
G-18	Gemalto	Y.PIN	te	general	general			try counter of pin/puk are not described	Detail the try counter for a PIN/pin unblock code.	Declined. The details of the retry counter is defined in each corresponding section.
G-19	Gemalto	Y.PIN	ed	general	general			The lack of a corresponding FIPS 201-2 draft of final does not provide sifficient context to adequately review these drafts	Publish an updated draft or final FIPS 201-2 that serves as the base for these special publications.	Accept

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
GSA-1	GSA - FICAM Testing Program	Chi Hickey	Technical	1	7	549-551	3.1.4	SP 800-73-4 Part 1 Draft, as currently written, allows PKI-CAK keypair to be generated off-card and injected into the PIV card. As written, this provides the ability for dual-chip cards to have the same PKI-CAK keypair and certificate on both chips. This is in conflict with FIPS 201-2 dated 5_31_12. Line numbers 1607-1608 page 59 section 4.2.2 requires the PKI-CAK keypair to be generated on card. In a dual-chip scenario, this mandates that each chip will have a unique and different PKI-CAK keypair.	This conflict must be resolved. The FICAM Testing Program recommends altering FIPS 201-2 to be consistent with SP 800-73-(3&4) Part 1, enabling off-card generation of the PKI-CAK keypair. This resolves a significant impact to E-PACS solutions, including: dual registration of PIV cards (once by contact, once by contactless), management of two PKI-CAK certificates with the same UUID/FASC-N, and performance at time of access (no decision time required to figure out which key is involved). The FICAM Testing Program will gladly discuss this issue with NIST as requested.	In response to a comment submitted on the July 2012 Draft FIPS 201-2 (DHS TWIC-11), FIPS 201-2 permits the asymmetric CAK to be generated off card. In addition, SP 800-73-4 will specify that any data object and keys that are available over both contact and contactless chip interfaces shall be the same. A footnote (to the additional text) will note that keys that have to be generated on-card cannot be made available over the contactless interface in dual chip implementations.
GSA-2	GSA - FICAM Testing Program	Chi Hickey	Technical	1	8-10	633	3.3.2	There is no discovery mechanism available to determine if a PIV card is dual-interface or dual-chip.	Add an entry to the Discovery Object to clearly denote if a PIV card is dual-interface or dual-chip.	Declined. A conformant PIV Card should behave exactly the same way regardless of the dual-interface or dual-chip configuration on the card. The host connects over contact or contactless interface and will only be able to perform actions allowed over the interface. So, adding discovery of card configuration is unnecessary and there is no standardized tag in ISO/IEC 7816 for this discovery.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
GSA-3	GSA - FICAM Testing Program	Chi Hickey	Technical	Part 1 and Part 2				NIST SP 800-73-4 provides many broad and far reaching variations in the specification. The magnitude of variations severely impacts relying party systems in complexity of leveraging PIV cards in interoperable solutions.	NIST should initiate a working group on this issue. The FICAM Testing Program recommends the working group include ICAMSC and current issuers. The objective is to reduce valid variations across all fields based on current issuer practices. If issuers are not doing it today, options remaining should be deprecated/illegal. The FICAM Testing Program recommends SP 800-73-4 should not be released until this analysis is complete and the specification is updated accordingly.	NIST has extensively worked with FICAM TP on the subject. The results are reflected in the Revised Draft, are documented in GSA-3a through GSA-3c, and are made available for agencies to comment.
GSA-3a	GSA - FICAM Testing Program	Chi Hickey	Technical	1		471	3.1.2	The Buffer Length field is redundant.You must read the whole CHUID using GET DATA and will know the buffer length after reading it.	Deprecate the Buffer Length field.	Resolved by deprecating Buffer Length in SP 800-73-4.
GSA-3b	GSA - FICAM Testing Program	Chi Hickey	Technical	1		493	3.1.2	The Organizational Identifier and DUNS fields in the CHUID are rarely, if ever, used, and add no value.	Deprecate the the OI and DUNS fields.	Resolved by deprecating OI and DUNS in SP 800-73-4 revised draft.
GSA-3c	GSA - FICAM Testing Program	Chi Hickey	Technical	1				The MSCUID is legacy and should be removed.	Remove MSCUID from tables 10, 15, 16, 17, 20-39.	Resolved by deprecating the MSCUID in SP 800-73-4 (tables 10, 15, 16, 17, 20-39).

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
HID-1	HID	Francois Eric Guyomarch	Te	1	10	657-661	3.3.2	Support of secure messaging is bound to the presence of CVC root URL. Root certificates may distributed differently than URL mechanism(Push Software mechanismes, pre-installed on OS, etc..)	Use a separate tag to indicate that secure messaging is supported rather than require the presence of CVC root URL tag. Make root CVC tag optional to accomodate for different deployment models.	Noted. The presence of cryptographic algorithm '27' or '2E' in tag 'AC' of the Application Property Template in response to the SELECT command indicates SM implementation. Declined. There is a requirement for an interoperable mechanism for relying parties to obtain the public key needed to verify the signature on the CVC. This does not preclude the existence of other methods for distributing these keys, and relying parties do not need to use the mechanism provided for in the standard if they have access to the public key by some other means. See also DoD-12.
HID-2	HID	Stephane Ardiley	Te	1	16	812-813	4.3	Table 3, doesn't give any reference to the CVC attached to the PIV Secure Messaging Key. It means we cannot read the CVC from the GET DATA command (as we read the certificate for any other key). Don't we want to read the CVC from the GET DATA command in some situations (and not only from the GENERAL AUTHENTICATE command with PIV Secure Messaging?		Declined. There is no need to obtain a copy of the Card Verifiable Certificate (CVC) through a means other than in the response to the key establishment protocol.
HID-3	HID	Francois Eric Guyomarch	Te	1	18	Table 4	5.1	Card Authentication key is "Always" on Contactless interface, this means card authentication can not benefit from security provided by SM/VCI interface	Suggest that VCI / Secure Messaging can be optionally used to protect access to 9E key	Noted. Section 4.2 states that the GENERAL AUTHENTICATE command may be performed over secure messaging, so the GENERAL AUTHENTICATE command may be performed over secure messaging using the '9E' key. However, PIV Cards must permit the GENERAL AUTHENTICATE command to be performed with the '9E' key over the contactless interface without secure messaging.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
HID-4	HID	Stephane Ardiley	Te	1	20	880-881	5.3	Table 5 only references ECC 256 and 384 for the approved key sizes. For demanding applications (like physical access control using PIV Secure messaging), we should benefit from using ECC 224 bits too. ECC224 is also approved as part of 800-131A and also FIPS140-2	Suggest to add support for ECC 224 (as well as in new version of 800-78) and increase performance during key establishment protocol for the PIV card Application	Declined. NIST has previously received comments requesting that the number of permitted curves be reduced. It is for this reason that only the two curves from NSA's Suite B are permitted. See also GSA-3.
HID-5	HID	Francois Eric Guyomarch	Te	1	20	892	5.5	The establishment of a VCI requires the presentation of a pairing code prior to use. This may adversely impact usability as the pairing code must be presented each time prior to use the card in Contactless mode. This is particularly relevant for PACS use cases where it is less conventient for users to enter pairing code on several PACS readers/Hosts and where fast establishment is important factor	The standard should document whether it is acceptable that the host caches the pairing code for subsequent use to minimize usage impact or consider a policy where pairing code needs only to be presented once per host rather than each time The specification should also specify how pairing codes are managed and distributed, and eventually renewed.	Resolved by adding additional information about the use of the pairing code in Section 5.1.3 of Part 1, including that it may be cached by hosts for subsequent use. See also G-17. It would not be possible to create a policy where the host only needs to present the pairing code to the card once. Since the secure messaging protocol in SP 800-73-4 does not provide any host-to-card authentication, the card could not distinguish a host that had previously established a VCI with the card from a new host.
HID-6	HID	Stephane Ardiley	Ed	1	20	896-906	5.6	This section refers to "Status Words". Part 1 of the 800-73-4 doesn't deal with APDU command format and response so this section should be removed from part 1	Add this section in part 2 like in section 3.	Noted. Part 2 specifies applicable status words on a command by command basis. Part 1 specifies all of the status words implemented within the PIV Card Application but not on a command by command basis.
HID-7	HID	Beatrice Salaun	Te	2	10	480-481	3.1.2	The following sentence makes reference to the APT : « * The Lc value is '05' for all PIV data objects except for the 0x7E interindustry tag (Discovery Object) and the application property template (APT), which have an Lc value of '03'. », but later in the "Response Syntax", it is not described as a possible response.	Why do we need the APT string returned from GET DATA ? (provided it is already returned as part of the SELECT command response)]	Resolved by removing mention of the APT from Section 3.1.2.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
HID-8	HID	Beatrice Salaun	Ed	2	11	514-517	3.2.1	Following sentence is correct as long as the authentication data are not verified in the card, otherwise this creates security issues and indication on the authentication data value:"If the key reference is '00', '80', or '98', and the authentication data in the command data field does not satisfy the criteria in Section 2.4.3, then the card command shall fail, and the PIV Card Application shall return the status word '6A 80'. The security status and the retry counter of the key reference shall remain unchanged."	Rephrase according to: "If the key reference is '00', '80', or '98', and the authentication data in the command data field does not satisfy the data format criteria in Section 2.4.3, then data aren't matched with the reference data in the card. As a result, the card command shall fail, and the PIV Card Application shall return the status word '6A 80'. The security status and the retry counter of the key reference shall remain unchanged."	Declined. SP 800-73-4 only specifies behavior that is manifested at the card edge. The proposed change is relevant only to the internal processing performed by the card.
HID-9	HID	Francois Eric Guyomarch	Te	2	13	544-546	3.2.2	It is not possible to change the pairing code via change reference data. This can cause security issues as the user can not change the pairing code to something only known to him.	Allow change reference data on the pairing code.	Declined. See HID-10. In order to protect the pairing code against brute force attacks without including a blocking mechanism (a try counter), the pairing code needs to be randomly selected. User selected pairing codes would be much more vulnerable to guessing attacks. In addition, some agencies may make a risk-based decision to print the value of the pairing code on the back of the card in order to ensure that cardholders don't have to memorize its value, which may be considered important given that it is expected that cardholders will very rarely need to type in their pairing codes, and allowing cardholders to change their pairing codes would effectively preclude agencies from doing this.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
HID-10	HID	Francois Eric Guyomarch	Te	2	14	577-579	3.2.3	No reset retry counter on pairing code can allow brute force attack against the pairing code	Allows reset retry counter on the pairing code	Declined. While the initial draft of SP 800-73-4 included a retry counter for the pairing code, it has been removed from the second draft in order to prevent an attacker from blocking the cardholder's ability to establish a VCI with the card by sending a few VERIFY commands to the card with incorrect pairing code values. The second draft requires the pairing code to be an 8-digit randomly generated value. This should make any brute force attack against the pairing code infeasible. It is believed that any attacker who would have access to the card for enough time to perform a brute force attack against the pairing code would also be in a position to insert the card into a contact card reader, which would obviate the need for the attacker to obtain the pairing code.
