#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
1	CFPB	Arash Nejadian				2.2, 2.4	PIV Card Credential Usage	Language should be added to address real-time certificate validation for PIV derived credentials. Credential Usage should be added as part of the PIV Derived lifecycle and certificate validation should be expanded on.	Resolved by comment #78.
2	CFPB	Arash Nejadian		24		Appendix D	Change “PIV Derived Application” to “PIV Derived Hosting Application” or “PIV Derived Client” in Appendix D.	PIV Derived Application: A standardized application residing on a removable, hardware cryptographic 805 token that hosts a Derived PIV Credential and associated mandatory and optional elements.	Declined. The term "PIV Derived Application" was specifically selected to mirror the terminology of the PIV Card. PIV Card Application refers to the application on the PIV card as specified in NIST SP 800-73-4 Part 2.
3	Coast Guard	James F Kelleher				3.4.1	Hardware Implementation requirements	While I realize that higher levels of security require stronger protections should not the basics be the same, especially when it concerns repeated unsuccessful activation attempts?	Resolved by comment #4. Note: The term has since changed to "Derived PIV Application" to align with "Derived PIV Credential".
4	Coast Guard	James F Kelleher				3.4.2	Software Implementation requirements	"While I realize that higher levels of security require stronger protections should not the basics be the same, especially when it concerns repeated unsuccessful activation attempts?"	Resolved by adding a requirement for a blocking mechanism to be used with software implementations in section 3.4.
5	POMCOR	Karen Lewison, Francisco Corella				1.2	Implement suggested solution for LOA 3 Credentials	SP 800-157 is ambiguous as to whether derived credentials include email-related credentials, i.e. digitial signature and key management private keys and associated certificates such as those present in a PIV card. Section 1.2 states that only the PIV Derived Authentication certificate is a Derived PIV Credential. But the informative Appendix A states that "a subscriber who has been issued a PIV Derived Authentication certificate for use with a mobile device may also have a need to use a digital signature and key management key with that mobile device." And the PIV Derived Application Data Model of normative Appendix B includes the digital signature private key and certificate, and both current and retired key management private keys and certificates.	Resolved by copying the last sentence of Section 1.2 to the end of the 2nd paragraph of Section 1.2. Note: Digital signature and key management certificates are not Derived PIV Credentials. The Derived PIV Authentication certificate (aka the Derived PIV Credential) is the only new PIV credential defined in Draft SP 800-157. Note: Draft SP 800-157 includes an informative appendix (Appendix A) that discusses digital signature and key management certificates in order to ensure that readers do not misinterpret Draft SP 800-157 as precluding the use of digital signature and key management certificates on the same devices as Derived PIV Credentials are used.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
6	POMCOR	Karen Lewison, Francisco Corella				General		Email reading, and to some extent writing, has traditionally been the main business use of mobile devices. Therefore users with email accounts need email-related credentials on their mobile devices as much as an authentication credential. Email-related credentials should be called derived credentials, and guidance related to them should be normative rather than informative.	Declined. HSPD-12 required the development of a Standard (FIPS 201) and specified that “the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems.” The purpose of SP 800-157 is to define a credential that is part the Standard that is practicable for use in gaining local access to Federally controlled information systems from mobile devices. SP 800-157 acknowledges the importance of digital signature and key management certificates and private keys by including information about them and by providing for the ability to store and use them within the PIV Derived Application. The fact that, other than the specification of the PIV Derived Application data model, information about digital signature and key management certificates is informative is not intended to imply that these credentials are less important than the Derived PIV Credential, just that they are not within the scope of this particular publication. Also see comment #5.
7	POMCOR	Karen Lewison, Francisco Corella				General		Guidance on the current and retired key management keys should explain that they must be the same as those on a PIV card because they must be used to decrypt the same collection of email messages, including old email messages that have been saved encrypted, and should specify or at least suggest that they should be downloaded from an escrow server.	Resolved by adding text to Appendix A about retired key management keys. "The retired keys should be the same as those on the PIV Card." Appendix A already notes that for most Subscribers it will be necessary for the key management key on mobile device to be the same as the one on the PIV Card and encourages the use of key recovery mechanisms. As Appendix A is informative, it cannot impose a requirement (i.e., a “must” or “shall” statement) that the same key management key be stored on both the mobile device and the PIV Card.
8	POMCOR	Karen Lewison, Francisco Corella				General		The PIV Derived Application Data Model might allow for the storage of more than 20 retired key management keys and certificates, since the constraints that limit the number of retired keys and certificates in PIV cards may not exist in mobile devices.	Declined. As noted in the response to DoD-28 in http://csrc.nist.gov/publications/fips/fips201-2/fips201_2_2012_draft_comments_and_dispositions.pdf, ISO/IEC 7816-4 limits each card application to 32 local key reference values. The PIV Derived Application and the PIV Card Application both limit the number of retired key management keys for the same reason, the limited number of available key reference values.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
9	POMCOR	Karen Lewison, Francisco Corella				General		The device-authentication credential can consist, for example, of a DSA key pair whose public key is registered with the back-end, coupled with a handle that refers to a device record where the back-end stores a hash of the registered public key. In that case the protocredential consists of the device record handle, the DSA domain parameters specified in Section 4.3 of the Digital Signature Standard (DSS) [9] and a random high-entropy salt. To regenerate the DSA key pair, a fast key derivation function such as HKDF [10] is used to compute an intermediate key-pair regeneration key (KPRK) from the activation PIN or password and the salt, then the DSA private and public keys are computed as specified in Appendix B.1.1 of the DSS, substituting the KPRK for the random string returned_bits. To authenticate to the back-end and retrieve the high-entropy key, the mobile device establishes a TLS connection to the back-end, over which it sends the device record handle, the DSA public key, and a signature computed with the DSA private key on a challenge derived from the TLS master secret. The DSA public and private keys are deleted after authentication, and the back-end keeps the public key confidential. An adversary who is able to capture the device and extract the protocredential has no means of testing guesses of the PIN or password other than regenerating the DSA key pair and attempting online	Declined. OMB Memorandum M-11-11 states that "Agency processes must accept and electronically verify PIV credentials issued by other federal agencies." The scheme that is described in this scheme would result in the creation of a PIV credential that could only be electronically verified by the agency that issued the credential, which would be inconsistent with M-11-11.
10	OT	Christophe Goyet	E	12	467	3.3	The use of the term "native" in this context is ambiguous as in Smart Card environment, it refers to a low level code specific to the hardware being used, as opposed to Java for instance. In your case, I believe you do not mean to exclude java as it is the language of Android applications, or do you?	Replace "using the native cryptographic interface of the mobile device;" with "using the underlying cryptographic interface of the mobile device;"	Accept
11	OT	Christophe Goyet	T	13	501	3.3.1.1	"The secure element used for the PIV Derived Application shall support the Advanced Security SD (ASSD)". Unfortunately it looks that the ASSD has been loosing traction lately amongst the microSD vendors and is no longer offered by many suppliers. I was told that even G&D who used to be a strong supporter of ASSD has removed this product from their offering in favor of a MicroSD with a non ASSD compliant interface.	An alternative solution can be seek-for-android devices based on SIM alliance openMobileAPI that allows plugin terminals to be developed by MicroSD provider.	Resolved by removing the requirement for ASSD since it is not widely supported. It should be noted that since there is no widely adopted interoperable standard transport mechanism to cite, Derived PIV Credentials on SD card variants may not be easily ported from one device type to another. Update text in section 3.3.1.1 to note that there is no widely supported transport mechanism for SD cards and as such there may be limited portability of the token.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
12	OT	Christophe Goyet	T	14	519	3.3.1.2	Are you refering to OTA as a generic term or as the OTA (Over the Air) as standardized term that refers to a baseband to update smart card using SMS as specified by NFC? Size of SMS is limited and if you want to personalize the derived credential with a 3KB certificate, you may run into problems. We would suggest not to restrict to OTA only but allow Web services Over the Internet (OTI) as it is easier to use, faster, and more important independant of the MNO.	Allow webservices with OTI in addition to OTA .	Resolved by removing "via over-the-air (OTA) mechanisms"
13	OT	Christophe Goyet	T	15	558	3.4.1	"When the private key corresponding to the Derived PIV Credential is stored in a (removable or embedded) hardware cryptographic module, Personal Identification Number based (PIN-based) Subscriber activation shall be implemented." Why do you preclude OCC now that it is authorized by FIPS 201-2?	Allow OCC as an alternative to PIN when supported by the token.	Noted. Additional token activation methods will be considered in the next version of this document.
14	OT	Christophe Goyet	T	18	631	B.1.1	Having an AID different from the PIV card application AID may break compatibility with existing PIV middleware, unless the difference is limited to the last two bytes (version number) . For instance Microsoft discovery process select PIV with the PIV AID minus the least significant two bytes. In addition to breaking compatibility with existing middleware, a different AID will not allow the token to emulate a PIV card as authorized in lines 467 to 470 bottom of page 12. If you really want a separate AID, it may be wise to add to SP800-73-4 a requirement that middleware shall select the PIV application using partial AID only, compatible with both PIV and PIV derived application, and specify that partial AID.	Use the same AID. Distinction between a PIV card and a derived credential could be achieved in a differnet way, like for instance use of the CHUID container (currently not included) but with a specific value. Or update SP800-73-4 to require PIV middleware to select the PIV application using only partial AID.	Declined. If the PIV Derived Application used the same AID as the PIV Card Application, it could cause problems for existing PIV middleware that expects certain data objects that are mandatory for the PIV Card Application to be present (e.g., the CHUID, Card Capability Container, or Cardholder Fingerprints). Using a different AID alerts middleware that the PIV Derived Application does not follow the PIV Card Application data model. For this reason using an AID that differs only in version number and then requiring PIV middleware to select the application using only a partial AID would not be a solution.
15	OT	Christophe Goyet	T	20	700	B.1.2.1	"References to contactless interface are not applicable" That may create a problem in case the token is used for card emulation. For instance, if the smart phone emulates a PIV card using the token to get access to buildings through contactless access control readers, should this transaction relies on access conditions for contact transactions, or a contactless transaction that require the use of FIPS 201-2 VCI?	The PIV derived application should be able to adjust its access control rules depending on whether the token is accessed from a application run locally on the mobile device or from the mobile device NFC interface.	Noted. As noted in Section 1.2, “The scope of the Derived PIV Credential is to provide PIV-enabled authentication services on the mobile device to authenticate the credential holder logically to remote systems.” Based on current policy, the Derived PIV Credential should only be used “where use of a PIV Card is not practical.” Thus, the PIV Derived Application should not be accessed over the mobile device's NFC interface, as any use case involving accessing the PIV Derived Application over an NFC interface (e.g., getting access to buildings) would be a use case in which it would be practical to use the PIV Card. NIST IR 7981, Section 5 (A Look in the Future), acknowledges that other use-cases may be considered in the future. However in their current state Derived PIV credentials are restricted to authentication of mobile devices to remote systems.
16	OT	Christophe Goyet			701	B.1.2.1	Today, embedded security elements are available in all Galaxy S4 from Samsung and Nexus from Google. These eSE are GlobalPlatform chips on which a PIV applet can be loaded. Applets in an eSE can be accessed via contactless interface if APDUs come from RF, but also via ISO as we simulate an ISO connection when APDUs come from the application processor. So it is possible for the applet on the eSE to behave differently depending on the application.	Allow the token to communicate in contact or/and a contactless mode.	Resolved by comment #15

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
17	OT	Christophe Goyet			717	B.1.4.2	Table B-2 does not list the Card Authentication key. Is that on purpose? Being able to use the mobile phone token to access facilities with the key 9E could be considered a valuable feature.	Add card authentication key 9E in table B-2	Resolved by comment #15
18	OT	Christophe Goyet			714	B.1.4.2	Does the PIV derived application has the same requirement regarding PIN policy (e.e. numeric only, 8 digit max etc…)?	State that the PIV derived application has the same PIN policy as described in SP800-73 part 2.	Resolved by adding text to Appendix B.2 clarifying the requirements of the PIV Card Application Password.
19	OT	A. Webb			682 and 686 and 702	B.1.2	1) The primary purpose of the security object in PIV is to link signed biometric objects with signed cryptographic objects. There are no biometric objects in derived PIV. This design allows the trio of signed security object, discovery object, and key history to be harmlessly copied from legitimate data models and placed on a counterfeit card. 2) It also allows detection of modification of unsigned objects. However, for the derived PIV data model, changing the discovery object or key history object is not harmful. The attack of changing the offCardCertURL to an arbitrary URL could also be done by manipulating a certificate. Adding a security object that differs from the 800-73 data model, which probably won't be used operationally, and that requires conformance testing is a needless burden.	Drop the security object in the derived PIV data model. If not, then have 800-73-4 allow moving the issuer certificate from the CHUID to the security object.	Declined. The Security Object is needed to protect the offCardCertURL included in the Key History Object. Please refer to page 3 of NISTIR 7676 for more information.
20	Precise Biometrics Inc	Jeff Scott	G	i	82-87	Authority	We assume that M-07-16 must be updated before this document is finalized		Noted. Appendix C (now Appendix D) states that "guidance will be made available by OMB to provide an alternative to the remote authentication policy in M-06-16 and M-07-16." It is an OMB decision whether this future guidance will be provided as an update to M-07-16 or in another form. The timing of the publication of the final version of SP 800-157 will be coordinated with OMB.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
21	Precise Biometrics Inc	Jeff Scott	G	iv	201	Executive Summary	"separate card readers" indicate readers that are (temporarily) connected to the device. Form fitted cases with including smart card readers should also be mentioned since they are more user friendly. The same smart card readers could also be used both for mobile device and PC	change to "separate card readers or form fitted cases"	Resolved by changing the two sentences starting on line 201 (line 181 in final document) to: "Mobile devices lack the integrated smart card readers found in laptop and desktop computers and require card readers attached to devices to provide authentication services from the device. For some department and agencies, the use of PIV Cards and attached card readers is a practical solution for authentication from mobile devices. Removed the first separate and changed the second to "attached"
22	Precise Biometrics Inc	Jeff Scott	G	iv	208	Executive Summary	"impractical" Although mentioned in the introduction (lines 239-240) that there are cases where it may be practical to use the PIV card, you can get the feeling by reading the document and the executive summary, that this is not often the case. Practical, currently available, approaches such as form fitted cases for mobile devices both adding functionality and protecting the devices are ignored.		Noted. Out-of-scope for this document. This topic is covered in NISTIR 7981.
23	Precise Biometrics Inc	Jeff Scott	G	5	236	1.1	"achieving substantial cost savings" This is a subjective statement - are there any calculations on the cost involved in implementing and managing derived credentials? A card reader solution would require no investment in and management of new credentials and the same card reader can be used both on the mobile device and the PC thus making it very cost effective		Noted. The cost savings discussed here is the savings from reuse of the PIV Identity proofing.