HID-11	HID	Beatrice Salaun	Te	2	16	624	3.2.4	What is the rationale of using INS = 87h and not 86h on the General Authenticate command (with OPACITY)? 87h means encapsulation in TLV of Command / Response Data Field, which requires additional data parsing and would impact performances. This is also not in line with the ANSI B10.12 (504-1) recommendations (where INS='86' is used in this case)	Align with ANSI 504-1 regarding General Authenticate command encoding	Declined. INCITS 504-1 allows both '86' and '87'. INCITS 504 is a superset of the PIV specification. PIV uses only '87'. See also GSA-3.
HID-12	HID	Stephane Ardiley	Ed	2	17		3.3.1	The specification doesn't explain how to load the Biometric OCC fingers 1 and 2. Is it out of scope of the version?		Declined. Card personalization is out-of-scope for SP 800-73-4.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
HID-13	HID	Beatrice Salaun	Te	2	20	685-686	4.1	Description is based on a configuration supporting all modes of OPACITY protocol, some described steps are not applicable to the mode presented in 800-73-4.	Step C2 should be CBicc = CBh, no need to do “CBh & F0”, as only accepted value will be 10h.	Declined. In OPACITY, bits b1 and b0 of CBH provide information about the client application's support for persistent binding (which is not supported in SP 800-73-4). A PIV Card may proceed to perform the key establishment protocol without persistent binding even if the client application indicates in bits b1 and b0 of CBH that it supports persistent binding. Thus the protocol in SP 800-73-4 correctly indicates that the PIV Card ignores the least significant 4 bits of CBH.
HID-14	HID	Beatrice Salaun	Te	2	20	685-686	4.1	Compared to ANSI 504-1, in step C9, T16(Qeh) has been replaced by Qeh in AuthCryptogramicc computation. What is the rationale for this change and discrepancy with 504-1?	Re-integrate T16(Qeh)	Declined. The key establishment protocol in SP 800-73-4 has been written to conform to SP 800-56A, which requires the entire ephemeral public key to be included in the key confirmation computation, not just the first 16 bytes of the key.
HID-15	HID	Francois Eric Guyomarch	Te	2	23	Step C5	4.1.2	The support of ECC-DH according to 800-56A is only supported on JavaCard 3.0 cards through the ALG_EC_SVDP_PLAIN algorithms. Most cards in circulation today follows JavaCard 2.x which supports the ALG_EC_SVDP_DH algorithm: http://javacard.kenai.com/javadocs/connected/javacard/security/KeyAgreement.html This algorithm is an implementation of the IEEE 1363 algorithm, which computes a SHA-1 on the output of the derivation primitive. This SHA-1 algorithm is hardcoded and can not be changed at the JavaCard level. So this creates a small difference with the 800-73-4 specifications as it stands right now which does not have this intermediate SHA-1.	Add the possibility to accept IEEE 1363 algorithm as KDF, including the additional SHA-1. This could be defined as a new cipher suite and would permit to support a larger number of card platforms	Declined. The IEEE 1363 algorithm is not a NIST Approved KDF, and so it cannot be used by the PIV Card Application. See also GSA-3.
HID-16	HID	Francois Eric Guyomarch	Te	2	24	Table 13	4,1,4	There is a discrepency in CS4 definition with ANSI 504 standard: CS4 requires AES256 rather than AES 192 in ANSI 504	Realign with ANSI Standard, or define another cipher suite algorithm id that do not conflict with ANSI 504 cipher suite definition	Resolved by defining a new cipher suite algorithm identifier ('2E').

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
HID-17	HID	Francois Eric Guyomarch	Te	2	27	748-750	4.2	Shall clarify if bit 3 encoding is for commands and bit 4 is for response	Clarify if bit 3 and 4 can defines security levels for individual commands resp. response or if this mode is not supported	800-73: Declined. Section 4.2 states that both bits shall be set when secure messaging is used (and neither are set otherwise), so there is no need to explain the meaning of the individual bits. ISO/IEC 7816-4 details the meaning of the various bit values, the SM bit values required by 800-73-4 detail the approved implementation for the PIV card application.
HID-18	HID	David Sanda	Te	2	31	842-843 & 852-854	4.2.4	Pictures shown in Fig 3 and 4 miss the "Le" on the protected message. The protected message shall have an Le set to '00' (for short APDUs). Here, the Le fields are MISSING (Fig. 3, Fig. 4 last APDU).	Le field is mandatory (as the answer will always have a data field - containing the protected SW and MAC even if there are no encrypted data). So the secure message is ALWAYS a Case 4 APDU and the Le on the secure message is ALWAYS '00'.	Accepted. Le field will be added with value zero in the last APDU of figure 4 and the APDU of figure 3. Text will change accordingly.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
HID-19	HID	Beatrice Salaun	Te	2	32-33	873-904	4.2.6 / 4.2.7	What Status words are sent within Secure Messaging ? Only 9000h? Are we saying that regardless of the error, it is sent in clear ? (For instance, should a 6300h SW1/SW2 be sent within Secure Messaging ?).		Noted. If secure messaging itself is not successful (e.g., the C-MAC in the request is either missing or incorrect) then PIV Card returns an error message in the clear, as specified in Section 4.2.7. If the secure messaging is successfully processed, then the response is sent within secure messaging, and the response includes the Secure Messaging Data Field followed by '90 00', where '90 00' indicates the successful processing of secure messaging. The BER-TLV encoded status words (tag '99') indicate the status response of the command itself. Thus, if the VERIFY command were submitted over secure messaging with an incorrect PIN value and the PIV Card was able to decrypt and verify the C-MAC on the command, the response would be submitted over secure messaging with the BER-TLV encoded status words indicating the VERIFY command was unsuccessful (e.g., '63 CX'), whereas the status words that followed the Secure Messaging Data Field would be '90 00' to indicate that the secure message was successfully processed.
HID-20	HID	Francois Eric Guyomarch	Te	2	34	906-907	4.3	An explicit method shall be supported to enable resetting the session keys. Under some use cases it is important that the PIV Middleware can have full control over the secure messaging keys without having to reset the card	Add a 'MANAGE SM' method to explictetly enable close the sessions	Declined. MANAGE SM is not a recognized ISO/IEC 7816 command. Shouldn't add this new proprietary command to the PIV Card Application.
HID-21	HID	Beatrice Salaun	Te	2	45		A6	The APDU sequence references C-APDU= "0C C0 00 00 00" and "0C C0 00 00 A3"	Should replace with "00 C0 00 00 00" and "00 C0 00 00 A3"	Accept.
HID-22	HID	Francois Eric Guyomarch	Te	3	4	263-269	3	The proposed solution to identify the current communication interface by reading a certificate may cause performance problems. Especially for PACS use cases where fast establishment is required this method will adversely impact the users experience	Add a new data object in the connectionDescription that returns the currently used communication interface	Declined. The use-case described in the comment is not likely to happen. In a PACS implementation the reader will know what interface is being used to contact the card.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
HID-23	HID	Francois Eric Guyomarch	Te	3	10	481	3.3.1	The standard does not specify what is the expected behavior and algorithm input in case of case 03(SM key) is used in the pivCrypt function Is the intent to enable passthrough to the General Authenticate function from the pivCrypt function and hence enable secure messaging establishment though that function or generally used the session keys for encryption from calling middleware ? If former this is redundant with the pivEstablishSecureMessaging function	Clarify the scope of use of the pivCrypt function with key 03.	Resolved by adding the clarification that pivCrypt shall return error code if used with key reference '03'.
IG-1	InfoGard	Sweymann	G	all				Thank you for providing a track change version.		You are welcome.
IG-2	InfoGard	Sweymann	G	1	1	364	1.3	"With the exception of the requirement for the 362 PIV Card Application … Federal departments and agencies must implement these recommendations no later than 12 months after the effective date of FIPS 201-2." Perhaps the initial part of the sentence exempts the agencies from the time for SP 800-73-4 conformant PIV applet avaliability. Otheriwse, the feasibility of this statement depends on many variables. Perhaps FIPS 201-2 (draft dated March 2011, effective date "immediately" on line 190) will be held in draft status until this is possible. If this statement implies availability to agencies of SP 800-73-4 applets, be aware that the current CVMP queue is 7 months or more. As well the SP 800-85A and the associated Test Runner update will take some time to complete including a documentation comment period.	Assuming the exemption of SP 800-73-4 applet availability, replace this clause: "With the exception of the requirement for the PIV Card Application ..." with this clause: "With the exception of deployment of cards with SP 800-73-4 conformant PIV Card Applications, ... ". If this is not the intent, and the effectiveness statement is inclusive of 80-73-4 applet deployment, consider a deadline relative to applet availability: "Federal departments and agencies must implement these recommendations no later than 6 months following availability of qualified cards on the GSA APL."	Declined. All cards that are currently available on the GSA APL can support all of the data objects and functions that are listed as mandatory in SP 800-73-4. So, implementation of these requirements is not dependent on the deployment of cards with SP 800-73-4 conformant PIV Card Applications. For the one new requirement that may not be supported by currently available cards, the text says that implementation of this requirement shall be phased in as new card stock that implements the requirement is acquired.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
IG-3	InfoGard	Sweymann	T	1	13	768	3.5	The table shows only Printed Information with the OCC access control condition. It seems odd that at least facial image, as a means for additional visual identification confidence rather than a useful automated biometric would not also be OCC, or even that OCC would be acceptable as a PIN substitute.	Change Facial image to "PIN or OCC". And / or, include an explanation of the NIST rationale for OCC access control condtions.	Declined. FIPS 201-2 requires the presentation of a valid PIN before biometric data may be read. SP 800-73-4 would not be an appropriate place to provide a rationale for the requirements included in the document.
IG-4	InfoGard	Sweymann	T	1	13	768	3.5	Should SP 800-73-4 define a PIN AND OCC access condition? Be aware that use of OCC is controversial at CMVP; it is theoretically possible that OCC meets 140-2 security strength conditions, since some OCC algorithm receiver curves pass the 1/10^6 threshold required by 140-2, but practicality of this setting is questionable and out of scope for lab assessment. Use of multi-factor authentication for authenticatoin to the card is much stronger; I believe all card vendors who support OCC do or can support PIN AND OCC access control.	Include a note that a PIN AND OCC access condition is acceptible as a PIN substitute. Though this may be seen as a given (since it implies PIN), it is better to be explicit that this method is allowed.	Declined. As noted, in cases where the access condition is either “PIN” or “PIN or OCC” it is already self-evident that the access conditions are satisfied if the security status indicators for both the PIN and OCC data are TRUE. While support for OCC by PIV Cards is optional, a PIV Card that does support OCC may not (for interoperability reasons) require both PIN and OCC as an access condition for any PIV data objects or keys.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
IG-5	InfoGard	Sweymann	T	1	20	831 or 891	5.1 or 5.5	Use of SM for a contactless VCI is good, and in fact more secure than the contact scenario. Section 5.1.2 seems to indicate that SM could be used over contact interface, but discussion with NPIVP indicate the SM is intended for contactless only. Clarification that SM is allowed for use on contact would be be best. The PIV spec for PIN in the clear, in whatever mode, is arguably the only factor limiting PIV cards to 140-2 Level 2 overall, and some attack scenarios could be eliminated by allowing SM in contact mode.	Add "SM" to Contact column for appropriate entries (particularly PIN, global PIN, OCC) with a note that SM usage is optional but permissible.	Declined. Adding "SM" to the contact column would mean "SM" is required for contact interface. This would be a non-backward compatible change. Also, there is nothing in SP 800-73-4 that states "SM" cannot be used over contact interface. While secure messaging may be used over the contact interface, the PIV Card must permit the full functionality of the PIV Card to be performed over the contact interface without secure messaging. While this may prevent a PIV Card from being FIPS 140-2 validated at an overall level higher than 2, it is necessary to ensure interoperability, and it is not considered to be a problem since FIPS 201 only requires the PIV Card to be FIPS 140 validated to Level 2 overall (with Level 3 physical security). Mentioning the contact interface in Section 5.5 would be confusing as the full capabilities of the PIV Card are available over the contact interface (with or without secure messaging) without the need to present the pairing code.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
IG-6	InfoGard	Sweymann	T	2	20	685	4.1	Thank you for the clear description of Opacity in Section 4.1. Currently, the Opacity protocol is not listed in FIPS 140-2 Implementation Guidance D.8, and as such could be interpreted as not allowed.	Please request that CMVP update IG D.8 to include Opacity, coordination will help new validations of PIV Applets to go through as quickly as possible.	Declined. SP 800-73-4 does not use the OPACITY protocol, but a SP 800-56A-compliant key establishment protocol that is based on OPACITY (i.e., changes were made to the protocol in order to make it compliant with SP 800-56A). So, it would be inappropriate to request that the CMVP implementation guidance be updated include OPACITY. Furthermore, the first scenario listed in IG D.8 is to have a CAVP KAS Certificate, and Section 7 of Draft SP 800-78-4 states that PIV Card Applications that implement the PIV Secure Messaging key shall obtain a CAVP certificate indicating that they correctly implemented the C(1, 1, ECC CDH) scheme from SP 800-56A.
NSA-1	NSA			2				It would be helpful to explicitly indicate the security goals achieved by the protocol. The simplified Opacity ZKM protocol as presented in SP800-73-4 provides: o One-way authentication of the card to the client. o Key confidentiality in sessions run without any interference from the attacker, even if the attacker previously/subsequently interacts with other parties running the protocol and controls some set of valid cards, but has not obtained the long-term private key of the card in question. (Note that the notion of key confidentiality achieved here is weaker than the standard one, since SK_ENC is not indistinguishable from uniform. Nevertheless, one can define a meaningful notion of key confidentiality and show that the simplified Opacity ZKM protocol achieves it.)		Noted. Section 4 of Part 2 already notes that the key-establishment protocol is a one-way authentication protocol that authenticates the PIV Card Application to the client application. Resolved issue of protocol providing a weaker notion of key confidentiality by eliminating use of SKENC to encrypt the GUID during the key-establishment protocol.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
NSA-2	NSA			2				It would also be useful to explicitly indicate what security goals are not provided: o The protocol does not provide forward secrecy. o The protocol does not provide authentication of the client to the card, and if such authentication is desired it must be provided by other means. o As the paper "A Cryptographic Analysis of Opacity" by Dagdelen et al. shows, the protocol does not achieve privacy/anonymity. It should be made clear that encryption of the GUID is there for compliance with other standards.		Resolved by adding a footnote in Section 4 of Part 2 that notes that the key-establishment protocol does not provide forward secrecy. Section 4 of Part 2 already notes that the key-establishment protocol is a one-way authentication protocol that authenticates the PIV Card Application to the client application, so this implicitly indicates that the client application is not authenticated to the PIV Card Application. Resolved by changing the protocol to return the GUID in unencrypted form.
NSA-3	NSA			2				We do not see any reason to encrypt the GUID, as it as it reduces the efficiency of the protocol and does not provide privacy. However, if the GUID is to be encrypted we recommend either (1) deriving an additional key with the KDF, and using that key to encrypt the GUID, or (2) using SK_{CFRM} to encrypt the GUID. The GUID is currently encrypted with SK_{ENC}, which is also used in the secure-messaging phase. This type of key reuse is usually discouraged. Although we do not see any problems with the use as specified, it could be problematic if the secure-messaging phase is ever modified.		Resolved by changing the protocol to return the GUID in unencrypted form.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
NSA-4	NSA			2				It appears that a goal of the simplified ZKM protocol in SP800-73-4 is interoperability with the version of the ZKM protocol in INCITS 504, which is known to have security vulnerabilities. Specifically, Appendix A of the paper by Dagdelen et al. shows that an attacker can masquerade as a valid card to a terminal running the ZKM protocol from INCITS 504. It is important to note that a PIV card implementing the SP800-73-4 protocol could be impacted by these vulnerabilities if the card interacts with a card reader/terminal running INCITS 504. In particular, an SP800-73-4 compliant card might be given access to a space that is also admitting malicious cards running masquerade attacks on the INCITS 504 version of the protocol.		Noted. As INCITS B10.12 is working to address the issues in INCITS 504 that were raised in "A Cryptographic Analysis of OPACITY," it should not be necessary for SP 800-73-4 to highlight security vulnerabilities in the protocol as described in the current version of the document.
NSA-5	NSA			2				This simplified ZKM protocol incorporates the "One-pass Diffie Hellman" scheme from NIST SP800-56A. This fact should be stated explicitly. In fact, this protocol could be described by simply pointing to SP800-56A for the One-pass Diffie Hellman scheme in its entirety and then specifying fields and extra steps that are required by SP800-73-4.		Resolved by adding text to the beginning of Section 4.1 of Part 2 that notes that the key-establishment protocol uses the One-Pass Diffie-Hellman, C(1e, 1s) Scheme from SP 800-56A.
NSA-6	NSA			2				If the desire is to ultimately support other values for the control bytes CB_H and CB_{ICC}, then these values should be included in the CMAC computation to ensure their integrity.		Resolved by including the control bytes in the OtherInfo string that is an input to the key derivation function.
NSA-7	NSA			2				The value of *len* used as input to the KDF in steps H10 and C7 is given in a table in Section 4.1.3, but it would be helpful to also specify *len* in 4.1.6.		Accept.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
NSA-8	NSA			2				The MAC value sent and verified is only 8 bytes long, which could lower the desired security if unlimited attempts are permitted. Therefore, restrictions on the maximum number of invalid attempts should be stated.		Noted. The MAC value that is used for key confirmation is 16 bytes long. While the MAC value that is used for secure messaging is only 8 bytes long, a single invalid attempt will result in the secure messaging session keys being zeroized.
NSA-9	NSA			2			4.1	In Section 4.1, Step H2, more details are needed to specify how to generate an ephemeral key pair. (More detail is given in SP800-56A, section 5.6.1.2, which references FIPS 186 Appendix B.)		Resolved by specifying that key generation shall be performed using an approved method from Appendix B of FIPS 186-4 and that full-public key validation shall be performed on the generated key.
NSA-10	NSA			2			4.1	Section 4.1, Step H7. More details are needed on how to perform public key validation of Q_{sICC}. According to SP800-56A, a full public key validation is required for static keys. One option is to have the CA perform this validation when it creates the certificate C_{ICC}. Then, the client will be assured that the public key is valid when he verifies the signature on C_{ICC} in step H16. If the Client application will perform the public key validation itself, then the "ECC Full Public-Key Validation" of SP800-56A should be specified here.		Resolved by specifying that the issuer of the CVC shall perform full public key validation before signing the certificate and by reordering the steps in the key-establishment protocol so that the client application verifies the signature on the CVC before using it for key agreement.
NSA-11	NSA			2			4.1	Section 4.1, step C4. More details are needed on how to perform public key validation of Q_{eH}. Since this validation is for an ephemeral public key, the "ECC Partial Public-Key Validation" of SP800-56A should be specified here.		Resolved by specifying that the PIV Card Application shall perform partial public-key validation as per Section 5.6.2.3.3 of SP 800-56A.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
NSA-12	NSA			2				Minor comments: o Misspelled “AuthCryptogram” on page 20, step C12. o Mixed hex notation, both 0x## and ‘##”. o Section 4.1.3, in the “Comment” section, C_{ICC} should be the Confidential card verifiable certificate, and C_{ICC}* should not be considered confidential, because it is the certificate sent by the ICC to the Client.		Resolved by correcting the spelling of AuthCryptogram and by removing “Confidential” and “for privacy” from the description of CICC*.
OT-1	Oberthur	C. Goyet	E	1	V	10th bullet		The words "or and" may need to be replaced with the word "or an" in the 10th bullet: "… Thus, removed the option to populate the GUID data element of CHUID with all zeros or **an** IPv6 address".	replace "or and" with "or an"	Accept.
OT-2	Oberthur	C. Goyet	E	1	3	401	2.1	That sentence line 401 is repeated on line 405. Statement in line 405 is more precise and should be the one to stay as it is located right after the statement that allows the use of unspecified tags as long as they are interindustry tags defined in ISO/IEC 7816. Statement in line 401 is too generic as it prevents the use of any unspecified names regardless of whether the tag is an ISO interindustry tag or not.	Remove line 401 that is superseded by line 405.	Declined. Line 401 refers to the namespaces specified in Lines 395 – 400, whereas Line 405 refers to the identifier and value namespaces specified in Lines 407 – 409.
OT-3	Oberthur	C. Goyet	E	1	24		table 8	If data elements of the CCC, except for the data model number, may optionally have a length value set to zero bytes (i.e., no value field will be supplied), as now stated on page 4 line 461, then this table has to be updated as the size of some data element is currently fixed to a value different from zero.	Change the type from Fixed to variable for the data element that can have a size set to zero.	Resolved by changing the entries in the “Max. Bytes” column to “0 or X,” where “X” is the acceptable non-zero length.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-4	Oberthur	C. Goyet	G	1	24		table 8	There seem to be two ways to deal with optional data element that are not present. Either include the tag but set the length to zero as specified page 4 line 461, or by not including the tag. It would be good for interoperability and compliance testing if NIST could standardize the way to deal with optional data elements when they are not available.	Standardize the way to manage optional sub-data element in a container by choosing only one of the two following methods: Tag absent or tag length set to zero.	Resolved by adding a sentence to section 3.1.1, 3rd paragraph and after 2nd sentence as follows: Note that unused optional data elements shall be absent.
OT-5	Oberthur	C. Goyet	T	1	9	622	3.3.2	The discovery object is a short data object that is quick to be retrieved from the card and that provides discovery information. Instead of including the full BIT within the discovery object , and making the reading of that DO slower even for middleware that do not support OCC, why not use one bit of the existing PIN Usage policy to indicate support for OCC? Like bit 5 for instance? Once the middleware knows that the card supports OCC, it can proceed like with any other cards that support OCC, i.e. by reading the BITG using its ISO tag i.e. 7F61 .	Use one bit of the PIN policy to indicate support for OCC without inflating the size of the discovery object with a BIT that can be retrieved directly with the ISO command (GET DATA with tag 7F61).	Resolved by using bit 4 of the PIN Usage policy to indicate support for OCC and making the BIT group template a separate data object.