24	Precise Biometrics Inc	Jeff Scott	G	5	247-248	1.1	An additional advantage is that it already adheres to M-07-16	add "and already adhereing to M-07-16"	Noted. M-07-16 is covered in Appendix C (now Appendix D) of SP 800-157 and NISTIR 7981.
25	Precise Biometrics Inc	Jeff Scott	G	5	248-249	1.1	Form fitted cases with smart card readers should be mentioned since, even if they formally are "separate from, but attached to" the mobile device in practice they are always attached to the device and almost becomes part of the device.		Resolved by replacing the sentence starting on line 248: "The approach requires smart card readers that are separate from, but attached to, the mobile device itself."
26	Precise Biometrics Inc	Jeff Scott	G	6	268	1.2	FIPS 201-2 specifies different authentication mechanisms that can be used to fulfill LOA 4. This document limits the LOA 4 authentication mechanism to PIV-AUTH. FIPS 201 also states that different authentication mechanisms can be used together as multiple authentication factors to achieve even higher authentication confidence at LOA 4. This granular multi factor authentication mechanism is not feasible in SP800-157 even if “card readers or NFC, is deemed impracticable”.	"and where granular authentication mechanisms at LOA 4 aren't required" after "deemed impracticable"	Declined. Draft SP 800-157 is aligned with FIPS 201-2 and SP 800-63. Table 6.3 of FIPS 201-2 lists the different Authentication Mechanisms applicable to Logical Access control. While there are several authentication mechanisms listed for local workstation environment (such as BIO, OCC, PKI Auth), only PKI-Auth is listed for "remote access control. Biometric authentication is not applicable to remote access control (as per SP 800-63:) because it uses information that is private rather than secret. Their security is often weak or difficult to quantify, especially in the remote situations.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
27	Precise Biometrics Inc	Jeff Scott	G	9	349-360	2.1	Has the following approach been considered? A LOA 4 derived credential could be remotely issued together with fingerprint templates collected at the time the PIV-card was issued and activated remotely using OCC-AUTH. This would be in line with remote resetting a PIV card using OCC-AUTH.		Noted. In order to maintain the same level of identity assurance as the PIV Card at LOA-4, the in-person issuance requirement of the PIV Card is being implemented within this document for Derived PIV Credentials at LOA-4.
28	Precise Biometrics Inc	Jeff Scott	T	14	534-537	3.3.1.3	The CCID standard is for smart card readers, a reader with a slot where a smart card can be inserted. The smart card like secure element cannot be removed from a USB token. Such a device already has an approved USB device class, namely ICCD, and this should be used instead of CCID.	Suggested that CCID should be changed to ICCD	Accept.
29	Precise Biometrics Inc	Jeff Scott	G	16	590	3.4.2	Alternative approach: Lockout mechanisms could be used for LOA 3 software as well. Unlocking mechanisms could be OCC-AUTH or a remote reset using BIO.		Resolved by comments #127 and #4.
30	Precise Biometrics Inc	Jeff Scott	G	18	645	B.1.2	Are the data objects listed here the only allowed optional data objects? Are SP800-73-3 objects such as Cardholder Fingerprints, Cardholder Iris images and Cardholder Facial Image implicitly forbidden to be stored in the derived PIV application by not being listed here?		Yes. Appendix B lists one mandatory data object and several optional data objects. As the definition of the PIV Derived Application neither mandates nor provides the option to include any other data objects, no other data objects may be included in the PIV Derived Application.
31	DOJ	Kyle T. Baughman				General	Smartphone Access Issue: and getting codes to access VPN and no place to put PIV card information in smartphone.	No Suggested Text	Noted
41	DOJ	Mike Fuller	content	iv		footer	Mobile definition in the footer can easily apply to laptops. Is this the intent or should that be differentiated?	Either unambiguously state that laptops are included, or refine the definition to not cover laptops.	Noted. Computing devices evolve over time. It is up to the agencies to decide what types of devices fall into the mobile category and where the use of the PIV card is impractical
42	DOJ	Adam Salerno	content	10	382-389	2.2	The maintenance on derived credentials mentions that the PIV credential issuance/revocation is decoupled from the derived PIV maintenance, however it does not call out effectively how important this management process is when considering IT security risks with compromised PIV or Derived credentials	Recommend adding a sentence or two describing possible attack vectors or concerns around the separate nature of these two credentials, and/or emphasizing the process to manage Derived credentials in relation to the PIV credential.	Resolved by comment #307.
49	DOJ	Edward Siewick	N.B.	11	411..413	2.4	FIPS 201 (next draft) ought to be modified to close this "no need to revoke" loophole (sec 2.5.2). CNSSI 1300 sec 4.9.3 has the same loophole, btw. However, NSS PKI RPS sec 4.9.3 tightens CNSSI 1300 requirement, explicitly closing the loophole: *"For hardware certificates, the RA Officer revokes all certificates when the token is turned in or the RA Officer is notified that the Subscriber no longer has a requirement regardless of whether the token is turned in or not. If the token is not turned in or the token is not protected from malicious activity prior to zeroization, the reason code for the revocation is 'compromise.' "*	n/c to SP800-157	Out-of-Scope. See resolution comment and resolution to DoD-25, DHS-5, DoE-54 and ICAM SC-25 from the FIPS 201-2 (first draft) comments at http://csrc.nist.gov/publications/fips/fips201-2/fips201_2_2011_draft_comments_and_dispositions.pdf (last column) for the request to reduce the size of CRLs by collected and destroying associated keys, rather than revoking associated certificates.
51	DOJ	Edward Siewick	content	11	n/a	2.4	There is no requirement to periodically reconcile the status across the entire population of fielded Derived PIV Credentials with the authoritative store for status records for the PIV Cards.	Add a periodic reconciliation procedure requirement.	Noted. Derived PIV Credential issuers are required to maintain a linkage between the Derived PIV Credential and the credential holder's ability to hold a PIV Card. See section 2.4.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
52	DOJ	Edward Siewick	conte nt	12	436..441	3.1	LOA-3, LOA-4, etc., should be used consistently as labels for only the OMB m04-04 and SP800-63 "Levels." There is a risk of conflating the labels used in the draft for "Levels" for e-Authentication identity proofing and token issuance methods as described in OMB 04-04 and SP800-63, and the similarly labeled security Levels regarding the hardening for cryptomodules provided in FIPS 140-2. COMMON refers to FIPS 140-2 in section 6.2.1 in connection with "id-fpki-common-pivAuth-derived-hardware" and "id-fpki-common-pivAuth-derived" policies. 436..441 makes this hard to parse out. Also, beware the SP800-63 mapping isn't LOA-3 to Level 3, LOA-4 to Level 4. The draft suggests this, though.	Use the "LOA-[3,4]" labels througout as references to SP800-63 Levels. Re-write the paragraph to use the alignments of e-Auth levels with the FIPS 140-2 levels as already specified in SP800-63-1, and section 3.2 of the draft.	Noted. Draft SP 800-157 only uses LOA-[3,4] to refer to M-04-04/SP 800-63 assurance levels. Section 3.1 in Draft SP 800-157 is only referring to M-04-04/SP 800-63 assurance levels and is noting the correspondence between certificate policies an e-Authentication assurance levels. Section 3.2 of Draft SP 800-157 specifies the cryptographic module validation requirements as [FIPS 140] Level 2 with Level 3 physical security when certificates are issued under the id-fpki-common-pivAuth-derived-hardware policy and [FIPS 140] Level 1 when certificates are issued under the id-fpki-common-pivAuth-derived policy. At no point does the draft suggest certificates issued under id-fpki-common-pivAuth-derived-hardware require the use of a [FIPS 140] Level 4 validated cryptographic module or that certificates issued under id-fpki-common-pivAuth-derived require the use of a [FIPS 140] Level 3 cryptographic module.
53	DOJ	Edward Siewick	conte nt	12	444..446	3.1	The language unlinks the PIV Derived Credentials from expiration events pertaining to the FIPS 201 certs. The statement needs better bounding. As written, it completely obviates the need for linkage to the status of the PKI certs or PIV Cards as developed in section 2.4. Presumeably, many FIPS 201 use cases that call for termination of a PIV Card should also trigger termination of the PIV Derived Credential.	The paragraph should be re-written to allow the term of validity for the PIV Derived Credential to stradle multiple validity terms of the FIPS 201 certs. However, if an expired FIPS 201 cert isn't replaced, the use case should require revokation of the PIV Derived Credential.	Noted. Derived PIV Credential issuers are required to maintain a linkage between the Derived PIV Credential and the credential holder's ability to hold a PIV Card. See Section 2.4. Issuers are allowed to vary the validity of the Derived PIV Credential. Also see comment #107.
55	DOJ	Edward Siewick	nit	15	563	3.4.1	LoA-4	adjust to LOA-4 for consistency.	Accept

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
56	Secure Access Technologies	Ben Ayed		5	254	1.1	2FA Soft Tokens that use (Internet - non Bluetooth) to communicate with the data terminal were not discussed as part of new technologies. Bluetooth LE Soft Tokens were not discussed as part of new technologies. Bluetooth LE Hard Tokens were not discussed as part of new technologies. RE: Bluetooth LE / Bluetooth Low Energy / iBeacon: Bluetooth LE is DIFFERENT from Bluetooth 2.0 and does not have ANY of the security concerns of Bluetooth 2.0. This is a high-security technology that is available on ALL major-brand mobile devices today. It provides similar functions to NFC, plus encrypted communication, plus proximity security and a LOT more. For example, proximity security prevents device loss and locks data when the user is not there. SecureAccessTechnologies.com provides an Adaptive 2FA Soft Token that communicates with any data terminal using ANY transport technology: Internet communication, Bluetooth LE, as well as RSA SecurID for Manual and Voice Authentication for Non-Repudiation. It guarantees accessibility with 2FA under ANY condition. The user experience is much superior than simple passwords because the user does not need to type a password everytime the device locks -generally forced by MDM- and which results in the users typing passwords 20-50 times a day, a lot of password resets, etc.	2FA Soft Tokens (Non Bluetooth), 2FA Bluetooth LE Tokens and BT LE Hard Tokens are commercially available with the following features: - These 3 tokens work with MOST major mobile device brands TODAY including Apple, Samsung, Microsoft - Provide continuous authentication and device loss prevention	Noted. We will consider including new/different type(s) of tokens for next revision of SP 800-157.
57	Secure Access Technologies	Ben Ayed		6	281	1.2	The current figure1-1 is very similar to MDM architecture... and seems to substitute or append a Derived PIV Credential to the MDM certificate. This figure gets rid of at least one authenticate factor compare to the current PIV model because the derived PIV credential is installed on the data device, and is "something the device has", and not "something the user has". This model does not maintain the existing security posture (2FA) of PIV cards, and use the old password model that says "Anybody that types the correct PIN on the government device, you will gain access to government data". Please note that with mobile devices: - How is this architecture going to ensure that the person in front of the government mobile device is a legitimate user and not an attacker?... Perhaps the device is lost and the user has not reported it, perhaps the attacker has recorded the user password and gained access to the user's device, perhaps it is a snatched device, perhaps it is an un-attended session... **Current statistics show that >70% of people who lose a device do not report it in the following 24hrs, and >70% of reported lost devices cannot be remote reached/wiped due to connectivity or battery problems.** - How is this architecture going to assure that passwords are secures when legitimate users have to type them 20-50 times a day on a flat surface? - How is this architecture going to protect against sophisticated attacks (Heartbleed) and others if it removed 2FA?	The updated figure below shows how Derived PIV Credentials are used on mobile device acting as a second factor to the data terminal without breaking the 2FA rules:	It is unclear in what way Figure 1-1 is considered to be similar to MDM architecture. Figure 1-1 depicts a mobile device being used to obtain remote logical access to an information system using a Derived PIV Credential. The figure does not indicate whether the private key corresponding to the Derived PIV Credential is stored in a removable hardware cryptographic module (e.g., UICC, USB token, or microSD) or an embedded cryptographic module). The figure does not get rid of an authentication factor compared to the PIV Card. The PIV Card, when using the PIV Authentication key, provides two-factor authentication. All of the options for Derived PIV Credentials specified in Draft SP 800-157 also provide two-factor authentication. When an embedded software cryptographic module is used, for example, this is a “multi-factor (MF) software cryptographic token,” as specified in SP 800-63-2.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
58	Secure Access Technologies	Ben Ayed		12	459	3.3	This section did not cover: a) 2FA Software Tokens SecureAccessTechnologies.com and DueSecurity.com provide 2FA Soft Tokens (internet) that are secure and cost much less than MDM. SecureAccessTechnologies.com also provides 2FA Bluetooth LE Soft Tokens with PKI, RSA SecurID, proximity function and voice authentication, and costs less than MDM in terms of license and operational costs. b) Proximity Tokens [non-attached, always on] Bluetooth LE provides an always-on non-attached hardware cryptographic token that can act as secure element, and can supply certs over encrypted wireless communication SecureAccessTechnologies.com provides proximity tokens that are metallic and water proof, and that act as SecureElement for any mobile device. These tokens are FIPS140-2 level3 standard.	3.3.3 2FA Soft Tokens 2FA Soft Tokens (non Bluetooth) can act as secure element, and communicate over encrypted wireless communication. These solutions are low-cost. low-risk and are commercially available. They provide improved user experience. 3.3.3 Proximity Tokens (Non-Attached Always-On) Bluetooth LE Soft Tokens and Hard Tokens provide always-on non-attached hardware cryptographic token that can act as secure element, and communicate over encrypted wireless communication. These tokens also provide a critical function for mobile security that is Proximity Monitoring/Continuous Authentication. These solutions are low-cost. low-risk and are commercially available. They provide improved user experience.	Resolved by resolution of comment #56.
59	Secure Access Technologies	Ben Ayed					Notes 1: Comparison of MDM and 2FA Soft Tokens - 2FA is a security technology... there are many competing technologies... it is open for innovation. MDM is ONE device management technology owned by Apple and Google, with a weak security value. MDM does not add any factor of authentication, and its security features are CONTROVERSIAL. In fact, MDM forces people to type passwords 20-50 times a day, thus making passwords unsecure. MDM remote-wipe does not work most of the time, as 70% of loss is not reported within 24 hrs, and 70% of reported devices cannot be remote wiped. Deployment/scalability: 2FA Soft Tokens are not invasive, deploy and scale very quickly. It is a one-to-one correspondence to PIV. MDM is invasive, and requires rearchiterure and a lot more integration...>> Lots of costs User Experience: 2FA Soft Tokens (internet) facilitate the user experience, simplify logging, protect against Heartbleed attacks... Security: 2FA Soft Tokens (with Wireless Bluetooth LE) provide further security and user experience and work with ANY mobile device today. Most major mobile device brands support	It is strongly encouraged to use derived PIV credentials on mobile devices while maintaining 2FA. Severak commercially available technologies such as 2FA Soft Tokens leveraging internet communication (Secure Access Technologies, SecureAuth, Duo Security), Bluetooth LE 2FA Soft Tokens (Secure Access Technologies), and Voice Authentication Challenge on a mobile device (Secure Access Technologies) do not require Any additional hardware, and have lower cost than most MDM vendors charges, and provide a lot more value such as MFA, biometric auth, continuous authentication, auto-wipe, device loss prevention... and are a lot more reliable than MDM as they run off-line.	NIST (157) The scope of SP 800-157 is limited to enabling authentication to remote information systems. Authentication to the local device is out-of-scope. SP 800-157 also does not address mobile device management issues, such as managing configuration settings on devices, ensuring that unapproved applications can not be loaded, and ensuring that agency data is removed from the device (especially in the BYOD case) when the person who has the device leaves the agency and should no longer have access to the information.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
60	Gemalto	Y.PIN	Tech	21	728	B.1.4.4	some issues exists regarding base band communication. The base band are different from one mobile to another and most of them could interpret the Status word. The SW 9000 is transparent and not modified by the B.B. The SW 61 xx (in T=0 protocol) is intercepted by the B.B. and the B.B send automatically a get response apdu command to get the datas. When reading huge amount of data such as a certificate (more than 1Kb) the allocated memory used to store the ICC response is not big enough and that leads to a mobile phone crash. for other error status, sometimes, the B.B could intercept them and change them into an exception so that it will not be possible to received the error code at Software level. (see Gemalto's contribution for GICS B10.12)	encapsulate the real SW into the data field and send 9000 SW. Introduce another command different than the ISO Get response command to retreive the data from the card to avoid any B.B. interpretation.	Noted.
61	Gemalto	J. McLaughlin	Policy	7	286-287	1.2	Scoping Derived PIV Credential to only the authentication certificate does not support the major use-cases required for mobile device support--that of decrypting e-mail and sending signed e-mail using the moblie device. While Appendix A recognizes digital signature and key management keys for mobile devices, these are not considered Derived PIV Credentials and therefore are second class citizens at best that does not support the major use-cases required.	Include PIV digital signatuare and key management keys in the definition of Derived PIV Credential.	Resolved by comment #6.
62	Gemalto	J. McLaughlin	Technical/Policy	20	700-701	B.1.2.1	PIV Derived Application may support contactless interface. It's within reason for a mobile device to perform as operations of the NFC (14443) interface of the mobile device. For example, using any of the Derived PIV Credentials, signature and key management keys with another devices such as a PC using the NFC reader; physical access to door readers.	Include use of contactless interface within scope as at least optional.	NIST (157) Resolved by comment #15.
63	Gemalto	J. McLaughlin	Technical/Policy	All	All	All	CHUID is not supported as a derived credential, therefore preventing the mobile device to be an alternative for physical access.	Include CHUID within scope.	NIST (157) Resolved by comment #15.
64	Gemalto	J. McLaughlin	Technical/Policy	15	560-562	3.4.1	Restricting the PIN length to six *bytes* is less than the PIV standard when hardware is quite capable to support the regural PIV standard	Modify to support the normal PIV standard.	Noted. Section 3.4.1 of Draft SP 800-157 says that “The required PIN length shall be a minimum of six bytes.” It does not restrict the PIN length to six bytes. Note: The final SP 800-157 allows for password instead of PIN only.
65	Treasury	Treasury	E	iv	199	Executive Summary	Footnote is unnecessary given that the mobile device definition is also provided in Appendix D (p.23).	Remove footnote 1.	Declined. As the definition of mobile device is critical to the scope of SP 800-157, it is useful to provide the definition up-front in addition to including it in Appendix E.
66	Treasury	Treasury	T	iv	200	Executive Summary	Document suggests that laptops are excluded from the definition of a mobile device; yet laptops may meet the mobile device definition stated in footnote 1 and Appendix D.	Revise definition as follows: "*Examples include smart phones, tablets, and e-readers but specifically exclude laptop computers where integrated smart card readers are more common."*	Resolved by comment #41.
67	Treasury	Treasury	E	iv	210	Executive Summary	Parenthetical reference to smart phones and tablets may not be necessary given that mobile devices have been previously defined.	Remove *"(such as smart phones and tablets)* ".	Noted. The additional detail helps some readers as they navigate the document; especially when making the point that the PIV Card is difficult to use with mobile devices.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
68	Treasury	Treasury	T	6	268	1.2	Citing specific use cases where technologies such as NFC are impractical would be helpful to illustrate where Derived Credentials may be necessary.	Add example use cases following "*is deemed impractical* " to illustrate scenarios where such technologies don't suit the business needs being satisfied here.	Resolved by comment #41.
69	Treasury	Treasury	T	6	268	1.2	"Impracticable" means "impossible to do". "...the use of PIV Cards with mobile devices, using either contact card readers or NFC" should not be deemed impossible, but rather, it may be deemed not practical	Change "impracticable" to "impractical or inconvenient"	Resolved by changing "impracticable" to "impractical"
70	Treasury	Treasury	T	6	280	1.2	LOA3 credentials derived from the LOA4 PIV authentication credential may weaken identity assurance, especially in cases where a relying party lacks the capability to distinguish the differing levels of trust between a PIV and PIV Derived credential through OID evaluation etc.	Consider removing LOA3 Derived Credential options or at least warn the reader of the basic risks inherent in their reliance and use.	Noted. The Certificate Policy OID of the PIV Card's Authentication credential is different than the OIDs for the Derived PIV Credentials. The Derived PIV Credential OIDs are further differentiated in that LoA-4 Derived PIV Credential has a different OID than the LoA-3 Derived PIV Credential.
71	Treasury	Treasury	T	6	282	1.2	"Figure 1-1 Use of Derived PIV Credential" does not provide the reader with any benefits. There needs to be a better representative diagram.	Recommend either removing this figure or providing suggested diagram that shows PIV linkage and use. There are many examples out there. Get rid of, or augment max.gov example with generic web applications, etc.	Declined. The figure is appropriate for the scope and purpose section. The figure also makes clear that the scope of the document is remote access control rather than physical access control.
72	Treasury	Treasury	E	7	283	1.2	Should use "[SP800-63]" document reference since the original (pre-HSPD-12) version of SP 800-63 did not include "derived credentials". SP 800-63-1 was the first version to reference derived credentials.	Change "SP 800-63" to "[SP800-63]"	Accept
73	Treasury	Treasury	G	7	286-292	1.2	The issuance of the Derived PIV Credential is a major component of the process described in this section and needs to be outlined and detailed more than the general concepts outlined in Draft NISTIR 7981 which accompanied this review.	Recommend providing greater detail around the issuance process of the Derived PIV Credential.	Noted. The Derivation process and issuance of the Derived PIV Credential is described in greater detail in Section 2.2. Different issuance processes have also been illustrated in Appendix C.
74	Treasury	Treasury	T	7	291	1.2	Suggest being more specific regarding the scope of this document.	Change "Only derived credentials..." to "Only PIV Card based derived credentials .."	Resolved by changing: "Only derived credentials issued in accordance with this document are considered to be Derived PIV credentials" with: "Only derived credentials issued based on the PIV card and in accordance with this document are considered to be Derived PIV Credentials."
75	Treasury	Treasury	T	7	302	1.3	Other audience stakeholders are more important than "software developers"; Issuers, Agency CIO's, managers, hardware developers, system integrators, etc. are all equally, if not more, important than "software developers"	Suggest rewording to "This document is targeted at stakeholders who will be responsible for procuring…"	Accept.
76	Treasury	Treasury	T	8	323	1.5	Suggest itemizing/separately bulleting terms used throughout the document. Most importantly, the term "Subscriber" should be used more often throughout the document and should be included in the suggested diagrams, above and below.	1. "PIV Cardholder": a person who possesses a valid PIV Card, regardless of whether they have been 325 issued a Derived PIV Credential. 2. "Applicant": a PIV Cardholder who is pending issuance of a Derived PIV Credential 3. "Subscriber": a PIV Cardholder who has been issued a Derived PIV Credential. 4. (include other terms used in the doc; .e.g., "Issuers", "Derived PIV Credential", "Revocation", "Termination", "Lifecycle", etc.) Also, include the assumption that the reader is familiar with "PIV Cards, "PKI", "Smartcards", etc.	Resolved by defining the "Derived PIV Credential" specific terms such as Subscriber and Applicant in Appendix E.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
77	Treasury	Treasury	E	8	326	1.5	Use of the terms "Applicant" and "Subscriber" to define PIV Derived roles may confuse the reader, who is likely to be more used to hearing them in the context of the PIV card itself.	Refer to these roles as "PIV Derived Applicant" and "PIV Derived Subscriber"	Resolved by comment #76.
78	Treasury	Treasury	T	9	332	2	Since a diagram was presented above for Derived PIV Credential Usage, it would be helpful and appropriate to include in this section a diagram that illustrates the Derived PIV Credential lifecycle. Showing the subscription/issuance, maintenance & termination processes	Recommend adding a Derived PIV Credential lifecycle diagram in this section.	Resolved by adding a modified version Section 3.2 of FIPS 201-2 including life cycle diagram (Figure 3-2) that is tailored to Derived PIV Credential lifecycle.
79	Treasury	Treasury	T	9	333-336	2	There are several incomplete thoughts here and erroneous connections. Are "Issuers" responsible for the process? Shouldn't the process be defined in this document or in the forthcoming revision to SP800-79? HSPD-12 doesn't mention Derived Credentials, so no accordance to HSPD-12 should be made here.	Recommend deleting or rephrasing according to the expressed rationale.	Declined. HSPD-12 mandates the establishment of a Government-wide standard for secure and reliable forms of identification. FIPS 201-2, which is the current version of the Standard that was developed as required by HSPD-12, specifies that derived PIV credentials may be issued in accordance with SP 800-157. So, Derived PIV Credentials issued in accordance with SP 800-157 are part of the "secure and reliable forms of identification" for this purposes of HSPD-12 and so need to satisfy the requirements of HSPD-12. The assessment process for Derived PIV Credentials is defined in the current draft release of SP 800-79.
80	Treasury	Treasury	T	9	334	2	"Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2)." just like how SP 800-79 references it "In light of the requirements for both improved security and protection of personal privacy, HSPD-12 established four control objectives, one of which includes the call for a form of identification that is "issued by providers whose reliability has been established by an official accreditation process.""	Provide footnote that references the related HSPD-12 clause.	Resolved by providing a reference to [HSPD-12] in Appendix G.
81	Treasury	Treasury	T	9	335	2	Should include a section on Derived PIV Credential Issuance Process Assessment that expands on this, to include, perhaps, a reference to the forth coming revision to 800-79-1 to include derived credentials; "Guidelines for Accreditation of Personal Identity Verification Card and Derived Credential Issuers".	Recommend adding a section on Derived PIV Credential Issuance Process Assessment.	Declined. The Accreditation of the Derived PIV Credential belongs to SP 800-79.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
82	Treasury	Treasury	T	9	337	2.1	The reader would benefit from an Issuance diagram showing the process(es) where an "Applicant" becomes a "Subscriber".	Recommend adding an Issuance diagram depicting this process.	Decline. There are only a very few steps required for an Applicant to become a Subscriber. Definitions for these terms will be added to the glossary in Appendix E.
83	Treasury	Treasury	T	9	337	2.1	Issuance section misses an opportunity to provide an example implementation, which would otherwise help to illustrate the concepts introduced here, in a similar manner to section 6 of FIPS-201. For instance, exemplifying “two or more electronic transactions” to authenticate a Derived Credential Applicant at LOA-3.	Consider including an example implementation either in this section or an appendix.	Resolved by adding an appendix that contains example issuance processes at LOA3 and LOA4.
84	Treasury	Treasury	T	9	341	2.1	The term "existing PIV card" is not descriptive enough.	Consider replacing "existing" with "valid".	Declined. If the Applicant's existing PIV Card (i.e., the current PIV Card that is in existence at the time) has been revoked then the PIV Authentication certificate on the card will have been revoked and then will be detected when the PKI-AUTH authentication mechanism is performed. Use of the term “valid” would be confusing as it could imply that an Applicant could legitimately possess multiple PIV Cards, some of which are not valid.
85	Treasury	Treasury	E	9	344	2.1	FIPS 201 reference should be displayed as "[FIPS201]" with no spaces to conform to document reference.	Change "[FIPS 201]" to "[FIPS201]".	Accept
86	Treasury	Treasury	T	9	345	2.1	The rechecking requirement to fall within seven calendar days does not seem restrictive enough as too much time may pass before an invalid credential may be discovered.	Suggest tightening to 18 hours, as consistent with other requirements stated in the Common Policy surrounding the publication frequency of validation objects.	Resolved by comment #150. Note that waiting 18 hours would only account for the delay due to revocation issuance frequency and could miss the revocation of a certificate if the certificate were not revoked before the time that the Derived PIV Credential was issued. Footnote 9 in Section 2.4 already recommends investigating the issuance of any Derived PIV Credentials in the case that a PIV Card is reported as lost or stolen.
87	Treasury	Treasury	T	9	350	2.1	The credential will always be issued over an electronic session.	Change sentence to start with "If the credential is issued remotely, …"	Accept
88	Treasury	Treasury	T	9	351	2.1	Delete "if necessary". Encryption is always necessary.	Delete ", if necessary,".	Declined. If the communication consists solely of a certificate request message being sent to the certification authority and the certificate being returned, then it may be the case that neither the request nor the response includes any information that requires protection from disclosure.
89	Treasury	Treasury	T	9	351	2.1	Requirement leaves too much room for interpretation as to how to protect the session.	Suggest removing TLS as an example and replacing with a statement indicating the minimum protocols, algorithms and key sizes used to protect the session.	Declined. It is not necessary for SP 800-157 to include such requirements as they are already addressed in other NIST Special Publications (e.g., SP 800-52 and SP 800-57).
90	Treasury	Treasury	T	9	355	2.1	In-person issuance requirement seems too stringent given that it should be possible for proof-of-possession of the PIV Derived Applicant's private PIV auth key, which is itself trusted under LOA-4.	Consider stating that in lieu of the in-person requirement, LOA-4 PIV Derived Credentials, "*may be issued as a result of successful proof-of-possession of the PIV Derived Applicant's private PIV Authentication key.* "	Resolved by resolution to comment #27.