OT-6	Oberthur	C. Goyet	T	1	10	652	3.3.2	There is another reason not to embed the BIT within the discovery object. The BIT is updated dynamically by the card following a successful enrollment and the discovery object is updated by the CMS during personalization and in post issuance when there is a change in the preferred PIN (Local vs Global). Having different write access conditions for two parts of the discovery object could lead to data corruption and make the system more complex to develop and to test.	Remove the BIT from the discovery object and have it read by a GET DATA with tag 7F61 as defined by ISO: 00 CB 3FFF 04 5C 02 7F60 00 .	Accept

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-7	Oberthur	C. Goyet	T	1	10	652	3.3.2	What is the link between the pairing code and the PIN policy? If the pairing code is supported by the card in the discovery object but shouldn't this be located outside of the PIN policy data element?	Remove pairing code information from the PIN policy data element and add it to a new data element that provides information about contactless interfaces i.e. support for SM, VCI and paring code.	Declined. While the pairing code may be used in a very different manner than the PIV Card Application PIN or the Global PIN, it is no different from the PIV Card's point-of-view. Just like the PINs, the pair code is presented to the card using the VERIFY command, the result is to set the corresponding security status to TRUE, and this security status is used as an operand in the specification of security conditions. So, it is appropriate to include information about the pairing code in the PIN Usage Policy along with the PIV Card Application PIN and Global PIN.
OT-8	Oberthur	C. Goyet	T	1	10	657	3.3.2	In SP800-73-4 draft, the CVC is used as a card authentication certificate for the Opacity protocol. Using the CVC encoding instead of the traditional X509 has some value (more compact) but storing the url to verify the opacity protocol signature in the discovery object defeats part of the benefit of the opacity protocol, which is to open a secure channel with a single APDU. If middleware has to send a additional APDU just to verify the opacity signature, that may create some issues in the field especially with contactless transactions that have to be as short as possible. An alternative approach that would still provide a discovery function for the Secure messaging support but without making it mandatory to establish the secure messaging would be to use one bit of tag 0x5F2F to indicate support for the Secure Messaging using the PIV Secure Messaging key specified in Table 4 and the SM protocol in accordance with the specifications in Section 4 of Part 2	Remove tag 0x5F50 from the discovery object and use one bit of tag 0x5F2F to indicate support for the Secure Messaging using the PIV Secure Messaging key specified in Table 4 and the SM protocol in accordance with the specifications in Section 4 of Part 2, and add tag 0x5F50 into the ICC CVC certificate returned by the card during the opacity protocol (section 4 of part 2).	Resolved by DoD-12 and by adding a footnote in Section 4.1.1 of Part 2 clarifying that the client application does not need to validate the content signing certificate at the time of CVC signature verification if it has previously validated the certificate or if it has obtained the public key needed to verify the signature on the CVC in some other secure manner. Support for secure messaging is indicated through the presence of the appropriate algorithm identifier in the 'AC' tag.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-9	Oberthur	C. Goyet	T	1	10	672	3.3.2	What is the purpose of the Security Object to enforce integrity of the discovery object? Modifying the BIT does not make OCC more likely to succeed as the BIT does not control the OCC engine but is only here to provide information on how minutia must be submitted for best performances. The only sensitive data seems to be the url to verify the CVC but relying on the Security Object for that means that the opacity protocol would now require 3 APDU (one for opacity, one to read and parse the discovery object to get the url to verify the opacity signature and one to read and parse the SOD to verify the integrity of the above url. This will seriously impact performances of a PIV transaction over the contactless interface. If the url is moved out of the discovery object and back into the ICC CVC where it belongs (see Oberthur comment #8 above), there may be no more need to enforce the integrity of the discovery object with the security object.	Remove line 672	Resolved by DoD-13. Note that none of the authentication mechanisms in Appendix B of Part 1 require relying parties to check the Security Object.
OT-10	Oberthur	C. Goyet	T	1	10	672	3.3.2	It would be better if the security object would not enforce the integrity of the discovery object as the discovery object is dynamic in nature. It changes every time the preferred PIN is switched between local and global, and it changes also when a fingerprint is re-enrolled for OCC. If the security object has to be recomputed every time the discovery object changes, that means that in addition to the admin key, the OCC enrollment application would need to have the key for the security Objet which may compromise the overall security if the enrollment is done locally.	Remove line 672 and state that the discovery object is dynamic in nature and not included in the security object protected data.	Resolved by DoD-13. Note that the Security object protects the integrity of all unsigned data objects.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-11	Oberthur	C. Goyet	T	1	17	831	Table 4	The table lists the global PIN but misses the Global PUK to unlock the Global PIN. It would be good for SP800-73-4 to reserve key reference ID ‘01’ for an optional Global PUK currently supported by several PIV cards.	Add key reference value ‘01’ for an optional Global PUK	Declined. Adding '01' reference for Global PUK is out of scope since Global PIN management is out of scope for PIV Card Application.
OT-12	Oberthur	C. Goyet	T	1	17	831	Table 4	Fingers for OCC are global parameters and if given a key reference value, that reference should be taken from the range of value allocated by ISO for global parameters. But the best would be not to give them any value and add the finger identifier in the ISO data object 7F2E as described in attached document.	If primary and secondary finger OCC are given key reference value, use values from the Global Reference value range instead of local reference value range.	Declined. The OCC references will remain in local scope, as the PIV card application is one application of possibly many and should not set global security requirements.
OT-13	Oberthur	C. Goyet	T	1	17	831	Table 4	Why do PINs (Global and PIV Card Application) have a security condition to use in contactless different from the fingers for OCC? If the secure messaging is believe to be secure enough to transmit fingerprint templates for OCC, it should be secure enough to transmit a PIN value as both PIN and Finger OCC can be subject to the same type of attacks.	Have the same security condition for use of OCC and PINs in contactless (i.e. VCI)	Declined. The security condition for use for OCC is secure messaging rather than VCI so that OCC may be used as an authentication mechanism. The PINs, however, are only used to authenticate the cardholder to the card, and there are no PIN-protected operations that may be performed over the contactless interface without first establishing a VCI. Requiring VCI as a security condition for use for the PINs prevents an attacker who does not know a card's pairing code from locking the card by establishing secure messaging and sending a few VERIFY or CHANGE REFERENCE DATA commands with incorrect PIN values.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-14	Oberthur	C. Goyet	T	1	17	831	Table 4	There is no need to define a key reference value for primary and secondary finger OCC. Verification can be done using the finger ID extracted from the BIT. The first finger listed being the primary and the second one the secondary. Using finger ID from the BIT allows to display the finger name (e.g. left index) when prompting the user to scan a finger for OCC instead of relying on the user to remember which finger was enrolled as primary and which finger was enrolled as secondary. For the VERIFY APDU, using the odd INS for biometric verification (fingerprint, iris, facial, etc) allows to include in the command data field the finger ID to verify, removing the need to reserve two key reference values from the small range authorized by ISO 7816-4. Cards with multi modal biometric OCC (fingerprint and Iris) and soon facial are already available and may be integrated into a future version of SP800-73-4. Since the range allowed by ISO/IEC 7816-4 for P1P2 in the VERIFY APDU is not extensible to support these new biometric modalities, it is important for PIV to define an architecture for biometric verification that can grow over time as new modalities for OCC become more widely available. Using the VERIFY APDU with odd INS as described in ISO/IEC 7816-4 allows to put the identifier of the biometric to verify in the command data field instead of in the P1P2 parameters. (See Oberthur comments on SP800-73-4 part 2).	Remove key reference value for both primary and secondary finger OCC.	Declined. Use of P1 P2 key reference values in VERIFY command is currently the only standard way to submit OCC data to the card. The suggested solution to use tag '95' is in conflict with the existing standard.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-15	Oberthur	C. Goyet	T	1	18	832	Table 4	Reference data (like PIN, PUK, Global PIN) and Key identifiers (9A, 9B, etc) are different in nature and use different APDUs (VERIFY vs GENERAL AUTHENTICATE). The associated identifier values can come from different name spaces and ISO/IEC 7816 let you have a PIN with identifier 80 as well as a key with identifier 80. So to provide greater flexibility for future evolution of SP800-73-4 you may want to split table 4 in two separate table, one for reference data and one for keys.	Split table 4 in two separate tables, one for reference data and one for keys.	Accept.
OT-16	Oberthur	C. Goyet	T	1	18	832	Table 4	'03' is a value for Global Key ID but in table 4 it is used for a local key ID (PIV Secure messaging key).	Use for the PIV secure messaging key an ID value within the range allocated by ISO/IEC 7816 for local keys (PIV keys) instead of Global Keys.	Declined. The PIV Secure Messaging key is intended to be a global key.
OT-17	Oberthur	C. Goyet	T	1	18	832	Table 4	Some of the security conditions for use over the contactless are set to Never. (PUK and 9B). Is there a rational for not authorizing these keys over the VCI? Now that the PIV form factor can expand outside of the smart card form factor, especially for derived credentials over the NFC interface, there is a need to do for these devices a full personalization over the contactless interface through a secure channel. Can you allow all operation currently available over the contact interface to be carried out over the contactless interface through the VCI ?	Allow all operation currently available over the contact interface to be carried out over the contactless interface through the VCI by changing security condition for contactless use of key 81 (PUK) and 9B (ADMIN) from NEVER to VCI.	Declined. The VCI is established through the use of a one-way authenticated secure session and FIPS 201-2 requires a mutually authenticated secure channel between the PIV Card and the card issuer for remote post issuance update operations, including PIN reset. Thus, the VCI is not appropriate for communication between the PIV Card Application Administrator and the PIV Card.
OT-18	Oberthur	C. Goyet	T	1	18	832	Table 4	Table 4 is not compliant with the second draft of FIPS 201-2 that states in line 1300 that : "Any operation that may be performed over the contact interface of the PIV Card may also be performed over the virtual contact interface.". To bring table 4 in compliance, security condition for use in contactless should be changed from Never to VCI.	Change security condition for contactless use of key 81 (PUK) and 9B (ADMIN) from NEVER to VCI.	Resolved by OT-17.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-19	Oberthur	C. Goyet	T	1	19	852	5.1.2	This section describes a PIV secure messaging key based on PKI and Opacity, i.e. at the PIV application level. Current PIV cards support a different secure messaging provided by the card platform like Global platform SCP03. In the same way as the Global PIN can be used instead of the PIN, could SP800-73-4 allow the global secure messaging to be used to fulfill SM access rights ? This would allow an easier migration to SP800-73-4 for CMS that perform PIV card personalization.	Add a sentence to state that the secure messaging provided at the Global level (i.e. by the platform) can also be used to fulfill the SM access conditions.	Declined. In order to ensure interoperability only the key establishment and secure messaging protocols specified in Section 4 of Part 2 may be used for secure messaging for non-card-management operations. However, PIV Card personalization is not standardized, and so GlobalPlatform SCP03 may be used for this purpose, as long as the requirements of FIPS 201-2 (e.g., Section 2.9.2) are satisfied. See also GSA-3.
OT-20	Oberthur	C. Goyet	T	1	19	859	5.1.2	It is stated that “The PIV Card shall store a corresponding card verifiable certificate (CVC) to support validation of the public key by the relying party.” But that additional certificate has been missed in part 1 table 2 and no tag identified to store that CVC.	Add a sentence to state that the CVC is personalized using PUT DATA with ISO /IEC 7816-6 tag ‘7F21’ (Card Holder Certificate)	Declined. Card personalization is out-of-scope for SP 800-73-4.