91	Treasury	Treasury	G	#####	365 / 403	2.2, 2.4	Language should be added to address real-time certificate validation for PIV derived credentials (mechanisms similar to CRL checking and OCSP responders).	Credential Usage should be added as part of the PIV Derived lifecycle and certificate validation should be expanded on. This is a challenging area due to mobile bandwidth constraints.	Declined. Certificate validation is performed by the relying party, not the mobile device, so mobile bandwidth constraints are not relevant to validation of the Derived PIV Credential.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
92	Treasury	Treasury	T	9	367	2.2	Provide additional clarity to "these include rekey, modification, and revocation."	Recommend changing statement to "the maintenance activities include rekey, modification, and revocation."	Resolved by replacing "these" with "these maintenance activities include"
93	Treasury	Treasury	T	9	367	2.2	Provide better clarity to the word "operations" in this context.	Recommend changing the word "operations" to "activities".	Accept
94	Treasury	Treasury	T	10	376	2.2	Provide reference to "The initial issuance process shall be followed for:"	Change to ""The Initial Issuance process (Section 2.1, above) shall be followed for:""	Accept
95	Treasury	Treasury	T	10	380	2.2	The "underlying certificate policy" does not seem specific enough given the assumption that any policies binding upon the PIV Derived Credential will emanate from the Common Policy.	Include "Common Policy" reference here.	Declined. The text correctly states that the certificate shall be revoked in accordance with the policy under which it was issued. The "Common Policy" defines 8 different certificate policies, and this number will increase to 10 once the two new policies for issuing Derived PIV Authentication certificates have been added. As the "Common Policy" may specify different requirements for each of the 10 different certificate policies, referring to the "Common Policy" rather than the "underlying certificate policy" could be ambiguous.
96	Treasury	Treasury	E	10	382	2.2	Use of the PIV Derived credential to support loss, theft or damage of the PIV card is a separate thought that should be in its own subsection.	Consider moving this paragraph to its own section 2.2.1 under Maintenance, entitled "*PIV Derived Credential as Alternate Token*".	Declined. The referenced sentence explains the rationale for the previous sentence.
97	Treasury	Treasury	T	10	382	2.2	The need for the Derived Credential to be unaffected by compromise of the PIV credential (and hence, is not truly "derived") represents a security risk, as acknowledged in the footnote. There may be practical reasons for this, such as it serving as a suitable "temp token", but it probably does not weigh favorably. Furthermore, according to NISTIR 7817 of Nov. 2012, section 3.7, "Termination of the primary credential,...should lead to the derived credential's termination." This statement seems to preclude use of the Derived credential as a replacement token for lost/stolen/damaged credentials."	In deference to the security risk acknowledged in footnote 5 and suggested in NISTIR 7817, consider stating that the Derived Credential IS affected by compromise of the PIV card in a cryptographically strong and linked manner.	Resolved by adding a footnote as follows: Departments and agencies may adopt a more stringent approach and terminate any Derived PIV Credential when the associated PIV Card is being replaced. Note 1: NIST has coordinated the initial draft of SP 800-157 with the FICAM LAWG team, that has requested that "Agency wants to leverage a PIV-derived credential as a back-up … in the case where … PIV Card was lost/stolen or PIV Card malfunctions." Note 2: SP 800-63-2 defines a derived credential as "A credential issued based on proof of possession and control of a token associated with a previously issued credential, so as not to duplicate the identity proofing process." So, there is no need for the Derived PIV Credential to be affected by the later compromise of the PIV credential in order to be "truly" derived. Both Section 5.3.5 of SP 800-63-2 and Section 3.7 of NISTIR 7817 note that a derived credential may be tightly coupled with the revocation status of the primary credential, but neither require or recommend this as a general rule. "Termination" is not the same as "revocation," so the quoted text in Section 3.7 of NISTIR 7817 does not apply. Section 2.3 of Draft SP 800-157 addresses termination, and does require the
98	Treasury	Treasury	T	10	392	2.3	Provide clarity on footnote 6 to specify the section in FIPS201 that lists reasons for termination.	Add section (i.e., Section 2.9.4 of [FIPS201]) to the FIPS201 reference for footnote 6.	Resolved by changing footnote 6 to "Section 2.9.4 of [FIPS201] provides a list of circumstances that require PIV Card termination."

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
99	Treasury	Treasury	T	10	400	2.3	Document does not address the difficulties associated with collecting and destroying an embedded, hardware-based token under explicit control and ownership of the PIV Derived Subscriber.	Document should indicate that collection and destruction of the token may not be possible in all cases, and suggest practices to be followed in cases involving embedded, hardware-based tokens under the explicit control and ownership of the PIV Derived Subscriber.	Declined. The document provides two possible methods for terminating the Derived PIV Credential. It is not necessary to explain that there may be circumstances in which it will not be possible to use one of the two methods. It is also reasonable to assume that readers will already be aware that it will not always to possible to collect a token from someone who no longer works at an agency (whether that person left voluntarily or involuntarily).
100	Treasury	Treasury	T	10	401	2.3	There needs to be additional clarity around the statement "In all other cases".	Recommend adding what those other cases could be. A PIV Derived Authentication private key that was created and stored on a hardware OR SOFTWARE cryptographic token that DOES permit the user to export the private key?	Declined. The sentence unambiguously states that if the conditions specified at the start of the first sentence of the paragraph are not satisfied then revocation is necessary.
101	Treasury	Treasury	T	11	403	2.4	Section should require the linkage to be cryptographically strong.	Suggest stating that the mechanism employed maintains a "*cryptographically strong link, in a manner equivalent to the chain of trust established between the Derived PIV Credential and its issuer."*	Declined. The term "cryptographically strong link" is not well defined.
102	Treasury	Treasury	T	11	413	2.4	This may be a misinterpretation of [FIPS201] Section 2.9.2 and 2.9.4.	1. Section 3.2 says "PIV Card Termination. The termination process is used to permanently destroy or invalidate the PIV Card and the data and keys needed for authentication so as to prevent any future use of the card for authentication." 2. [COMMON] 4.9.3 allows for not revoking certificates when a PIV card is terminated, but does recommend that the certificates be revoked. 3. FYI: USAccess revokes PIV certificates when a card is terminated, whether or not it was destroyed. 4. Always revoking PIV Card certificates when a card is terminated/revoked will keep someone from fraudulently using a stolen PIV Card from being able to use it to obtain a fraudulent Derived PIV Credential, as referenced in footnote 5 on page 10.	Noted. While USAccess may always revoke, it is not a requirement in FIPS 201-2 or [COMMON], so issuers of Derived PIV Credentials cannot assume that all issuers of PIV Authentication certificates will do this. If a PIV Card is collected and destroyed then it cannot be used to obtain a fraudulent Derived PIV Credential, even if the remnants of the destroyed card are later stolen. If the "destroyed" PIV Card could be used to perform a challenge-response with the PIV Authentication private key then the card was not actually destroyed. See also comment #308.
103	Treasury	Treasury	T	11	417	2.4	Statement refers to the issuer as an "agency" but this may not always be the case.	Replace "*agency*" with "*issuer*".	Resolved by changing "agency" to "agency or issuer."
104	Treasury	Treasury	T	11	422	2.4	Termination status may also be (perhaps optimally) triggered rather than queried.	State that the BAE process, "*may trigger the delivery of, or be queried for, the termination status of the PIV card…*"	Decline. GSA has confirmed that the BAE is a query only system. It does not support push notification.
105	Treasury	Treasury	T	11	426	2.4	Realizing this is a high-level example, document misses an opportunity to describe that the notification must be performed in a manner that guarantees delivery/subsequent action and ensures integrity of the termination message., optimally through digital signature verification.	Indicate, "*Such notification should guarantee delivery/subsequent action and ensure integrity of the termination message.*"	Resolved by adding text to the bullet on line 425 (line 562 in the final document) that states "Such notification should provide evidence of receipt and the integrity of the termination message."

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
106	Treasury	Treasury	T	11	430	2.4	The linkage could be updated in other scenarios as well.	Consider instead describing that the linkage is updated "*whenever the private PIV authentication signing key changes.*"	Resolved by revision to Section 2.4.
107	Treasury	Treasury	T	12	445	3.1	Not keeping the expiration dates in sync between PIV and PIV Derived credentials will likely introduce many new lifecycle management challenges. Managing the PIV card lifecycle has been challenging enough, as it has been widely observed; this layers an additional set of challenges beyond that, and the benefits gained are questionable when weighed against them.	Recommend that expiration dates between PIV and PIV Derived credentials should be kept in sync.	Resolved by rewording the text in Section 3.1 to state that alignment is not required but it may simplify lifecycle management. This is a department or agency-level policy decision. SP 800-157 does not require that the expiration PIV credentials and Derived PIV Credentials are the same. If an issuer feels that aligning the expiration dates of both credentials eases lifecycle management the issuer is free to do so.
108	Treasury	Treasury	T	12	453	3.2	Should just be "Level 3".	Delete "Level 2 or higher that provides"	Declined. The requirement for [FIPS140] Level 2 or higher that provides Level 3 physical security" is the same as the requirement for PIV Cards. In addition, cryptographic modules that implement the PIV Derived Application cannot be validated as FIPS 140-2 overall Level 3, since they export keying material in plain text form.
109	Treasury	Treasury	T	12	463	3.3	Considering the high frequency in which people and organizations change devices, embedded tokens may be too difficult to manage over time and may present additional security risks: residual key material is more likely to exist on abandoned devices outside the possession and control of the intended user. Also, it is easier to destroy a removable token rather than e.g. a phone that was personally procured.	Consider restricting cryptographic token types to removable tokens.	Noted. Departments and Agencies have a suite of choice for Derived Credential tokens. They can also revoke the associated certificate in all instances.
110	Treasury	Treasury	T	12	465	3.3	While USB based removable modules may be seen as analogous to PIV Card interchangeability, neither the SD card nor the UICC universally fits this analogy due to the numerous cases in which both technologies are integrated circuits. Furthermore, it is often difficult to remove SD cards without turning off the mobile device first.	End statement with something like, "*…to attempt token portability between mobile devices in a manner that strives toward PIV Card interchangeability to the maximum extent possible.*"	Declined. An SD card or UICC that is integrated into the mobile device would not be a removable cryptographic token. The referenced text only refers to removable hardware tokens. The fact that it may not be convenient to remove and re-insert the token on a regular basis is not relevant to the issue of interchangeability.
111	Treasury	Treasury	T	13	471	3.3	This document does not acknowledge or describe the considerable risks inherent in the use and reliance upon software tokens issued to devices that are commonly "always on".	Recommend removing the software token option, or at least, acknowledge and describe the inherent risks.	Resolved by adding text about some risk and describing the hybrid approach in section 3.3.
112	Treasury	Treasury	T	13	479	3.3.1	Unnecessary to limit the requirement for the PIV Derived Application to be implemented in its own security domain only in cases, "When the removable hardware cryptographic module supports multiple security domains…"	Consider removing everything preceding the statement "…the PIV Derived Application shall be implemented…"	Resolved my removing the sentence starting on line 479.
113	Treasury	Treasury	T	13	483	3.3.1	Section may become quickly outdated given that the discrete list of token technologies that follow is subject to rapid and frequent change.	Consider a more generic approach that allows for any technology provided that it adheres to a baseline set of technical requirements with reference examples; this would allow for emerging token models to meet the spec more easily and rapidly as they are brought to market. Alternatively, consider moving specific examples to an appendix that may be more easily and rapidly updated.	Declined. A more generic approach would not allow for the document to impose the technical requirements necessary for interoperability. Placing the list of acceptable types of removable hardware cryptographic tokens in an appendix would not allow for the list to be updated any more easily or rapidly than can be done with the list appearing in the body of the text.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
114	Treasury	Treasury	T	13	492	3.3.1	Provide better clarity to "the Derived PIV Credential."	Recommend changing to "the Derived PIV Authentication key".	Resolved by changing "the derived PIV credential" to "Derived PIV Authentication private key and its corresponding certificate" on line 492 (line 656 in the final document).
115	Treasury	Treasury	E	13	495	3.3.1.1	Reduce use of the term "size" and clarify that the reference is to physical rather than logical size (storage space).	Replace phrase with, "*The SD format is available in original, "mini", and "micro" physical sizes* ."	Resolved by replacing the sentence with "The SD format is available in three different physical sizes – "original," "mini," and "micro."
116	Treasury	Treasury	T	14	510-511	3.3.1.1	Provide clarify to "The secure data transfer commands are not relevant for PIV Derived Application use."	Should provide more information on what secure data transfer commands are being referenced here.	Resolved by comment #11.
117	Treasury	Treasury	T	14	516	3.3.1.2	Notwithstanding the reference to GlobalPlatform card specifications, this section lacks an indication of the input/output transport mechanism supported by APDUs.	Consider a high-level reference to APDUs in this section.	Resolved by adding to the 2nd to last paragraph: The APDUs as specified in Appendix B shall be used with this secure element containing the PIV Derived Application.
118	Treasury	Treasury	T	14	517	3.3.1.2	References to more specific GlobalPlatform guidelines would help here.	In addition to the existing reference to the general 2.2.1 card spec, statement should also include reference to GlobalPlatform UICC configuration guidelines, such as 1.0.1 published here: http://www.globalplatform.org/specificationscard.asp	Declined. The Global Platform UICC configuration addresses management issues that are outside the scope of this specification.
119	Treasury	Treasury	E	14	524	3.3.1.2	Second instance of the statement "The PIV Derived Application shall be implemented…" as it appears in the more general section 3.3.1 (line 480).	Remove second instance of this statement.	NIST (157) Resolved by comment #112.
120	Treasury	Treasury	T	14	530	3.3.1.3	Should include consideration for the fact that a derived token (e.g., smartphone) may not be able to be power charged when the USB token is connected.	Does the USB token have to be connected throughout a session when accessing a web application? Or, can it be removed once the derived credential is authenticated to the web application?	Noted. Out-of-scope for this document. This behavior is application specific.
121	Treasury	Treasury	T	15	558	3.4.1	Statement makes it appear as if knowledge-based activation of the private key should only be implemented in cases involving hardware crypto modules.	Consider generalizing the requirement by moving it to a section describing private key activation more broadly, to encompass any point at which the private key is invoked from the Derived credential using PIN or password.	Resolved by combining Hardware and Software activation sections.
122	Treasury	Treasury	T	15	560	3.4.1	PIN requirements stated in this section, such as those surrounding PIN construction stated here, run the risk of falling out of sync with requirements binding upon the PIV credential itself, especially giving the rapidly evolving nature of documents such as 800-73.	Consider indicating that PIN requirements follow those stated in the latest publication of 800-73.	Declined. The PIN requirements stated in Section 3.4.1 come from FIPS 201-2, not SP 800-73. FIPS 201 is not a rapidly evolving document.
123	Treasury	Treasury	T	15	562	3.4.1	Was the intention to use six "bytes" or six "digits/characters" here?	Recommend updating to "digits" or "characters".	Resolved by changing “bytes” to “characters.”
124	Treasury	Treasury	G	15	562	3.4.1	Do we feel comfortable relying essentially on the PIN as the one thing that the employee has that someone who finds/steals a mobile device doesn't have? Hopefully true biometric support will become more common on mobile devices and better processes are in place for notifications/report during loss/theft of devices.	It is recommended that the longest practical PINs we can get away with will be used.	Declined. Given that the removable hardware cryptographic module includes a mechanism to limit the number of consecutive unsuccessful authentication attempts, a minimum PIN length of 6 should be sufficient.
125	Treasury	Treasury	E	15	563	3.4.1	For consistency all occurrences of "LoA" in the doc should be changed to "LOA", per the acronyms in Appendix E.	Change "LoA" to "LOA".	Accepted.
126	Treasury	Treasury	T	16	584	3.4.1	Requirement leaves too much room for interpretation as to how to protect the session.	Suggest removing TLS as an example and replacing with a statement indicating the minimum protocols, algorithms and key sizes used to protect the session.	Resolved by comment #89.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
127	Treasury	Treasury	T	16	590	3.4.2	The requirement to follow the initial issuance process when the password is forgotten will likely place significant burden on the Derived credential holder and support operations alike.	If possible, consider password reset requirements that do not require the credential holder to go through initial issuance with each forgotten password. Such requirements may involve, for example, proof-of-possession of the private PIV auth key.	Resolved by adding language stating that: Implementation of password reset is permitted for software-based LOA-3 Derived PIV Credentials and the hardware-based password reset mechanisms apply.
128	Treasury	Treasury	T	16	592	3.4.2	The absence of a lockout mechanism for unsuccessful activation attempts misses an opportunity to mitigate the tremendous risk inherent in the existence of an easily-duplicated private key connected to an "always-on" device in a software module.	If possible, require a lockout mechanism as consistent with mechanisms tied to hardware modules. If not possible, recognize the risk here and suggest other ways in which this may be mitigated.	Resolved by comment #4.
129	Treasury	Treasury	T	17	595	Appendix A	The inclusion of key management keys as optional Derived keys risks significantly complicating the usage and management process beyond the PIV scenario as most (all?) current decrypting applications / APIs lack the capability to find the right key across multiple tokens. This especially holds true as keys are renewed and updated over time; and as there is no stated limit to the number of Derived keys and tokens that may be issued.	Consider acknowledging some of the complications inherent in the practice of issuing key management keys to multiple devices, to further assist agencies considering such an option.	Declined. Applications will not need to look across multiple tokens to find the appropriate key management key.
130	Treasury	Treasury	E	17	616	Appendix A	"certificate for a" is repeated within the same sentence.	Remove duplicate phrase.	Accept
131	Treasury	Treasury	E	18	639	Appendix B	All read access control rule requirements stated here cite specific sections of 800-73Part1, which are subject to shift as the document is updated.	Consider a general statement that, "*The read access control rule for X.509 PIV Derived Certificates and the PKI cryptographic function access rule for the corresponding private key are described in [SP 800-73Part1]* ."	Declined. The section numbering in SP 800-73 is relatively stable, and including specific section numbers improves the readability of the document.
132	Treasury	Treasury	T	19	661	Appendix B	Given the lack of a requirement for which sets of keys are stored in history, the derived credential may or may not have the PIV decryption keys, or derived keys issued to other devices.	Consider recommending (here or in a non-normative section of the document) that, "*The key history container should be comprised of all historical keys from PIV and derived tokens to the extent possible.* "	Resolved by comment #7.
133	Treasury	Treasury	E	20	696	Appendix B	Table seems unnecessary as it maps each Derived Application data object to a PIV data object of the same name in almost all cases.	Consider replacing the table with a statement indicating that "*Excepting the X.509 Certificate for PIV Derived Authentication, which maps to the X.509 Certificate for PIV Authentication, PIV Derived Application Data Objects map to the corresponding named PIV Card Application Objects within [SP800-73Part1].* "	Noted.
134	Treasury	Treasury	E	21	716	Appendix B	"PIV Unblocking Key" is assumed to be a typo.	Replace with *"PIN Unblocking Key"*	Accept
135	Treasury	Treasury	T	21	724	Appendix B	Statement that crypto algorithm requirements should adhere to [800-78] may be too broad given that many mobile devices lack the computational power to perform certain crypto operations at higher key lengths. This may be the case in the foreseeable future as well.	Consider limiting crypto requirements to algorithms such as ECC which are better suited for limited-capability devices; at least in some cases demanding heavy computation such as signing operations.	Noted. A PIV Derived Application is not required to implement all of the algorithms in SP 800-78, it only needs to implement at least one of them. So, a PIV Derived Application may be designed to only support ECC even though SP 800-78 also permits the use of RSA. Also, it is unlikely that mobile devices or the removable cryptographic modules that may be used with mobile devices would have less computational power than the cryptographic modules on PIV Cards.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
136	Treasury	Treasury	T	23	772	Appendix B	Document misses an opportunity to describe how Derived Credentials may play a role in addressing recent concerns regarding smartcard removal policies. For example, the types of Derived Credentials best suited to align with an agency's requirement for the smartcard to be removed following authentication are not expressed in this section.	Consider acknowledging such concerns and adding a reference to the types of Derived Credentials that may help to address them.	Declined. It would not be appropriate for SP 800-157 to address agency-specific policies such as this one.
137	Treasury	Treasury	T	23	776	Appendix C	Section does not mention that NIST SP800-53 also includes the "Control Access Provision" requirement; for example IA-2 requires this for privileged and non-privileged accounts.	Consider adding a reference to NIST SP800-53 to broaden the implication behind the "Control Access Provision" requirement.	Noted. This particular control enhancement is based on the OMB memorandum referenced Appendix C (now Appendix D).
138	Treasury	Treasury	G	24	793	Appendix D	Definition should be "PIV Derived Credential" rather than "Derived PIV Credential" (this holds true for other references within the document).	Reverse word ordering to indicate "PIV Derived Credential", and change other references accordingly throughout the document.	Declined. The term “derived PIV credential” is used in FIPS 201-2 and so it cannot be changed in this document.
139	Treasury	Treasury	T	24	798	Appendix D	Given the desire to exclude laptop computers as stated in line 200 of the Executive Summary, the definition provided here might not go far enough - most laptop models fit each of the four qualifications given. It is possible (i) might exclude laptops; however "easily carried" is a relative term.	Consider explicitly stating, "*This definition is not intended to include 'laptop' computers which are closer in lineage to desktop computer counterparts than other mobile devices. Such systems typically include 'fold-down' construction, full-sized keyboards, and desktop-based operating systems.* "	Resolved by comment #41.
140	Treasury	Treasury	G	24	805-806	Appendix D	Change “PIV Derived Application” to “PIV Derived Hosting Application” or “PIV Derived Client” in the following statement: “PIV Derived Application: A standardized application residing on a removable, hardware cryptographic 805 token that hosts a Derived PIV Credential and associated mandatory and optional elements.”	When we say PKI application we usually mean a PKI-enabled application (an applications that has been integrated with PKI such as Secure S/MIME email). When we say PIV application we usually mean a PIV-enabled application (this web portal is PIV-enabled). Using the term “PIV Derived Application" is misleading when talking about an application hosting the PIV Derived Credential. It could be interpreted as a mobile application that supports authentication using PIV Derived credentials. A better term would be “ PIV Derived Hosting Application” or PIV	Noted. This terminology is consistent with SP 800-73 and as the Derived PIV Credential is based on the PIV card application therefore the term Derived PIV Credential is appropriate in this context.
147	USDA Mobility PMO	Peter Cox		18	589	3.4.2	Enforcing LOA-2 password rules to software implementations will increase the risk for compromise. Given the complexity of the level 2 passwords, it is highly likely that the password will be stored somewhere on the device and copied when needed. I recommend using a PIN with the rules that apply for the PIV card.	I recommend using a PIN with the rules that apply for the PIV card.	Resolved by aligning software activation requirements with hardware activation requirements. See comment #18
148	USDA Mobility PMO	Peter Cox		18	591	3.4.2	More frequent reissuing of derived certificates will increase the burden/cost of managing certificates and maintaining the chain of trust between the PIV credential and correct derived credential. To keep the cost down yet preserve the level of security, I would require the use of the PIV card to reset or unlock the PIN. This enforces the chain of trust and requires a LOA-4 authentication to reset or unlock a LOA-3 credential.	To keep the cost down yet preserve the level of security, I would require the use of the PIV card to reset or unlock the PIN.	Resolved by comment #127.
149	USDA Mobility PMO	Peter Cox		18	593	3.4.2	I believe that allowing for not having a lockout mechanism is too great a security risk against brute force attacks. I highly recommend that the same lockout rules apply as for the PIV card.	I highly recommend that the same lockout rules apply as for the PIV card.	Resolved by comment #4

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
150	USDA	Adam Zeimet	T	9	344-346	2.1	The requirement to "recheck" a PIV-Auth certificate 7 days following the issuance of a Derived PIV credential should be removed. A lost or stolen card is still protected by a second factor which mitigates the risk that a lost or stolen card can be used to issue a derived PIV credential. FIPS 201-2 requires that lost or stolen PIV credentials be revoked within 18 hours or less, making the 7 day requirement unnecessarily long. NIST SP800-63-2 refers to credential rechecking in section 5.3.5 "Requirements for Derived Credentials", but the recheck is an option (based on the wording "should"). This recommendation should not be be carried forward as a requirement in 800-157. Additional mitigating factors can include procedures that ensure Derived PIV credentials are only issued to known\trusted devices or tokens as well as leveraging an Identity Management System (IDMS) or BAE to ensure that Dervied PIV credentials are only issued to approved individuals with active cards that have not been lost or stolen. The recheck requirement does not exist for any other PIV transaction (ie. authentication or digital signature) implying that the non-repudiation of any transaction is sufficient without needing to revalidate later. Accordingly, this requirement represents a costly technical addition with little security benefit or value.	Remove requirement	Resolved by changing "shall" on line #345 (line 391 in the final document) to "should."
151	USDA	Adam Zeimet	E	9	362-364	2.1	The text in this paragraph beginning with "Issuing several Derived PIV Credentials…." is a highly subjective comment. This implementation will depend on Agency use case requirements. Commentary may be more appropriate for NISTIR 7981 and\or this language should be in the form of instruciton\advice, not opinion.	Move opinion commentary to NISTIR 7981 and change language here to the form of 'advice'. For example, "Agencies should ensure that an appropriate management system is in place when issuing multiple PIV-D credentials due to added risk\complexity… etc"	Declined. The information is useful for departments and agencies.
152	USDA	Adam Zeimet	G	10	370	2.2	Is there a similar set of requirements for LOA3?		No.
153	USDA	Adam Zeimet	T	10	389	2.2	On the last sentence of this paragraph, wording should be more absolute regarding name changes to a ensure consistent standard is implemented across Agencies and to ensure that the ID proofing information stays consistent across both PIV and the derived credential.	Change the word "may" to "shall" (6th word from the end of the sentence\paragraph).	Declined. There is no requirement for the PIV Authentication certificate or the PIV Derived Authentication certificate to include the cardholder's name. If the PIV Derived Authentication certificate does not include the Subscriber's name then a name change would not result in a need to issue a new certificate.
154	USDA	Adam Zeimet	G	11	430-432	2.4	It it intended that the FASCN is the linkage?		This is implementation dependent.
155	USDA	Adam Zeimet	G	16	586-589	3.4.2	Requiring an alpha numeric password will be a detriment to the concept of a derived PIV credential used on mobile devices, where the typing interface is often difficult to use. This will reduce the user experience and usability of these credentials.	Allow numeric PIN's with additional management controls (lockout etc., similar to LOA4)	Resolved by comment #147.
156	USDA	Adam Zeimet	T	16	590-591	3.4.2	Password reset should be supported. Reissuing credentials may present both a high and unecessary cost to the Agency. The initial issuance process can and should still be followed to reset the password, but the password should be reset without re-issuance of a new token. Additionally, the technical impact of this on the PKI SSP will be high in both volume of certifcate issuance as well as size of Credential Revocation Lists.	Allow for resetting of a password without reissuing a credential (certificate) for LOA3. Require that the initial issuance process be followed to reset (ie. prove possession of PIV, excluding other PIV-D credentials the user may have).	Resolved by comment #127

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
157	USDA	Adam Zeimet	T	16	592-593	3.4.2	No reason not to require a lockout. Ideally a lockout would be used with a shorter password requirement (ie. numeric PIN).	Remove sentence completely or change language to require lockout.	Resolved by comment #4
158	DoS	CR Froehlich	G	iv	193-195	Executive Summary	The PIV Card is neither used government-wide nor as intended. It is not used government-wide for physical access, and potentially requires having PIV/CAC credentials from that network for logical access as well as requiring the user to have a valid account on the network for local access.	Delete the phrase ", which is currently…"	Declined.
159	DoS	CR Froehlich	G	iv	197-198	Executive Summary	PIV Card readers are neither ubiquitous nor integrated. It is still most commonly used as a flash pass for physical access; is not fully deployed within all agencies; and, it not necessarily interoperable across agencies.	Reword to read: "...where the PIV Card can provide for common authentication ... across the federal government when fully implemented."	Declined.
160	DoS	CR Froehlich	A	5	N/A	N/A	The page numbering of the basic document is in error--while it switches from roman numerals to arabic numerals, it does not revert to page 1.	Revise page numbering	Accept
161	DoS	CR Froehlich	T	5	234-235	1.1	It is the PKI infrastructure that supports electronic authentication rather than the PIV infrastructure. PIV is only an identity verification process utilizing specific PKI keys and credentials.	Reword to read: "...investment in the PKI infrastructure for electronic authentication..."	Declined. Derived PIV Credentials leverage the current investment in the entire PIV infrastructure, not just the PKI.
162	DoS	CR Froehlich	T	5	260-261	1.1	It is unclear if this requires continuous interaction between the mobile device and the PIV Card, if it must be repeated for each specific actions (e.g., signing), or if it is only upon establishing connection.	Reword to clarify how the card is used vis-a-vis the device (e.g., "... need to continuously hold or place...").	Resolved by comment #120.
163	DoS	CR Froehlich	T	6	271-272	1.2	PKI, both before and after the creation of the PIV Card, required the use of FIPS 140 validated cryptographic modules; this practice needs to be continued.	Reword to read: "...tokens may be either FIPS 140 approved hardware or software..."	Declined. This section provides purpose and scope not requirements.
164	DoS	CR Froehlich	T	6	276-277	1.2	Given that this is a PIV Derived Credential, will NIST include a provision limiting such credentials to GFE in the same manner that FIPS 201 limited PIV Cards to FTE and on site contractors, etc.; and what is the rationale behind whatever decision is made?	Modify this section to address limitations on issuance of PIV Derived Credentials and the rationale for the decision	Declined. Draft SP 800-157 already states that Derived PIV Credentials may only be issued to individuals who possess valid PIV Cards. The credentials are issued to individuals, not devices, and there is no intention to prevent the private key from residing on a personally owned device. SP 800-157 is not the appropriate venue to either support or preclude BYOD policies.