OT-21	Oberthur	C. Goyet	T	1	19	859	5.1.2	The way to load the CVC certificate has not been defined and could be either (PUT DATA in NIST format like for all the other PIV X509 certificates or PUT DATA in ISO format like for other ISO data objects like the Discovery object ‘7E’.	Add a sentence to state that the CVC is written into the card using an ISO/IEC 7816-4 PUT DATA. (00 DB 3FFF Lc Tag Lgt Value)	Resolved by OT-20.
OT-22	Oberthur	C. Goyet	T	1	20	880	Table 5	This table is not in line with the same table listed in SP800-78-4 draft table 6.2. Either remove the table and points to SP800-78-4 or do a cut and paste of the 800-78-4 table 6.2	Remove table and make reference to SP800-78-4 table 6.2.	Declined. Table 5 of Part 1 lists cryptographic mechanism identifiers, which are used by the GENERATE ASYMMETRIC KEY PAIR command, whereas Table 6-2 in SP 800-78 lists cryptographic algorithm identifiers, which are used by the GENERAL AUTHENTICATE command.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-23	Oberthur	C. Goyet	T	1	20	881	5.3	It is stated that “All other cryptographic mechanism identifier values are reserved for future use”. Could you please keep in this table the value ‘0E’ defined by NIST in the original SP800-73 for ECDSA or ECDH with ECC: Curve P-224. Most of the PIV cards in the field today do support ECC224 and time critical transactions outside of HSPD#12 but using a PIV card like public transport application may use opacity with ECC224 to save a few milliseconds. Same with TDES and AES in CBC mode that are still supported by current cards although removed from the latest edition of SP800-78.	Replace that sentence with “All other cryptographic mechanism identifier values not previously defined by NIST are reserved for future use.”	Declined. NIST cannot guarantee reservation of '0E' for ECC P-224 in future but the current version of SP800-73-4 will not use '0E' to reference any other algorithm. Based on the comments received previously NIST has reduced the number of permitted curves.
OT-24	Oberthur	C. Goyet	T	1	20	888	5.4	It is stated that “If implemented, SM for non-card-management operations shall ….” However the document does not specify what a card management operation is and is not. Is the CHANGE REFERENCE DATA a card management function? What about RESET RETRY COUNTER?	Define what “non-card-management” operations are.	Resolved by defining the term card management operation in Appendix D.1 of Part 1, Appendix B.1 of Part 2, and Appendix A.1 of Part 3 that defines “card management operation” as “any operation involving the PIV Card Application Administrator.”

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-25	Oberthur	C. Goyet	T	1	20	888	5.4	It is stated that "If implemented, SM …shall ONLY be..". Could you please clarify what the "if implemented" refers to? Does it refer to any secure messaging in general or does it refer to the Secure Messaging using the PIV Secure Messaging key specified in Table 4 and the SM protocol in accordance with the specifications in Section 4 of Part 2? I'm asking that question because most PIV cards today implement other types of Secure Messaging like Global Platform SCP03 for instance that offer the same level of security (AES encryption). Allowing these legacy Secure messaging protocols would allow compatibility with existing Card Management Systems as well as some middleware for PACS and LACS.	Change sentence line 888 with: "If support of the Secure Messaging using the PIV Secure Messaging key specified in Table 4 and the SM protocol in accordance with the specifications in Section 4 of Part 2, is indicated in the Discovery Object (see section 3.2.2) then this secure messaging shall be the one used by PIV applications for interoperability."	Declined. While other secure messaging protocols (e.g., GlobalPlatform SCP03) may be used for CMS to PIV Card communication, only the protocol specified in SP 800-73-4, for interoperability reasons, may be used to perform non-card-management operations within the PIV Card Application.
OT-26	Oberthur	C. Goyet	T	1	20	888	5.4	For interoperability, it is important to define one common secure messaging mandatory for all PIV cards, but can other secure messaging be authorized as an option? (A similar approach was defined for CAK (Key 9B) for which the asymmetric value is mandatory and a symmetric value optional.) The main benefit would be to allow compatibility with existing Card Management Systems that rely on Global Platform SCP03 secure messaging. That would also remove the need to split commands between card management and non card management operations as such difference often depends on the application using the card.	Change sentence line 888 with: "If support of the Secure Messaging using the PIV Secure Messaging key specified in Table 4 and the SM protocol in accordance with the specifications in Section 4 of Part 2, is indicated in the Discovery Object (see section 3.2.2) then this secure messaging shall be the preferred one used by PIV applications for interoperability."	Resolved by OT-25.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-27	Oberthur	C. Goyet	T	1	20	892	5.5	The virtual contact interface has for prerequisite the establishment of a SM. However SM is defined in section 5.4 is for non card management operation. Other types of secure messaging are used for card management like Global Platform SCP03, and it would be good that the VCI could be used over any kind of AES based secure messaging and not only the SM described in section 4 of part 2.	Allow platform level secure messaging like GP SCP03 to be used as a base SM for VCI.	Resolved by OT-25.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-28	Oberthur	C. Goyet	T	1	20	892	5.5	The addition of a pairing code verification to establish a Virtual Contact Interface does not seem to be justified. The purpose of the Virtual Contact Interface is to provide over the contactless interface the same level of security of the communication link than over the contact interface. A successful secure messaging should be enough to prevent eavesdropping and ensure confidentiality and integrity of the transmitted data, without need of a pairing code. In normal operation, user consent can be demonstrated in contact by the user inserting the card into the slot of the contact reader, and in contactless by bringing the card within an inch of the contactless reader. This type of contactless user consent is not bullet proof as some hacker may develop a reader with a higher reading range, but it is not bullet proof in contact either as most often the card stays in the contact reader after the single sign-on with the PIN being already verified, therefore giving access to all PIN protected data and operation to any rogue application that could access the PC. At least in contactless the transaction is often shorter so PIN protected data/operations are less exposed, and the Diffie-Hellman from the Secure messaging protocol does raise the bar for hackers.	Remove the paring code that creates usability challenges across its use cases and replace first sentence of 5.5 (line 892) with: “The establishment of a secure messaging over the contactless interface creates the Virtual Contact Interface (VCI).”	Declined. The fact that a PIV Card is within reading distance of a card reader does not provide the same level of consent to access the data on the card (e.g., the digital signature certificate) as when the cardholder inserts a card into a card reader. The use of a key-establishment protocol that provides mutual authentication is not an acceptable alternative, as it does not address the issue of user consent and it does not address interoperability (i.e., it only works with readers that have been provisioned with a certificate that can be validated by the PIV Card). See also G-17.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-28 (cont.)								The Pairing code creates usability challenges across its use cases. Does it have to be remembered by the user in addition to its PIN, is it encode on the optional magstripe or on a bar code printed on the card ? In any cases, adding a pairing code requires the contactless reader to be retrofitted with a data entry extension (e.g. Pinpad, magstripe reader, 2D/3D bar code scanner etc) that adds cost to the device and makes it bulkier. It also impacts transaction time as an extra step (data entry of the pairing code) is now required from the user. If needed for critical transaction, a better alternative to the pairing code to protect against rogue reader is to use as an option, a secure messaging with mutual authentication like GP SCP03 and Opacity FS. The mutual authentication added by Opacity FS to Opacity ZKM adds a little bit of card processing time, but such extra time is not significant compare to the extra time require for the card holder to key in the pairing code.		

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-29	Oberthur	C. Goyet	T	1	26	942	Table 14	Maximum size of the Agency card serial number in the printed information container has been increased from 10 to 20 byte in this edition of SP800-73. However a byte requires two characters (0-F) to be printed which bring the size of the printed number actually printed on the back of the card to 40 hex nibble which won't fit on the back of the card. (The size of the window to print this number as defined in FIPS 201 is pretty limited.). If the number is increased from 10 to 20 bytes, you need to specify that Agency Card Serial Number has to be a numeric value only, and then define how this number is to be encoded: Binary or BCD.	Specify that the Agency Card Serial Number is a numeric value of up to 20 digits encoded in binary.	Declined. Table 14 specifies the type for Agency Card Serial Number as "TEXT," thus the encoding is neither binary nor BCD, and each character (digit) of the serial number requires one byte to encode. To make the Agency Card Serial Number anything other than TEXT (ASCII) would be a non-backward compatible change.
OT-30	Oberthur	C. Goyet	T	1	27	950	Table 18	Remove Biometric Information Template from the Discovery object and replace it with bit 5 of the PIN usage policy to indicate that the OCC is supported by the card. See Oberthur comment # 6	Remove Biometric Information Template from the Discovery object and replace it with bit 5 of the PIN usage policy to indicate that the OCC is supported.	Resolved by OT-5.
OT-31	Oberthur	C. Goyet	T	1	27	950	Table 18	Remove Uniform resource locator from the Discovery object. See Oberthur comment # 8.	Remove Uniform resource locator from the Discovery object	Resolved by DoD-12.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-32	Oberthur	C. Goyet	T	1	45	1180	Section C.3	Could you please clarify whether the tag AC is supposed to list all cryptographic algorithms supported by the card or only the one supported for the Secure Messaging. As per my reading of ISO 7816-4, tag AC is supposed to list all the cryptographic algorithms supported by the card, but since most smart card chips today can handle all the algorithms listed in SP800-78-4 and some more, PIV card application updated for SP800-73-4 will most likely have tag a AC with all possible algorithms listed (and probably even more if algorithms supported by previous versions of SP800-78 like 2 Key Triple DES and CBC versions of all symmetric algorithms are also listed). This would result in a tag AC of up to 34 bytes that would be transmitted every time the PIV application is selected, bring no new information, but slow down transaction especially for PACS. Even if the tag AC is restricted to cryptographic algorithms for Secure messaging, most new PIV application are likely to support both cipher suite CS2 and CS4 therefore include both 27 and 2B algorithm identifiers in tag AC, telling nothing about which key is actually present (i.e. personalized) for Secure messaging.	Remove section C.3 with tag AC that adds overhead without providing useful information.	Resolved by adding the following text in-place of the sentence on line 467 of NIST SP 800-73-4 part 2 below table 4 in the select command section. • " 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."

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-33	Oberthur	C. Goyet	T	1	45	1180	Section C.3	What is the use case for the use of CS4 and therefore the need for a PIV Algorithm Identifier for Secure Messaging? Secure messaging was added to provide a Virtual Contact Interface (VCI) for contactless operation. Most contactless operations include performance requirements that call for a transaction as short as possible, therefore the use of CS2. According to section 5.4 line 888, the Secure messaging defined by NIST is for non card management operations, so the AES128 encryption provided by CS2 should be more than enough to guarantee the confidentiality of the finger OCC transmitted to the card. CS2 would not be strong enough to protect the loading of AES 192 or AES 256 into the card during personalization, but CS4 provides only 192 bit strength and therefore still not be suitable to load AES 256 keys. Besides, since there is only one PIV Secure Messaging key in table 4, so if that key is set to ECC P-384 to allow card management operation with the NIST Secure Messaging protocol, then the card will be slower for all other operations like finger OCC or public transit applications. Our recommendation is to remove the PIV Secure Messaging Discovery from the response to the SELECT command and define a single crypto suite for VCI (CS2 or even better CS1 as it is faster). Other crypto suite may still be supported by the card for card management system but don't need to be listed in SP800-73-4 for interoperability .	Remove the PIV Secure Messaging Discovery from the response to the SELECT command and have a single crypto suite (CS2) for interoperability i.e. for non card management operations.	Declined. The GENERAL AUTHENTICATE command may be performed over the virtual contact interface. When the GENERAL AUTHENTICATE command is performed with a key management key the response includes plaintext secret keying material. When plaintext secret keying material is transmitted over the contactless interface, it must be protected at the same level as the security strength of the key management key pair. Since the key management key may be an ECC P-384 key, there needs to be an option for secure messaging with 192 bits of security strength. As noted, for performance reasons, it would be inappropriate to require all PIV Cards to implement secure channels with this level of security strength.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-34	Oberthur	C. Goyet	G	1	45	1180	Section C.3	Secure messaging was added to provide a Virtual Contact Interface (VCI) for contactless operation. Most contactless operations include performance requirements that call for a transaction as short as possible. That's why the key establishment protocol rightfully selected by NIST is self contained within a single APDU. To make the transaction even faster PACS systems often skip the application selection if the card ATS indicates that the PIV application is the one selected by default upon card power-on, and if not, issue a SELECT APDU with no Le byte which according to ISO 7816 indicates that the reader does not want the card to return any data, so it can proceed right away with the GENERAL AUTHENTICATE command for Opacity Key Establishment. Adding APDU overhead to retrieve the type of secure messaging (tag AC from the response to the SELECT command) and the HTTP URL to verify the signature of the Card Verifiable Certificate (tag 5F50 from discovery Object) could significantly impact performances and add issues if the card disconnects between these APDUs. The HTTP URL with tag 0x5F50 could be easily included in the Card Verifiable Certificate returned by the card during the opacity protocol, and the Cipher Suite could be always CS1 that provides faster key establishment.	Remove the HTTP URL from the discovery object and the PIV Secure Messaging Discovery from the response to the SELECT command.	Resolved OT-8.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-35	Oberthur	C. Goyet	G	2	3	328	2.2	Could you please clarify the meaning of "Reserved for Future Use". NIST has defined in part one the tags for the various application data objects used on the PIV interface, but because PIV is an application and not a smart card operating system, there are additional data objects used for card management purposes by the card operating system that are not defined by NIST and cannot be reserved for future use. Not all of these system data objects are interindustry data object defined in ISO/IEC 7816. Some of these system tags are defined by Global Platform, and the card manufacturer had to define its own set of system tags when none were available from ISO to fit the requested purpose. To avoid conflict with NIST, these proprietary system Data Objects have a tag on two byte (NIST BER_TLV Tags are on 3 bytes unless they are defined in ISO 7816). Reserving for future use all unspecified BER_TLV Tags would be very difficult and bring little value. Could the restriction apply only to 3 byte BER_TLV tags ?	Remove sentence starting line 326: "Part 1 also…"	Declined. The statement applies PIV Card Application only as the title suggests.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-36	Oberthur	C. Goyet	G	2	3	326	2.2	In addition to proprietary BER-TLV tags for system data objects addressed in the previous comment from Oberthur, the card platform may support additional algorithm identifiers and cryptographic mechanism identifiers. For instance some cards support additional algorithms like ECC Curve P-521 algorithm for the crypto suite CS5 from GICS (ANSI 504). Some cards also support additional cryptographic mechanism identifiers like Opacity FS from ANSI 504 that are available for card personalization and other card management services. If NIST is open for PIV to be implemented on a GICS platform, the restriction around unspecified algorithm identifiers, Key reference values and cryptographic identifiers may need to be lifted. A solution would be to leave to the card manufacturer the responsibility to ensure its systems tag, values of algorithm identifiers, key references, and cryptographic mechanism identifiers could coexist peacefully with the ones defined by NIST in this Special Publication. This has been done with success by Oberthur since its first *"NIST Special Publication 800-73-1 End Point Specification Compliant™"* card back in 2006.	Remove in both part 1 (Section 2.1 page 3) and ^part 2 (section 2.2 page 3) the restriction about unspecified algorithm identifiers, Key reference values and cryptographic identifiers being reserved for future use. The restriction about unspecified OID with the NIST root may be kept.	Declined. The PIV Application namespace belongs to NIST and NIST will continue to reserve the names, tags, values, references, and identifiers for the PIV application. NIST specifications do not interfere with cards supporting other applications or the Card operating system. NIST does not place any restrictions on other applications on GICS platform or any other platform.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-37	Oberthur	C. Goyet	T	2	5	368	2.4.2	Having a on-card security status specific for each OCC finger may not be practical and raises several issues. It is preferable to have a single security status for OCC regardless of the finger that was last submitted for OCC. Let me try to explain why: Having in the card a security status specific to each finger forces the reader to provide to the card the identity of the finger against which the submitted template shall be compared. That information (finger ID) cannot be reliably captured by single print sensors. One cannot assume that the first finger submitted will always be the primary finger. If the user has a bandage on the primary finger, it may decide to submit its secondary finger, and unless the reader include some kind of keyboard to allow the card holder to indicate primary vs secondary finger, the verify command will fail and the security status associated to the primary finger will become locked after a few attempts. The use of a 10-print-fingerprint sensor could solve the issue but at a much higher cost than the use of almost ubiquitous single print sensors (swipe or flat). A simple solution is for the single print reader to send the Verify command without specifying the id of the finger being submitted (i.e. with ISO/IEC 19785 biometric subtype set to zero. See attached contribution called “Biometric Data Template for OCC enrollment and verification”.). This will instruct the card to perform a “one to two” comparison (i.e. to compare the input template to both referenced fingers stored in the card) as opposed to a “one to one” when the finger id is provided.	Have a common security status for all fingers that support OCC instead of one security status per finger.	Resolved by modifying the VERIFY command to perform a 1:2 match when OCC data is submitted.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-37 (cont.)								Also having a separate security status for each finger enrolled for OCC is more complex to manage by the card. The security condition "PIN AND (primary fingerprint OR secondary fingerprint)." Is already supported by most smart cards that offer OCC, but not "Secondary fingerprint only" or "Primary fingerprint Only". Support for three security status indicators of the cardholder (PIN, primary fingerprint, and secondary fingerprint) can still be achieved with OCC but with an off-card security status. The reader send three VERIFY command, each with a different reference data ID (PIN, primary fingerprint, and secondary fingerprint) and store within the reader the security status for each verification. At the card level, it will be only a two factor authentication (PIN + OCC) regardless of the number of fingerprint being verified. The OCC security status keeps only the status from the last OCC operation.		
OT-38	Oberthur	C. Goyet	T	2	5	381	2.4.2	Biometric data are usually dealt with as Global parameters instead of local ones as their number is limited and to avoid problem when multiple instances are created on a given card. Is there a strong rational from NIST to list finger OCC as local security status indicator? If not , could it be changed to local please? Thanks.	Change security status indicator for OCC from local to global.	Resolved by OT-12.
OT-39	Oberthur	C. Goyet	T	2	5	383	2.4.2	Here the pairing code is said to be local but part 1 gave it a Global ID ('03'). I believe it makes more sense to consider the pairing code as global as done in part 1 instead of local here.	Change pairing code from local to global (if it is not removed completely – see comments on part 1)	Declined. Part 1 specifies that the PIV Secure Messaging Key ('03') is global, but that the pairing code ('98') is local. Whereas the secure messaging that is specified in Section 4 of Part 2 may be used by other card applications, the VCI and the mechanism for establishing it (pairing code) is specific to the PIV Card Application.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-40	Oberthur	C. Goyet	T	2	5	405	2.4.3	If the PUK is of fixed size (8 bytes) there are no more need for padding so why should we exclude FF? Allowing any 8 byte value allows the PUK to be created by a random number generator without requiring any special processing.	Allows the PUK to be a random value of 8 bytes. (i.e. extend the range of each byte to FF)	Accept.
OT-41	Oberthur	C. Goyet	T	2	8	453	3.1.1	The Le field value in the APDU table should be listed as the number of data content bytes to be retrieved instead of the length of application property template. The length of the application property template is variable and not known in advance. Beside to speed up transaction especially in contactless, some application who don't check the FCI returned may want to retrieve only the first few bytes of the application property template. They may also omit Le to instruct the card to perform the selection without returning any data (Besides the status to inform about correct execution).	Replace the text to describe Le with: "number of data content bytes to be retrieved"	Partial read of data object is not supported. To retrieve the entire APT an le field of 0 will do the job. SP 800-73-3 does not support partial read of data object. Part 2 commands will better reflect this.
OT-42	Oberthur	C. Goyet	T	2	9	470	Table 3	See Oberthur comments #32 and 33 on Section C.3 in Part 1 and remove tag AC from the response to Select.	Remove the cryptographic algorithm identifier template 'AC' from the response to Select.	Resolved by OT-32.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-43	Oberthur	C. Goyet	T	2	9	460	Table 3	In addition to the application property template (tag '61') the card may optionally return in the PIV FMD the DO 7F66 to provide extended length buffer size information (see ISO/IEC 7816-4 section 12.7.1 Extended length information) when extended length APDU are supported by the application. Use of extended length APDU allows to cut in half the transaction time to retrieve data or certificate from the PIV application and should be proposed as a preferred alternative to command chaining. Oberthur can do a demonstration to NIST if needed.	Add tag 7F66 extended length buffer size information in the FMD of the PIV application i.e. response to select (same level as tag 61) and define its content as the concatenation of 4 I/O buffer sizes: *'02' L .xx .xx. = DO maximum length of **command** APDU **without** secure messaging* *'02' L .xx .xx. = DO maximum length of **response** APDU **without** secure messaging* *'02' L .xx .xx. = DO maximum length of **command** APDU **with** secure messaging* *'02' L .xx .xx. = DO maximum length of **response** APDU **with** secure messaging.*	Resolved by OT-60 and GSA-3.
OT-44	Oberthur	C. Goyet	T	2	9	470	Table 5	Table 5 of part 1 list only algorithms for on board key generation. The reference should be only SP800-78-4 table 6.2 that does list the 11 algorithms instead of just 4.	Remove reference to Table 5 of part 1.	Accept.
OT-45	Oberthur	C. Goyet	T	2	9	470	Table 5	A card may support ECC for ECDSA but not for ECDH. However both algorithms share the same identifier. How do you tell the difference in this data object?	Add a different value for ECDSA and for ECDH in the list of cryptographic algorithms supported.	Declined. The algorithm identifier '27' or '2E' shows that it is an ECDH function.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-46	Oberthur	C. Goyet	T	2	9	470	Table 5	What is the benefit to add a object identifier with tag 06 mandatory if the value is always set to 00? Most PIV cards will support all algorithms defined in SP800-78 and adding for each of them the object identifier double the size of the Data Object 'AC' and slows down the response to the SELECT PIV application.	Remove, or make optional, object identifier tag 06 from the cryptographic algorithm identifier template 'AC'	Declined. ISO/IEC 7816-4 mandates tag '06'.
OT-47	Oberthur	C. Goyet	T	2	10	481	3.1.2	The APT is already retrieved from the response of the SELECT APDU. What is the rational to introduce another way to retrieve the same data ? This adds complexity for interoperability testing and brings very little benefits.	Remove the APT form the list of DO that can be retrieved with GET DATA.	Accept. Note: a ISO/IEC 7816 compliant card should be able to retrieve the APT with GET DATA APDU.