165	DoS	CR Froehlich	T	8	326-328	1.5	The FCPCA Certificate Policy (CP), reflecting FIPS 201, refers to an “Applicant” as someone who is in process of applying for PIV card; and a Subscriber as someone who has been issued a PIV card—most probably with digital signature and encryption certificates also installed on the card. SP 800-157 unnecessarily modifies those established definitions.	Revise the definitions of "Applicant" and "Subscriber" to coincide with FIPS 201 and the Federal Common Policy Certification Authority (FCPCA) Certificate Policy (CP).	Resolved by comment #76.
166	DoS	CR Froehlich	T	9	333-336	2	This statement ignores the facts that the characteristics and configuration of the certificates, and the operations and security of the issuing CA are also subject to an annual PKI compliance audit in accordance with the FCPCA CP that is separate from the identified “independent assessment.” There are also existing requirements for Derived Credentials in SP 800-63-2 that are not specifically related to use with mobile devices.	Reword to read: "In accordance with [HSPD-12], the reliability of the Derived PIV Credential issuer shall be established through an official accreditation process. The processes, as outlined in [SP800-79] and the Federal Common Policy Certification Authority (FCPCA) Certificate Policy (CP), shall include an independent (third-party) assessment. Derived Credentials shall also comply with the requirements in SP 800-63."	Declined. The referenced text is about the official accreditation process, not certification compliance audits or general issuance requirements. So references to [COMMON] or SP 800-63 in this text would be inappropriate.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
167	DoS	CR Froehlich	T	9	342	2.1	If the document means "valid" then this should say that—active has no meaning in this sense.	Reword to read: "The PIV Authentication certificate shall be validated 341 as being valid and not revoked prior to issuance of a Derived PIV Credential, and..."	Resolved by changing part of the sentence from: "The PIV Authentication certificate shall be validated as being active and not revoked" To: "The PIV Authentication certificate shall be validated."
168	DoS	CR Froehlich	T	9	344-346	2.1	This requirement is unclear; who performs this check and how? The 7-days exactly reflects the exemplar language in SP 800-63 ["(e.g., after a week)"]; however, the RA for the Derived Credential issuing CA can (should) check the status of the certificate immediately—the FCPCA CP requires that revoked credentials be posted within 6 hours.	Reword to read: "The revocation status of the Applicant's PIV Authentication certificate shall be checked immediately and rechecked seven (7) calendar days following issuance of the Derived PIV Credential – this step protects against the use of a compromised PIV Card to obtain a Derived PIV Credential."	Declined. The PKI-AUTH authentication mechanism already includes a check of the revocation status of the PIV Authentication certificate, so the requirement to "check immediately" is already in the text.
169	DoS	CR Froehlich	T	9	349-354	2.1	While this may be acceptable IAW SP 800-63, the FCPCA CP requires that the "Applicant" appear in person or by trusted agent proxy for initial issuance for other than Common High ("*For all other policies, RAs may accept authentication of an applicant's identity attested to and documented by a trusted agent to support identity proofing of remote applicants, assuming agency identity badging requirements are otherwise satisfied* .") Automated remote authentication is only accepted for renewals, and then only if the original certificate is still valid. It also presumes that the certificate is being issued by the same CA, whereas SP 800-157 permits the Derived Credential to be issued by a different CA.	Reword the first sentence in the paragraph to read: "An LOA-3 Derived PIV Credential shall be initially issued in person, but may be renewed remotely or in person in accordance with [SP800-63] and the FCPCA CP."	Declined. The change proposal that has been submitted for the Common Policy to add the new certificate policies for Derived PIV Authentication certificates allows for certificates to be issued under the id-fpki-common-pivAuth-derived policy without an in person appearance.
170	DoS	CR Froehlich	T	9	355-359	2.1	The first two sentences are contradictory. The first mandates the use of the biometric on the PIV Card; the second -- in an attempt to replicate the LOA-3 multiple transaction requirement -- permits the use of "...a biometric that was recorded in a previous transaction" without further specificity. If the intent is to use the PIV Card biometric, then this should clearly state that.	Reword to read: "...issuance process, the Applicant shall identify himself/herself using a biometric sample that can be verified against the PIV Card in each new encounter."	Declined. The two sentences are not contradictory as the first sentence applies to the initial in person identification and the second sentence applies to subsequent in person identifications.
171	DoS	CR Froehlich	T	9	359-360	2.1	Retention of biometric samples has PII considerations; SP 800-157 should clearly make reference to protecting them in accordance with the Privacy Act.	Reword to read: "...used to validate the Applicant in accordance with the Privacy Act [PRIVACT]."	Resolved by adding a footnote at the end of the sentence as follows: The retained biometric shall be protected in a manner that protects the individual's privacy. See also resolution to comment # 243.
172	DoS	CR Froehlich	T	9	361-364	2.1	This identifies a potentially serious threat but makes no policy/recommendation about corrective action.	Reword to establish at least a guideline or pointer to the location of any such corrective action.	Noted. Federal Departments and Agencies should consider the risk associated with the issuance of multiple derived PIV credentials as a part of their risk management process.
173	DoS	CR Froehlich	T	9 & 10	368-369	2.2	This statement is unnecessarily vague—the only CP applicable to PIV certificates is the FCPCA CP.	Reword to read: "…in accordance with the Federal Common Policy Certification Authority (FCPCA) Certificate Policy."	Resolved by comment #95.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
174	DoS					General	At this time, D-PIV only appears to be associated with the parent PIV-Card Issuer. Is this the intent of the standard? Should another agency or issuer be allowed to issue D-PIV creds based on a PIV card issued by another issuer?	Strong binding between D-PIV and the PIV issuer is highly recommended. Additional guidelines, in terms of when D-PIV needs to be revoked (based on PIV lifespan, revocation status, etc.), need to be developed. Information is needed on the circumstances when a D-PIV needs to be revoked because the PIV card has been revoked or terminated (in alignment with the guidelines of the assiciated	Noted. Please refer to Section 2.3 (previously Section 2.2) that discusses the relationship between the status of the PIV Card and the Derived PIV Credential.
175	DoS				695	B.1.2.1	D-PIV mentions that the container used for D-PIV will be different from the PIV container	More details are needed around what containers would be used in relationship to D-PIV and the other contents and how that content is linked back to the parent PIV credential.	Declined. Section B.1.2 lists the one mandatory data object for the PIV Derived Application along with all of the optional data objects and provides detailed information about the contents of each data object. The body of the document, along with Appendix A, already specifies what link, if any, there is between the data stored in the PIV Derived Application and the data stored on the PIV Card.
176	DoS	CR Froehlich	T	10	369-378	2.2	The citation of specific PKI policy requirements in a NIST SP, vice the Federal Common Policy, is inappropriate.	Delete this text and refer to the Federal Common Policy Certification Authority (FCPCA) Certificate Policy (CP).	Noted. NIST consulted with the CPWG and the CPWG did not feel that the original text was inappropriate.
177	DoS	CR Froehlich	T	10	379-381	2.2	These provisions must be consistent with the FCPCA CP. Given that PIV is only covered by the Federal Common Policy, the vague reference to an unnamed certificate policy, as well as the inclusion of a policy directive, is inappropriate. In addition, a damaged PIV Card is not cause for revocation of the certificates housed therein, therefore there is no reason to presume that a damaged mobile device should require revocation of the associated certificate.	Reword to read: "...Credential is lost, stolen, or compromised, the PIV ... revoked in accordance with the Federal Common Policy Certification Authority (FCPCA) Certificate Policy (CP)."	Resolved by comment #95. Also, if a cryptographic module has been damaged then the status of the keys on the token are unknown and so the corresponding certificates need to be revoked.
178	DoS	CR Froehlich	T	10	382-389	2.2	This represents a significant change in bedrock thinking of the Federal PKI, which has always been that any loss or theft of one credential bound to the identity of an individual results in the revocation of all credentials bound to that individual's identity. The Derived Credential is directly related to the credentials on the PIV Card, which substantiated the identity of the holder of all of these credentials. This portion also fails to differentiate between situations in which the PIV Card is unavailable (e.g., the Subscriber is not physically located at a terminal/workstation with a card reader) and the PIV Card is no longer in the possession and/or under the positive control of the Subscriber. Lastly, since the identity of the certificate holder is the same across both PIV Card and Derived Credentials, any change in the underlying identity attributes must result in a change to all certificates based on those attributes.	Reword to read: "The Derived PIV Credential is directly affected by loss, theft, or compromise to the Subscriber's PIV Card due to the inter-relationship of the Subscriber's proof of identity.[5] The ability to use the Derived PIV Credential is especially useful in circumstances when the PIV Card is unavailable or unusable, yet the Subscriber is able to use the Derived PIV Credential to gain logical access to remote Federally controlled information systems from his/her mobile device. Similarly, the Derived PIV Credential may be directly affected by the revocation of the PIV Authentication certificate depending on the circumstances. Some maintenance activities for the subscriber's PIV Card may trigger corresponding maintenance activities for the Derived PIV Credential. For example, if the subscriber's PIV Card is reissued as a result of the Subscriber's name change, a new PIV Derived Authentication certificate with the new name will also need to be issued."	Declined. If a applicant for a PIV Card uses a driver's license and a passport to identify himself or herself when applying for a PIV Card, there is no requirement to revoke the PIV Card if either the driver's license or passport is subsequently lost or stolen. There is no more reason that the subsequent lost or theft of a PIV Card should have any effect a Derived PIV Credential, as long as there is evidence that the PIV Card wasn't lost or stolen until after the Derived PIV Credential was issued and there is no evidence that the cryptographic token containing the PIV Derived Authentication private key was lost or stolen. See also comments #97, #153.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
179	DoS	CR Froehlich	T	10	391-395	2.3	How does this provision correspond to the fact that the preceding paragraph allows the PIV Derived Credential to continue effectiveness if the PIV Card is compromised (i.e., lost or stolen)? Even in benign termination situations, FIPS 201 and the FCPCA CP require certificate revocation and card destruction. Further, the termination of the PIV Derived Credential MAY be terminated if the entity determines that it is no longer required. A MAY statement could permit the Subscriber to retain the credential even if the sponsoring entity determines that it is no longer required.	Reword to read: "A Derived PIV Credential shall be terminated when the department or agency that issued the credential determines that the Subscriber is no longer eligible to have a PIV Card (i.e., PIV Card is terminated[6]). A Derived PIV Credential shall also be terminated when the department or agency that issued the credential determines that the Subscriber no longer requires a derived credential, even if the Subscriber's PIV Card is not being terminated."	Accept.
180	DoS	CR Froehlich	T	10	398-401	2.3	The statement "If the PIV Derived Authentication private key was created and stored on a hardware cryptographic token..." is misleading. All LOA3 certificates must be generated on a FIPS 140, level 1 (software) or higher token; and, LOA4 certificates must be generated on a FIPS 140 level 2 (hardware) or higher token with physical security at FIPS 140 level 3 or higher per SP 800-63. In addition, FIPS 140 does not permit export of the private key from hardware in any event.	Reword to read: "If the PIV Derived Authentication private key was created and stored on a hardware cryptographic token at LOA-3 or LOA-4 that does not permit the user to export the private key, then termination of the Derived PIV Credential may be performed by either:..."	Declined. Adding "at LOA-3 or LOA-4" does not add anything since all Derived PIV Credentials are issued at either LOA-3 or LOA-4. FIPS 140 does permit private keys to be exported from hardware.
181	DoS	CR Froehlich	T	11	409-411	2.4	This statement is inconsistent with the first sentence in this subparagraph; and, it is inconsistent with the provisions of FIPS 201 and the FCPCA CP, which state, respectively: "(§2.9.4) A PIV card is terminated when the department or agency that issued the card determines that the cardholder is no longer eligible to have a PIV Card. The PIV Card shall be terminated… " Similar to the situation in which the card or a credential is compromised, normal termination procedures must be in place as to ensure the following: + The PIV Card itself is revoked: ● The PIV Card shall be collected and destroyed, if possible. ● Any databases maintained by the PIV Card issuer that indicate current valid (or invalid) FASC-N or UUID values must be updated to reflect the change in status.	Reword to read: "The issuer of the Derived PIV Credential shall not solely rely on tracking the revocation status of the PIV Card certificate as a means of tracking the termination status of the PIV Authentication certificate. This is because there are scenarios where the card's PIV Authentication certificate is not revoked even though the PIV Card has been terminated."	Declined. There is no such thing as a "PIV Card certificate" and FIPS 201-2 refers to termination of PIV Cards, not certificates. The current text is consistent with FIPS 201-2, which states that the PIV Authentication certificate on a PIV Card does not need to be revoked when a PIV Card is terminated if the PIV Card has been collected and destroyed.
182	DoS	CR Froehlich	T	11	420-429	2.4	It is unlikely that this situation would occur, but would have to be addressed in the FCPCA CP.	Consider adding "must be compliant with the FCPCA CP".	Declined. This text is about mechanisms by which the issuer of a Derived PIV Credential may monitor the status of a PIV Card. The Common Policy is not relevant to this.
183	DoS	CR Froehlich	T	12	444-446	3.1	There should be only one certificate policy related to any PIV certificate—the FCPCA CP. Further, there are existing conditions in the FCPCA CP regarding the expiry relationships between certificates and the PIV card (i.e., the former cannot exceed the latter).	Reword to read: "The expiration date of the PIV Derived Authentication certificate is based on the Federal Common Policy Certification Authority (FCPCA) Certificate Policy (CP)."	Declined. Requirements relating the expiration of certificates on a PIV Card to the expiration date of the PIV Card itself are not relevant to the PIV Derived Authentication certificate.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
184	DoS	CR Froehlich	T	13	471-473	3.3	The FCPCA CP already contains language that may be in conflict with this provision: §6.2.4.2 "Subscriber private signature keys whose corresponding public key is contained in a certificate that does not assert id-fpki-common-authentication, id-fpki-common-cardAuth, or id-fpki-common-High may be backed up or copied, but must be held in the subscriber's control. Backed up subscriber private signature keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module." §6.2.4.5 "Device private keys may be backed up or copied, but must be held under the control of the device's human sponsor or other authorized administrator. Backed up device private keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the device's cryptographic module."	Consider deleting this text in favor of having it addressed in the FCPCA CP.	Declined. The text is not in conflict as the text in the Common Policy notes that when the certificate is not issued under a "hardware" policy the corresponding private keys may be backed up or copied.
185	DoS	CR Froehlich	T	17	605-609	Appendix A	Depending on the PKI product used by the issuer(s), this may or may not be possible. In addition, FIPS 201 and the FCPCA CP have strict rules regarding the binding of certificates to Subscriber identities. A given person may receive multiple certificates, but not under the same identity name space, which are clearly specified in the FCPCA CP.	Add the following as a footnote: "Depending on the PKI product used by the issuer(s), this may or may not be possible. In addition, FIPS 201 and the FCPCA CP have strict rules regarding the binding of certificates to Subscriber identities. A given person may receive multiple certificates, but not under the same identity name space, which are clearly specified in the FCPCA CP."	Declined. The text in lines 605-609 (line 926-930 in final document) is not proposing the issuance of additional certificates, but that the same private keys and certificates appear on both the PIV Card and the mobile device.