OT-48	Oberthur	C. Goyet	T	2	10	488	Footnote 4	The GET RESPONSE is not linked to GET DATA and can be used following any command that returns data. The GET RESPONSE command can be used even to retrieve small PIV data object (if "Le" in the Get Data was different from '00', and Large PIV data object can be retrieved without GET DATA by simply using extended length APDU as described in the 1995 edition of ISO/IEC 7816-4 and subsequently moved to ISO/IEC 7816-3.	Replace the sentence with "The GET RESPONSE command is used to retrieve data was not fully returned by the preceeding APDU.	Declined. The footnote is in the context of GET DATA command.
OT-49	Oberthur	C. Goyet	e	2	11	497	3.2.1	This sentence duplicate the paragraph above and can be safely deleted	Delete sentence	Declined. Second sentence is an explicit 'shall' statement and therefore is needed to make the requirements unambiguous.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-50	Oberthur	C. Goyet	T	2	12	534	Command syntax	Use odd INS '21' for biometric verification as this allows greater flexibility to support multimodal biometrics in the future. Even for OCC, a BERTLV command data field would allow to transmit in the command data field : -the actual biometric data (tag '81' containing the minutiae for Finger OCC) - the Biometric Type as per ISO/IEC 19785-1 ('08' for fingerprint but next generation PIV cards could also support '10' for iris and '02' for facial), -the Biometric subtype (aka Finger ID) as per ISO/IEC 19785. This is especially important for the Biometric subtype as this is the only way to the OCC to be performed when 2 fingers are enrolled for OCC and the reader does not know which finger has been scanned: ISO/IEC 19785 allows value 00 for Biometric subtype when the finger ID is not known. The command data field may then be structured as described in the attached contribution from Oberthur called Biometric data template for finger OCC.	Allow both INS = 20 or 21	Declined. SP 800-73-4 will use Even INS only since ISO/IEC 7816-4 does not provide standardized tag for using OCC references in Data Field for Odd INS. Also, see also GSA-3
OT-51	Oberthur	C. Goyet	T	2	12	534	Command syntax	For Biometric verification, the Verify command could P1P2= '00' '00' since the identity of the finger being submitted is now included in the command data field. This frees up some Global Reference data Identifier for future uses.	Set P2 = 00 for OCC.	Resolved by OT-50

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-52	Oberthur	C. Goyet	T	2	13	546	3.2.2	The sentence “If any other key reference value is specified the PIV Card Application shall return the status word '6A 81'.” Is not compatible with cards that support a Global PUK. Please allow the global PUK to be changed.	Allow the global PUK to be changed as well	Resolved by OT-11.
OT-53	Oberthur	C. Goyet	T	2	13	546	3.2.2	Add a sentence to explain how to change the finger OCC.	Add the following sentence: Finger OCC cannot be changed through CHANGE REFERENCE DATA. A PUT DATA command with the new biometric data template 7F2E in the command data field can be used to enroll, update or delete a finger for OCC.	Declined. Card Management (including post issuance updates) is out of scope. A PIV card may use tag 7F2E to enroll, update or delete a finger for OCC, but is not required to.
OT-54	Oberthur	C. Goyet	T	2	13	546	3.2.2	Add a sentence to explain the access conditions to enroll a finger OCC. Since finger OCC is a substitute to PIN verification, why not let the card holder self enroll using the fingerprint scanner connected to its PC? (same logic as giving the card holder the rights to change its PIN value). This will speed up deployment of OCC by not requiring a connection to the CMS to enroll, while letting each user decide to enroll or not.	Set the access condition to enroll a finger for OCC to be either Application Admin Key authentication or PIN verification.	Declined. As per FIPS 201-2, biometric enrollment is done in-person. Subsequent re-enrollment (post issuance updates) to the card require mutual mutually authenticated secure session between the card and the administrator. Also, allowing cardholder to change OCC will weaken the factors of authentication.
OT-55	Oberthur	C. Goyet	T	2	13	552	3.2.2	Add reference 01 for Global PUK	Add reference 01 for Global PUK	Resolved by OT-11. See also GSA-3

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-56	Oberthur	C. Goyet	T	2	13	554	3.2.2	Only the new reference data has to be checked by the card to comply with the Pin Policy. Very often the default value before personalization does not comply with the new PIN policy but is changed to a complying one during perso using the change reference data. If the PIN policy is checked also during the VERIFY, not testing the old value during the CHANGE REFERENCE DATA allows to fix the card are change the PIN to a compliant one.	In the CHANGE REFERENCE DATA command, only the new reference data has to be checked by the card to comply with the Pin Policy.	Resolved by G-10.
OT-57	Oberthur	C. Goyet	T	2	14	574	3.2.2	How do you reset the security status associated to a given finger OCC ? Since it is not possible to “forget” your fingerprints, the most likely cause of a finger OCC locked status is a poor quality enrolment. The best way to fix is by performing a new enrollment. A finger OCC enrollment resets the finger OCC PTC.	State that a finger OCC enrollment resets the finger OCC PTC.	Resolved by stating that a finger OCC enrollment may reset the finger OCC counter.
OT-58	Oberthur	C. Goyet	T	2	14	579	3.2.2	The sentence “Any other key references in P2 shall not be permitted and the PIV Card Application shall return the status word '6A 81'. “ does not allow to reset the Global PIN.	Add the Global PIN to the sentence so it can be reset too.	Declined. Global PIN management is out of scope for PIV card application. See OT-11.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-59	Oberthur	C. Goyet	T	2	15	613	3.2.4	The secure messaging defined in this document is for non card management operation (see section 5.4 of part 1). Secure messaging for card management operation may use more secure cryptography like Opacity FS or Opacity SKM with cryptosuite CS5. It is important to allow other cryptographic identifier if used for card management.	.Remove sentence starting line 615: "If key reference…"	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-60	Oberthur	C. Goyet	T	2	15	623	Footnote 6	Modify footnote to allow use of extended length APDU as an alternative to GET Challenge.	Change footnote 6 with : "For cryptographic operations with larger keys, e.g., RSA 2048, the GET RESPONSE command **may be** used to return the complete result of the cryptographic operation. Extended length APDU may be use as a faster alternative ."	Declined. Extended length support adds another option in PIV specifications that makes interoperability more difficult. See GSA-3.
OT-61	Oberthur	C. Goyet	e	2	18	661	3.3.2	Not all keys listed in Table 4 of part 1 can be generated on card.	Remove reference	Resolved specifying the key references in the P2 row of the affected table, which are the following: '03', '9A', '9C', '9D', '9E'.
OT-62	Oberthur	C. Goyet	e	2	18	668	Table 12	Titled for table 12 should read: " Public encoding for ECC" as both ECDSA and ECDH keys can be on board generated.	Change table 12 title to " Public encoding for ECC"	Accept. Table 11 will also reflect accordingly.
OT-63	Oberthur	C. Goyet	T	2	24	709	Table 13	This table defines algorithm identifiers that are conflicting with ANSI 504. For instance CS2 in ANSI 504 table 19 has two algorithm identifiers: 27 is for Opacity FS and it is 28 that is for Opacity ZKM. Here 27 is use for Opacity ZKM… Such conflict would prevent creating a PIV card on a GICS platform….	Set algorithm for CS2 to '28' to be compliant with ANSI 504.	Declined. Table 23 of ANSI 504 says that '27' is for OPACITY ZKM – Constant 256 and that '28' is for OPACITY FS – Constant 256.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-64	Oberthur	C. Goyet	T	2	24	709	Table 13	CS4 in this table uses the algorithm identifier 2B from ANSI 504 but the algorithm is AES 256 instead of AES 192 in ANSI 504. However the header of the table mentions a 192 bit channel strength for CS4. While AES 192 provides the appropriate level of security strength for these cipher suites, AES 192 is not included in Suite B and it seems this was the reason to jump to AES 256. That brings two comments: - If PIV does not want to use AES192 because it is not included in NSA Suite B, why not simplify the PIV specs and remove AES192 from 800-78-4? - Instead of replacing AES192 with AES256 and having to add a mention that the channel strength is only 192 bit, why not offer a real 256 bit channel strength by moving from CS4 to CS5 ? This would allow to use this secure messaging for card management (i.e. loading of keys that are not generated on-board).	Instead of CS4, use CS5 from ANSI 504 or keep AES192 to be consistent between the encryption algorithm and the actual channel strength.	Declined. Cipher Suite CS5 specifies the use of an ECDH P-256 ICC key agreement key, which, when used with the key establishment protocol in Section 4 of SP 800-73-4 Part 4 would create a secure session with a channel strength of only 128 bits, which is not sufficient for a PIV Card that supports the virtual contact interface and that has ECDH P-384 key management keys. Note: In SP 800-78-4, AES 192 is only permitted for use for symmetric Card Authentication key and the PIV Card Application Administration key, neither of which is intended to provide interagency interoperability. There is no requirement for PIV Cards, Card Management Systems, or relying parties to be able to process this algorithm, except at agencies that have particularly chosen to use this algorithm and key size. Removing this key size option would create an unnecessary burden for any agency that may have already deployed PIV Cards that use AES 192 for one of these keys.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-65	Oberthur	C. Goyet	T	2	24	709	Table 13	What is the use case for CS4? Secure messaging was added to provide a Virtual Contact Interface (VCI) for contactless operation. Most contactless operations include performance requirements that call for a transaction as short as possible, therefore the use of CS2. According to part 1 section 5.4 line 888, the Secure messaging defined by NIST is for non card management operations, so the AES128 encryption provided by CS2 should be more than enough to guarantee the confidentiality of the finger OCC transmitted to the card. CS2 would not be strong enough to protect the loading of AES 192 or AES 256 into the card during personalization, but CS4 provides only 192 bit strength and therefore would be suitable for AES 192 but not AES 256 keys. So there is a need for a stronger secure messaging with AES 256 for card management and personalization, like CS5 from ANSI 504 but used with Opacity ZKM instead of Opacity FS to keep the same protocol as for CS2	Replace CS4 with CS5 from ANSI 504 but use algorithm Identifier = '2E' as this is ZKM and not FS. And allow both a fast secure messaging with CS2 and a strong SM wit hCS5. That means supporting in the PIV card two different secure messaging keys.	Declined. A secure channel with 192 bits of security strength is needed for PIV Cards that support the virtual contact interface and that have ECDH P-384 key management keys. The key establishment protocol in Part 2 of SP 800-73-4 is provided to support non-card-management operations, and there are no non-card-management operations that require more than 192 bits of security strength.
OT-66	Oberthur	C. Goyet	T	1	16		Table 3	For greater interoperability of the PIV application, you may want to add to this list of data objects the ACD (tag 7F63) and CCD (tag 7F62) from ISO/IEC 24727.	Add ACD and/or CCD from ISO/IEC 24727.	Declined. Discoverability of the PIV Card application's capabilities is already provided by the Discovery Object. Duplicate data object should be avoided. See GSA-3.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
OT-67	Oberthur	C. Goyet	T	1	20	881		It is stated that "All other cryptographic mechanism identifier values are reserved for future use". This statement raises an additional issue as SP800-73-4 defines the interface for a PIV application and not for a card operating system. Card management commands to personalize the PIV application may use cryptographic mechanisms outside of the scope of SP800-73-4. So instead of saying that all other cryptographic mechanism identifier values are reserved for future use, could you just say that All other cryptographic mechanism identifier values should not be used for interoperability.	Replace that sentence with "All other cryptographic mechanism identifier values should not be used for interoperability."	Resolved by OT-35.
OT-68	Oberthur	C. Goyet	T	2	25	717	Table 14	Add in the CVC tag 5F50 to provide inside the CVC the URL to verify the opacity protocol signature without having to issue a separate command. See Oberthur comment #6	Add in the CVC tag 5F50 that was initially in the discovery object.	Resolved by OT-8
SCA-1	Smart Card Alliance	Stephan Ardiley	T	1	20	880	Table 5 "06"	RSA 1024 will sunset Dec 31 2013 to be replaced with RSA 2048 keys which are longer and will require additional time at an access control reader.	Allow ECC P224 in appropriate use cases. This will minimize transaction time and increase throughput.	Resolved by HID-4. See also GSA-3.
SCA-2	Smart Card Alliance	Bob Fontana	T	1		868	5.1.2.	The content signing certificate needed to verify the digital signature of a CVC of a valid PIV Card shall not be expired.	Expand to: The content signing certificate shall never expire before any of its signed content expires. This needs to apply to all content not just the secure messaging	Declined. The current text is consistent with FIPS 201-2, which states that the content signing certificate on a valid PIV Card shall not be expired. This language allows for the case in which the data on a PIV Card is re-signed in the middle of the card's lifetime (e.g., at the same time that the X.509 certificates are re-keyed), thus allowing more flexibility for the issuer without adding complexity for the relying party.
SCA-3	Smart Card Alliance	Stephan Ardiley	T	1		853	5.1.2. 1	If the PIV Card supports secure messaging, the PIV Secure Messaging key shall be generated on the PIV Card and the PIV Card shall not permit exportation of the PIV Secure Messaging key.	Provide clarification as to when the Card Auth key vs. secure messaging key is used.	Noted. See Section 3.2.4, Part 2 of SP 800-73-4.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
SCA-4	Smart Card Alliance	Lars Suneborn	T	1	7	541	3.1.3	The Public Key Infrastructure (PKI) cryptographic function (see Table 4) is protected with a Personal Identification Number (PIN) or On-Card biometric Comparison (OCC) access rule. In other words, private key operations using the PIV Authentication key require the PIN or OCC data to be submitted and verified, but a successful submission enables multiple private key operations without additional cardholder consent.	Change to: The Public Key Infrastructure (PKI) cryptographic function (see Table 4) is protected with a Personal Identification Number (PIN) or On-Card biometric Comparison (OCC) access rule. In other words, private key operations using the PIV Authentication key require the PIN or OCC data to be submitted and verified, but a successful submission enables multiple private key operations without additional cardholder consent during the same, uninterrupted session.	Declined. The proposed added text does not serve to clarify the requirement, especially since subsequent operations may be performed based on the security status of the Global PIN being TRUE even after the application session has ended, since the security status of the Global PIN is not affected by the selection of another card application.
SCA-5	Smart Card Alliance	Lars Suneborn	G	1	7	547	3.1.4	The PKI cryptographic function (see Table 4) is protected with an “Always” access rule. In other words, private key operations can performed without access control restrictions.	Change to: The PKI cryptographic function (see Table 4) is under an “Always” access rule. Private key operations can be performed without access control restrictions.	Resolved by changing the sentence to: "The PKI cryptographic function (see Table 4) is under an “Always” access rule, and thus private key operations can be performed without access control restrictions."
SCA-6	Smart Card Alliance	Lars Suneborn	T	1	12	738	3.4	This specification provides support for two UUIDs on a PIV Card. The Card UUID is a UUID that is unique for each card, and it shall be present on all PIV Cards. The Cardholder UUID is a UUID that is a persistent identifier for the cardholder, and it is optional to implement. The requirements for these UUIDs are provided in the following subsections.	This specification provides support for two UUIDs on a PIV Card. The Card UUID is a UUID that is unique for each card, and it shall be present on all PIV Cards. The Cardholder UUID is a UUID that is a persistent identifier for the cardholder, and it is optional to implement. For PACS interoperability, the Card UUID can be used. The requirements for these UUIDs are provided in the following subsections.	Declined. Asserting that the Card UUID can be used for PACS interoperability may be controversial, since it will be several years before all valid PIV Cards include a Card UUID.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
SCA-7	Smart Card Alliance	Adam Shane	T	1	12	736	3.4	Need to make clear that the Card UUID is not the card unique identifier.	Add statement that the Card UUID is not the card unique identifier.	Declined. The term "card unique identifier" does not appear in SP 800-73-4 (or FIPS 201), so there cannot be a need to make clear that the Card UUID is not the card unique identifier.
SCA-8	Smart Card Alliance	Lars Suneborn	T	1	12	750	3.4	Please clarify which identifier is intended to be used for PACS.	Please clarify which identifier is intended to be used for PACS.	Noted. It would not be appropriate for NIST to attempt to restrict which unique identifier(s) a PACS uses, although for interoperability reasons, a PACS should be capable of accepting any valid PIV Card, even one that does not contain some optional unique identifiers or unique identifier that were previously optional. Revised NIST SP 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), will addresses your question in great detail.
SCA-9	Smart Card Alliance	Lars Suneborn	G	1	43	1119	Appendix B, Table 41,Summary. Asymmetric CAK, card holder Validation steps	Column Cardholder Validation Steps (Holder V) Posession of Card The heading of column 4 (Cardholder Validation Steps is unclear. Some of the examples does not validate the card holder.) Asymmetric CAK does not bind the card to a specific cardholder.	Change to: Possession of card alone does not provide cardholder validation.	Declined. SP 800-63 recognizes three factors of authentication. A challenge/response with the asymmetric CAK is a demonstration that the entity responding to the challenge is in possession of the PIV Card, and this counts as one factor of authentication ("something you have") of the cardholder.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
SCA-10	Smart Card Alliance		G	1	43	1119	Appendix B, Table 41, Summary. Symmetric CAK, card holder Validation steps	Column Cardholder Validation Steps (Holder V) Possession of Card (See # 9 above). Symmetric CAK does not bind the card to a specific card holder.	Change to: Possession of card alone does not provide cardholder validation.	Resolved by SCA-9.
SCA-11	Smart Card Alliance	Lars Suneborn	G	1	43	1119	Appendix B, Table 41, Summary CHUID Validation	Column Cardholder Validation Steps (Holder V) Posession of Card (See # 9 above).CHUID Validation does not bind the card to a specific card holder.	Change to: Possession of card alone does not provide cardholder validation.	Resolved by SCA-9.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
SCA-12	Smart Card Alliance	Lars Suneborn	G	1	2	367	1.3 Effective date	The requirement to enforce minimum length for the PINs, pairing code, and PUK, at the card level is a security requirement that did not appear in previous versions of SP 800-73. This is inconsistent with bullet 9, Revision History Table pg. v. : DoD does not see any value of using the paring code. There is not a credible use case that warrants the added technology implementation issues. We see very little risk once the secure contactless interface is established using Diffie-Hellman and therefore will strongly non-concur with anything stronger than saying that the use of the paring key is optional and will be based on the risk profile that individual agencies are comfortable with. The value of the card validating the terminal is of little value to DoD when evaluating the use cases expected for future applications, as compared to the technical changes required to implement such a method.	The requirement to enforce minimum length for the PINs, pairing code, and PUK, at the card level is a security requirement that did not appear in previous versions of SP 800-73. Biometric OCC using the contactless interface does not require a PIN entry. The PIN/Pairing code creates usability challenges across its use cases. Does this need to be a different PIN and if not does this need to be entered twice? Can the biometric OCC be used in lieu of a pairing code or PIN across the use cases? The pairing code concept shall be optional until at least validated through practical future applications.	Noted. Bullet 11 in the Revision History notes that card level enforcement of length requirement for PINs is new. Draft SP 800-73-4 permits biometric OCC to be performed over the contactless interface without PIN or pairing code entry. While pairing code is optional to implement, it is mandatory to implement those use cases that require a virtual contact interface. Biometric OCC may not be used in lieu of a pairing code or PIN. The access control rules specified in SP 800-73-4 shall be implemented as specified. DoD has noted in its own comments that it non-concurs with the requirement to implement the pairing code in order to enable access to the full functionality of the PIV Card over the contactless interface. However, OMB and the Federal CIO Privacy Council have indicated that the X.509 certificates (other than the Card Authentication certificate) contain personally identifiable information that needs to be protected against unauthorized access (skimming), and that the establishment of a one-way (card-to-host) authenticated secure channel is not sufficient to meet this requirement. Per HSPD-12, the requirement to protect privacy is mandatory and thus cannot be optional based on individual agencies' risk profiles.

#	Organization	Commentor	Type	73-4 Part #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	NIST Resolution/Response
SCA-13	Smart Card Alliance	Lars Suneborn	G	1	18	831	Table 4 "9A" Contact less	VCI and (PIN or OCC) This creates an additional Card PIN that a user must remember and enter at an access control point. The result is inconsistent PIN entry processes, additional delays, additional opportunity for PIN confusion and PIN entry errors with resulting lock out that requires PIN reset operations.	See comment 11 above	Resolved by adding additional clarifying text about use of the pairing code. See also G-17 and HID-5.
SCA-14	Smart Card Alliance	Lars Suneborn	G	1	18	831	Table 4 "9C" Contact less	VCI and (PIN Always or OCC Always) This creates an additional Card PIN that a user must remember enter. The result is inconsistent PIN entry processes, additional delays, additional opportunity for PIN confusion and PIN entry errors with resulting lock out that requires PIN reset operations.	SM and PIV Card Application PIN or OCC Always.	Resolved by SCA-13.
SCA-15	Smart Card Alliance	Lars Suneborn	G	1	18	831	Table 4, "9D"	See 11 above	See 11 above	Resolved by SCA-13.
SCA-16	Smart Card Alliance	Lars Suneborn	G	1	18	831	Table 4, Retired Key Management Key	See 11 above	See 11 above	Resolved by SCA-13.
SCA-17	Smart Card Alliance	Lars Suneborn	G	1	9	630	3.3.8 Discovery Object	Bit 5 indicates whether the pairing code is implemented.	Bit 5 indicates whether the optional pairing code is implemented.	Accept
SCA-18	Smart Card Alliance	Sal D'Agostino	T	2	20/26	685	4.1 Key Establishment Protocol	The key establishment protocol….	Interoperability would be better served using algorithms other than ECC as described =Z; as an example RSA could be used. It is not obvious that the tradeoff needs to be completely geared toward performance. Related to balance of sections of in 4.1	There has been substantial support for the adoption of OPACITY as the key establishment protocol, and OPACITY only works with ECC.

List of Organizations

DoD	Department of Defense
E	Entrust
ES	Electrosoft
G	Gemalto
GSA	General Services Administration
HID	HID Global
IG	InfoGuard
NSA	National Security Agency
OT	Oberthur
SCA	Smart Card Alliance