186	DoS	CR Froehlich	T	17	611-618	Appendix A	While policies do not absolutely prohibit issuing multiple certificates to the same individual, they do prohibit issuing multiple certificates to the same identity, (i.e., John Q. Public can have only one certificate issued under the name space specified in the FCPCA CP). Each certificate issued would require its own identity, and there would be no way to associate the identities between the certificates automatically.	Add the following as a footnote: "While policies do not absolutely prohibit issuing multiple certificates to the same individual, they do prohibit issuing multiple certificates to the same identity, (i.e., John Q. Public can have only one certificate issued under the name space specified in the FCPCA CP). Each certificate issued would require its own identity, and there would be no way to associate the identities between the certificates automatically."	Noted. Certificate policies do not prohibit issuing multiple certificates to the same identity. Many PIV Cards issued today include three certificates issued to the same identity (a PIV Authentication certificate, a digital signature certificate, and a key management certificate). Some CA products may not allow multiple digital signature certificates to be issued to a single identity, but this would be a product limitation, not a policy limitation. This product limitation may be overcome by either using different subject names in the different digital signature certificates or by issuing the different certificates from different certification authorities.
187	SSA	Eric Mitchell		14	530	3.3.1.3	This Special Publication allows for alternative form factors, such as USB tokens, with nearly all the functionality of a PIV smart card. However, contactless PACS functionality is not addressed. Due to the lack of durability in the smart card form factor, alternative/additional credential form factors could benefit the PACS realm as well.	Consider specification of contactless PACS functionality for derived credentials.	NIST (157) Resolved by comment #15
188	Smart Card Alliance	Adam Shane, AMAG Technology	G	10	394	2.3	"...Subscriber no longer requires a derived credential, …" Derived credentials that are not Derived PIV Credentials are out of scope of the document per section 1.2.	Change statement to, "...Subscriber no longer requires a Derived PIV Credential , …"	Accept.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
189	Smart Card Alliance	Adam Shane, AMAG Technology	T	9		2	Section 2, Lifecycle activities, is missing a major component of the lifecycle - operational use of the Derived PIV Credential. This should most logically be inserted before "Termination" but could be added as section 2.5.	Insert a section on "Usage" at the 2.n level between 2.2 and 2.3. Reference existing federal guidance on usage, perhaps SP 800-63 section 8.3.2.	Resolved by comment #78.
190	Smart Card Alliance	Adam Shane, AMAG Technology	T	15	562	3.4.1	"The required PIN length shall be a minimum of six bytes." The number of bytes used to represent the PIN is very different than the number of digits in the PIN. For example, using a Unicode encoding (2 bytes per character) the PIN could be as little as 3 digits in the above requirement. By the same token, 6 numeric digits can be encoded into as little as 20 bits (under 3 bytes).	State the requirement in terms of fuctionality ("digits" or "characters"), not implementation ("bytes"). FIPS 201 states "The required PIN length shall be a minimum of six digits." If the intent is to allow any alphanumeric, this could be expanded to "The required PIN length shall be a minimum of six characters."	Resolved by comment #123.
191	Smart Card Alliance	Adam Shane, AMAG Technology	G	20	712	Appendix B	Section B.1.4.1 is missing.	Sections B.1.4.2 through B.1.4.4 should be renumbered.	Accept
192	Smart Card Alliance	Adam Shane, AMAG Technology	T	20	700	B.1.2.1	Need to be consistent with FIPS 201-2	FIPS S 201-2 Page 41 Section 4.2.2 states: " Any operation that may be performed over the contact interface of the PIV Card may also be performed over the virtual contact interface".	Resolved by comment #15. Note the focus SP 800-157 is Derived PIV Credentials not the PIV card.
193	Smart Card Alliance	Chris Edwards, Intercede	T			3.3	Some vendors have produced a small keyfob-sized Bluetooth card reader that takes a Micro-SIM form factor secure element (e.g., the Tyfone SideKey). This allows an existing approved PIV card, physically cut-down and without the contactless antenna, to be used by a Bluetooth enabled smart phone. Technically the connection to the chip itself is over the contact interface, but there is a contactless component in the overall system. This is an attractive option in many respects, as it enables FIPS140 approved hardware to be used immediately with a smartphone. However, the SP 800-157 restrictions on contactless communications could be interpreted as disallowing such devices, even though the communications channel does have AES encryption.	Clarify if a derived credential stored on an external hardware device where the secure element is inserted in, or is part of the device that then connects to the phone with a wireless interface (e.g., Bluetooth) is allowed. This may be an attractive use case since it enables FIPS140 approved hardware to be used immediately with a smartphone.	Resolved by changing: "Three kinds of removable hardware tokens are specified..." to: "Three kinds of removable hardware tokens are permitted..." See also resolution of comment #56.
194	Smart Card Alliance	Andrew Atyeo, Intercede	T	12	442	3.1	It is not clear whether the intention is that the DN for the Derived PIV authentication certificate should be the same as the DN for the original PIV authentication certificate used to issue this derived credential. Since the FPKI common policy worksheets tend to describe the structure of the individual certificate types (rather than the relationship between different	Guidance would be helpful in SP800-157 to indicate whether the DN of the derived credential should be bound to the original credential or not.	Declined. Requirements for the subject DNs in certificates are specified in Section 3.1.1 of the Common Policy.
195	Smart Card Alliance			6	267	1.2	This document provides guidelines for cases in which the use of PIV Cards with mobile devices.	S	Noted.
196	Smart Card Alliance			iv	209	Executive Summary	SP 800-157 does not address use of the PIV Card with mobile devices, but instead provides an alternative to the PIV Card in cases in which it would be impractical to use the PIV Card. Instead of the PIV Card, SP 800-157 provides an alternative token, which can be implemented and deployed directly on mobile devices (such as smart phones and tablets).	SP 800-157 does not address use of the PIV Card with mobile devices, but instead provides an alternative to the PIV Card in cases in which it would be impractical to use the PIV Card. Instead of the PIV Card, SP 800-157 provides an alternative token, which can be implemented and deployed directly with mobile devices (such as smart phones and tablets).	Accept.
197	Smart Card Alliance			10	385	2.2	Similarly, the Derived PIV Credential is unaffected by the revocation of the PIV Authentication certificate.	Similarly, the Derived PIV Credential is not necessarily affected by the revocation of the PIV Authentication certificate.	Accept.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
198	Smart Card Alliance			11	425	2.4	The issuer of the PIV Card maintains a list of corresponding Derived Credential issuers and sends notification to the latter set when the PIV Card is terminated	The issuer of the Derived PIV Credential shall notify the original PIV issuer when a derived credential is created.	Resolved by adding the following sentence at the beginning of the bullet: The issuer of the Derived PIV Credential notifies the original PIV issuer when a Derived PIV Credential is created.
199	Smart Card Alliance			11	430	2.4	The linkage beween the Derived PIV Credential and the subscriber's PIV Card shall be updated when the Subscriber obtains a new PIV Card.	It is the responsibility of the issuer of the derived PIV Credential to maintain the link to the original, or updated PIV credential.	Noted
200	Smart Card Alliance			11	430	2.4	Need consistent and efficient policy and method to revoke a PIV derived credential afer the original non-compromised PIV has been returned and destroyed.	A non-compromised PIV credential that has been returned and physically destroyed does not require the certificate to be placed on the CRL. Clarify how derived credential issuers know this have ocurred.	Noted. This topic is discussed in Section 2.3 (now Section 2.4) of this document. There are numerous ways to manage the link between the PIV Card and its associated Derived Credentials, this document provides three potential use cases.
201	NASA	Dennis Kay	Addition	10	381	2.2	We believe there is another case for Derived PIV Credential termination when a subscriber's mobile device, with a PIV derived credential is encoded, is transferred to another individual.	After line 381, recommend including the following text: "In the case of the transfer of ownership of a mobile device to another individual, and when a removable (non-embedded) hardware cryptographic token is not removed for installation in a different mobile device in possession of the subscriber, the PIV Derived Credential encoded in removable and embedded tokens shall be revoked."	Resolved by stating that key shall be zeroized (or the certificate revoked) when tokens or mobile device are transferred.
202	NASA	Dennis Kay	Editorial	10	379-381, plus text in #1	2.2, 2.3	The text in lines 379-381, and our suggested addition in #1, more closely aligns with "Termination".	Lines 379-381, with the addition of the text "In the case of the transfer of ownership of a mobile device to another individual, and when a removable (non-embedded) hardware cryptographic token is not removed for installation in a different mobile device in possession of the subscriber, the PIV Derived Credential shall be revoked," should be moved to section 2.3 Termination, inserted between lines 397 and 398.	Declined. The text in line 379-381 (line 209-211 in final document) is not about termination. See also comment 201.
203	NASA	Dennis Taylor	Technical	17	601-605	Appendix A	FIPS 201-2 states: “Key Management Key. This key may be generated on the PIV Card or imported to the card.” This leads to the idea that we have some freedom here. However SP 800-73-4 Part 1, 3.2.2, X.509 Certificate for Key Management, and SP 800-Part 1, 3.2.4 states: “This key pair may be escrowed by the issuer for key recovery purposes.” We believe this statement indicates any KMK not resident on card may only be used for escrow. Minimally we believe this statement can be subject to such ambiguous interpretation.	Acceptable storage locations and uses for the KMK key should be explicitly defined.	Declined. It is unclear why the text in SP 800-73 is interpreted as stating that any copy of the KMK not on the card may only be used for escrow. As noted in Appendix A, the acceptable storage locations for the private key depend on the policy under which the corresponding certificate was issued.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
204	NASA	Dennis Taylor	Addition	15	549	3.3.2	Section 3.3.2 Embedded Cryptographic Tokens: We would like to see specific mention of the Trusted Platform Module (TPM). The TPM has a very large industry presence and has the backing of a large community of industry partners. The TPM technology is quite mature and in the desktop/laptop area quite ubiquitous. It is becoming more prevalent on the smaller mobile device platforms. Specific mention of this acceptable hardware token here would likely encourage even greater industry support. Conversely, an obvious omission of reference might cause a negative inference.	Insert sentence in line 549, after "device.": "An example of a hardware embedded cryptographic token is a Trusted Platform Module (TPM)."	Resolved by including a pointer to the NISTIR in Section 3.3.2. (TPM, TEE, OS key store, SE).
205	NASA	Ridley DiSiena	Technical	17	596-618	Appendix A	Appendix A describes a valid S/MIME use case of a mobile device leveraging the same key management key certificate as used on the PIV Card with a secondary digital signature certificate other than the digital signature certificate issued to the PIV Card. Some certificate authority products being used to issue PIV cards today do not allow multiple active digital signature certificates issued to the same DN (distinguished name). Is it the intent of NIST SP 800-157 that multiple active digital signature certificates should be issuable to the same subject DN from the same certificate authority? Furthermore if the guidance is not specific would this imply that to overcome current product limitations, issuance of alternate signature certificates under different DNs or even different CAs is perfectly acceptable as long as they conform to the requirements of the certificate policies. These issuance differences could result in an identity duality with unique challenges that had not been previously encountered.	Additional guidance for alternative digital signature certificates issuance should be provided.	Declined. It is not the intent of SP 800-157 that a single CA should be able to issue multiple digital signature certificates with the same subject DN, nor does SP 800-157 discourage issuing multiple digital signature certificates from the same CA with the same subject DN. Issuers may choose to issue additional digital signature certificates from different CAs or with different subject DNs.
206	NASA	Ridley DiSiena	Technical	17	596-618	Appendix A	Appendix A implies a use case where a subscriber may actively use both the digital signature certificate on the PIV card and an alternative digital signature certificate. Depending if there are differences in the certificate policies in each certificate, this could introduce scenarios where there will be a mix of digital signature assurance levels being used for digital signing for the same individual. Considering the intent of FIPS 201-2 to have the digital signature key generated on the card and not be exportable, allowing an alternative signature certificate with relaxed policies introduces the question of appropriate usage of each certificate.	Additional guidance for alternative digital signature certificate usage should be provided.	Declined. It is up to Departments and Agencies to consider this risk as they create their digital signature certificate issuance and usage policies.
207	Sublett Consulting	Christine Sublett	E	6	281	1.2	This shows a mobile device with Derived PIV Credential as an access terminal, and it should show it as a second factor of authentication. 1-Factor authentication is not equivalent to PIV + data terminal. Attackers could login with a PIN from the user’s terminal.	Add a system physically separate from the Mobile Device with Derived PIV to connect.	Resolved by comment #57.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
208	Sublett Consulting	Christine Sublett	T	12	459	3.3	This section is missing information about proximity tokens.	New section: Proximity tokens can be either soft tokens that store keys in the keychain or SE or hardware Bluetooth LE tokens that store keys. They act as a second factor and are physically separate from the data terminal. Encrypted communication with the data terminal is performed over the Bluetooth LE channel. The device requires only passive user action; keeping it in their possession. Proximity security alarms and locks data when left unattended. This solution provides high availability, as all major mobile platforms support Bluetooth LE.	Resolved by resolution to comment #56.
209	Sublett Consulting	Christine Sublett	T	23	789	Appendix B-B2	PIV Derived Authentication Certificate: Add a row: Token Type=Proximity Token Assurance Level=Very High	PIV Derived Authentication Certificate: Add a row: Proximity Token: Very High	Resolved by resolution to comment #56.
210	Sublett Consulting	Christine Sublett	G	24	807	Appendix D	Missing	Add definition of Proximity Token: Proximity tokens can be either soft tokens that store keys in the keychain or SE, or hardware Bluetooth LE tokens that store keys.	Resolved by resolution to comment #56.
211	Wave	Thibadeau	General Problem	Multiple		General	There is no mention of TPMs despite Windows Phone, etc. No definitional difference between pure software, firmware and hardware. Examples where restrictive Industry Standards are already referenced include SD Cards, NFC, UICC, X.509, etc.	Add "TCG TPM" or "TPM" as appropriate	Resolved by comment #204.
212	Wave	Thibadeau	misleading	iv	footnote 1	Footnote	too restrictive on list, not realistic	add "portable laptops", "smart glasses", "smart watches" among the examples	Resolved by comment #41.
213	Wave	Thibadeau		6	271	1.2	have example of all but embedded, TPM is a valid example	"mobile device." Should be "mobile device (such as a TPM)."	Resolved by comment #204.
214	Wave	Thibadeau		15	546	3.3.2	In every other class you mention a specific token …why isn't a TPM called out here. TCG has a mobile 2.0 spec nearly out and the TPM 2.0 is suitable for Phones … as proven by the Windows / Nokia Phones.	"cryptographic modules" should read "cryptographic modules such as TPMs.	Resolved by comment #204.
215	MSFT	Paul Fox	E	9	345	2.1	How often does the applicant's PIV auth certificate have to be checked for revocation? Section 2.4 talks about linked PIV cards being zeroized in which the associated PIV-Auth certificate will not be revoked.	The revocation status of the Applicant’s PIV Authentication certificate shall be rechecked ***and CMS PIV card status every*** seven (7) calendar days following issuance of the Derived PIV Credential – this step protects against the use of a compromised PIV Card to obtain a Derived PIV Credential.	Declined. Section 2.1 (Section 2.2 in final document) is about the issuance of the Derived PIV Credential, and advices one recheck seven calendar days following issuance of the Derived PIV Credential. The requirement to terminate the Derived PIV Credential if the PIV Card has been terminated is addressed in Sections 2.3 and 2.4.
216	MSFT	Paul Fox	T	10	386	2.2	Please define manditory PIV Card maintenance triggers that would require updating the derived credential	No Suggested Text	Resolved updating existing text to read: "Some maintenance activities for the subscriber’s PIV Card may trigger corresponding maintenance activities for the Derived PIV Credential, since the Derived PIV Credential will need to be reissued if any information about the Subscriber that appears in the credential changes. For example, if the subscriber’s PIV Card is reissued as a result of the Subscriber’s name change and the Subscriber’s name appears in the Derived PIV Authentication certificate, a new Derived PIV Authentication certificate with the new name will also need to be issued"

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
217	MSFT	Paul Fox	T	11	420	2.4	Recommend defining the fequency of the Backend Attribute Exchange / URRS to account for zeroized PIV cards	No Suggested Text	Resolved by adding text to section 2.4 that an 18 hour interval is recommend to maintain consistency with revocation requirements in FIPS 201-2.
218	MSFT	Paul Fox	T	16	578	3.4.1	Are remote, non-biometric matched PIN unlocks for LOA-4 derived credentials allowed?	No Suggested Text	Yes. The steps required for a remote password reset are specified in lines 578-584 (lines 419-425 in final document), and none of the steps involve performing a biometric match.
219									Duplicate removed
220		Paul Fox	T	10	386	2.2			Duplicate removed
221		Paul Fox	T	11	420	2.4			Duplicate removed
222									Duplicate Removed
223	MSFT					General	Enhanced security assurance through embedded tokens. With advances in trusted computing technology or other hardware-based security features, Microsoft has moved to provide our customers benefits with practical features over a very long period of time. Trusted computing technologies have become widely available through the efforts of organizations like the Trusted Computing Group that define specifications for hardware such as the Trusted Platform Module (TPM). The Trusted Computing Group has published TPM specifications for almost ten years and TPM 1.2 was accepted as an ISO/IEC 11889 standard in 2009. Today, TPM can be found on more systems than ever before with over 4 million TPM chips shipped worldwide.	TPM has been recognized as an important security component in protecting information systems and end users. TPM exemplifies hardware-based protection of both the hardware and software cryptographic module scenarios by acting as an embedded hardware module or a mechanism to protect the software-based module. While alternatives to PIV form factors such as microSD or USB can be acceptable token types, the evolution of security is trending towards removable (external) form factors as less desirable than embedded mechanisms such as TPM. Moreover, using embedded form factors provides the added assurance of tying the credential directly to the device itself, which provides protection against tampering and reduces the need for higher levels of assurance that can be cost prohibitive and gratuitous for most use case scenarios.	Noted.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
224	MSFT			9	347-348	2.1	Desirable security outcomes achieved through Level of Assurance 3 for Derived Credentials. In determining the policy around appropriate levels of assurance acceptable with a mobile device, the USG needs to balance several factors including security, end user experience, and cost, among others. That is, given the form factor of a tablet or smartphone and the security measures in place today, a) what types of activities can be securely performed and b) what is the commensurate authentication required to support those activities? When examining the majority of mobile device use cases employed by federal agencies today, LOA 3 derived credentials provide substantial security improvements over the prevailing and increasingly insufficient username/password paradigm and demonstrate alignment with the current applications in use at most of the Executive branch agencies.	The security features in LOA 3 derived credentials on a mobile device based on LOA 4 physical PIV credential is an advantageous solution and paradigm for achieving the goal of HSPD-12 to “promote interoperable authentication mechanisms at graduated levels of security based on the environment and sensitivity of the data.” In fact, having a model that leverages both a LOA 4 PIV card and a LOA 3 PIV derived credential could achieve the right balance between authentication assurance vis a vis the mobile device form factor. For example: High Business Impact (LOA-4) – PIV card required Medium Business Impact (LOA-3) – PIV Derived Credential In such a scenario, the LOA3 derived credential can be protected and verified using the TPM-based platform solutions. Using the TPM to tie the user to the machine, creating a derived PIV LOA3 credential based on the user’s PIV card and a TPM-based protection of that credential, which uses PKI-based certifications can be a viable alternative. Since the security of and user need for LOA 4 using a derived credential has not yet been fully considered, we encourage NIST to reference the use of the actual PIV LOA 4	Noted. As described in NIST IR 7981, there are several options for LoA-4 credentials -- including the use of the PIV Card.
225	MSFT					General	Implementation of Derived Credentials guidance is critical for success. Governments and enterprises have recognized the security challenges prevalent in the information and communication technology ecosystem. While software-based security has matured over time with the release of new software products, hardware-based security assurances have taken more time to mature because of their dependency on hardware and software. Organizations need a significant amount of time to deploy new hardware. Reaching a point where an organization is able to capitalize on hardware based security features in a uniform way is challenging and often elusive.	Given the varying levels of security parity among hardware and software providers, NIST, OMB, and DHS collectively play a pivotal role in synchronizing the security features currently available in consumer technology with the agencies’ growing appetite to adopt this technology in the federal enterprise- an environment in which the security parameters and governing policies for newer technology are still being defined. We urge this collective to maintain a phased policy development and implementation approach that continues to leverage the expertise of device and services providers. In so doing, the federal government can position itself to successfully integrate BYOD and effective information security as it embraces the digital government era.	Noted.
226	MSFT					General	Organizations need a significant amount of time to deploy new hardware.	Suggested agencies to maintain a phased policy development and implementation approach that continues to leverage the expertise of device and services providers. In so doing, the federal government can position itself to successfully integrate BYOD and effective information security as it embraces the digital government era.	Noted.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
227	Apple Inc.	Shawn Geddis		6	276-277	1.2	States purpose is to provide PIV-enabled authentication services. What about the use for S/MIME which is not authentication, but rather signing and encrypting email communication. What about for additional Data-At-Rest protection (Encryption). Is the Derived Credential solely for remote user authentication and nothing else ? If this is indeed restricted to just user authentication, it severely limits the scope of use and value add to the mobile device. Appendix B suggests that there are additional uses, since the data objects support other uses.	The scope of the Derived PIV Credential is to provide PIV-enabled services on the mobile device as is done currently on a desktop device with the PIV Card.	Resolved by comments #5 and #6.
228	Apple Inc.	Shawn Geddis		10	378	2.2	Notes that you must follow the initial issuance process if "re-key of a derived PIV Credential at LOA-4 to a new hardware token" There does not seem to be any reference to the identification or retention of what HW token storage container is in use relating to a credential. If it is never retained, how would the system know if it was a "new" hardware token ? What happens if a particular hardware token was damaged and replaced by a similar hardware token type? Are you requiring HW Tokens to maintain unique and unmodifiable HW ID so that you can always ensure it is the same one ?	(If you are looking to ensure that a LOA-4 credential isn't being re-issued to a new HW token without going through the initial issuance process, there would need to be unique identification of the HW Token retained by the system.)	Resolved by adding a footnote stating that the issuer has to uniquely identify the token at re-issuance to ensure that the new credential is issued to the same token.
229	Apple Inc.	Shawn Geddis		10	382	2.2	The loss, theft or damage of a Subscriber's PIV Card would seemingly cause all derived credentials to be revoked to mitigate risks. It should follow logic of starting over with initial issuance.	"All Derived PIV Credential(s) shall be revoked if the Subscriber's PIV card has been lost or stolen. If the PIV card has been damaged, the Derived PIV Credential is unaffected."	Resolved by comments #97 and #178
230	Apple Inc.	Shawn Geddis		10	385-386	2.2	"The Derived PIV Credential is unaffected by the revocation of the PIV Authentication Certificate." Functionally, the Derived Credential is bound by the PIV Card Credential, so it should absolutely be affected by revocation of the PIV Auth Cert.	"All Derived PIV Credential(s) shall be revoked if the PIV Authentication certificate has been revoked."	Resolved by comments #97 and #178
231	Apple Inc.	Shawn Geddis		12	444-446	3.1	Expiration of PIV Derived Authentication Certificate is not based/related to the expiration of PIV Auth Cert or Card ? This would be problematic in that you now have "derived" certificates that have no real bounding by that which was used for its derivation. If there is no bounding, then why even use derivation ? It is really PIV Authentication which authorizes the issuance of the Derived PIV Credential and that is it — no bounding is enforced at all.	The PIV Derived Authentication certificate shall expire no later than the date of expiration of the PIV Authentication certificate or expiration of the PIV Card.	Resolved by comment #107.
232	Apple Inc.	Shawn Geddis		15	545-552	3.3.2	This embedded Cryptographic Tokens section is extremely weak in defining what an acceptable "container" is. Other than the requirements in Section 3.2, there is no apparent possibility for certification of any HW implementation that is not one of those listed in the Non-Embedded section. There needs to be potential for a vendor to pursue and achieve certification for HW containers other than those listed as long as they have well-defined physical and logical interfaces. For SW Containers, there seemingly lacks any clarification in controls or interfaces required other than what is noted in Section 3.2.	Suggest allowing/qualifying Embedded implementations by what technology is used to communicate with it. For example, Non-Embedded allows for use of **Global Platform, ASSD**, **CCID/ICC**. If the embedded HW provides the same interface, then it should be allowed as well.	The cryptographic token interfaces are platform-specific and thus the use of a generic requirement allows different platforms to satisfy the generic requirement without imposing new / different interfaces/requirements. FIPS 140-2 will be levied for the security of the embedded module.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
233	Apple Inc.	Shawn Geddis		16	586-588	3.4.2	“…a password-based mechanism shall be used…”. Since it says “shall”, it is required. Why can’t additional mechanisms such as biometric unlock be allowed for software implementations ?	“For software implementations (LOA-3) of Derived PIV Credentials, any mechanism proving this is the authorized holder of the token shall be used. At a minimum, this shall be a password-based mechanism, but alternative mechanisms can be used."	Resolved by comment #13.
234	Apple Inc.	Shawn Geddis		16	590-591	3.4.2	Why can’t a SW Crypto module be allowed to perform a password reset ? The Subscriber should be allowed to use their PIV Card to “Authorize” the Password Reset on their SW Module.	For software cryptographic modules, password reset is supported if the PIV Subscriber successfully authenticates to the device using the original PIV Card & PIN. Otherwise, the initial issuance process shall be followed if the password is forgotten.	Resolved by comments #4 and #127
235	DHS	Mark Russell	G			General	800-157 provides limited guidance on the actual expected use of the credential. Is it envisioned that derived credentials would be used each time the user unlocks the screen, as in the desktop world? Or would screen unlock continue to use either native or MDM-provided PIN/password unlock capabilities, and PKI credentials be used when connecting to back-end systems? 800-157 may not be the venue, but guidance on expectations for authentication on mobile devices would be very helpful. There are several considerations that are unique to mobile, or more important in mobile use cases than on the desktop, including the need to support disconnected use of the device, the difficulty of entering complex passwords on virtual keyboards, the frequency with which devices will need to be unlocked, etc.	More general guidance is needed on mobile authentication requirements.	Declined. Section 1.2 of Draft SP 800-157 states that “The scope of the Derived PIV Credential is to provide PIV-enabled authentication services on the mobile device to authenticate the credential holder to remote systems.” So, unlocking the screen would be out of scope as would be disconnected use of the device.
236	DHS	Greg Powell	G	iv	208	Executive Summary	“This publication specifies use of an additional common identity credential, a PIV Derived Credential, which may be used where the use of a PIV Card is not practical”. Can this reference and the subsequent references in the document to “ … implementing and deploying PIV Derived Credentials to mobile information technology (IT) platforms (such as smart phones and tablets) … “ be expanded (on an exception basis only) to include for example other types of mobile computers such as laptops and notebooks with TPM, USB, or other secure element integration for Derived Credentials? For “covert operator/under cover agent” use cases (e.g., federal air marshals, border patrol agents, and other special agents) that could use the Derived Credential as the “alternative identifier” for laptop network authentication when operating under cover vice displaying and using the government issued PIV Card for network authentication.	Consider expanding the scope of use cases for derived credentials to accommodate this type of scenario.	Resolved by comment #41.
237	DHS	Paul Grassi	E	5	247	1.1	Expense is not an advantage to using a PIV card contact with a mobile device, as the management of sleds has a cost	Remove 'expense'	Declined. The text in SP 800-157 doesn't say which is cheaper, it merely says you don't have issue new credentials in the PIV card case.
238	DHS	Matt Ambs	T	9	345	2.1	The re-check of revocation status should happen sooner (e.g., 3 days).	Change 7 days to 3 days	Resolved by comment #150.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
239	DHS	Levi Stamper	E	9	346	2.1	The re-check of revocation status does not actually protect against the use of a compromised PIV credential to obtain a derived credential, but rather simply allows detection after the fact.	Re-word to indicate that this is a detective and not preventive measure.	Resolved by changing the sentence to: "The revocation status of the Applicant's PIV Authentication certificate should be rechecked seven (7) calendar days following issuance of the Derived PIV Credential – this step can detect the use of a compromised PIV Card to obtain a Derived PIV Credential"
240	DHS	Mark Russell	T	9	345	2.1	For organizations that issue both PIV credentials and derived credentials, it would be much more effective to check for any derived credentials and take appropriate action as soon as a PIV credential is reported lost or stolen, rather than waiting for the 7 days to pass. With such a process in place, the 7-day re-check would seem to add administrative overhead without much value. I suppose the delayed re-checking makes sense in cases where a different agency issues the derived credential that the one that issued the original PIV credential. Should there be a requirement for agencies to inform the PIV issuer when a derived credential is created based on their PIV credentials? This would allow for immediate notification of changes in the status of the PIV credential.	Instead of prescribing a 7-day (or any set interval) re-check of revocation status, maybe just lay out a basic requirement (e.g., ability to identify derived credentials that are issued based on lost/stolen PIV cards) through a post-issuance confirmation process.	Resolved by comment #150.
241	DHS	Paul Grassi	T	9	347	2.1	In conflict with M-11-11. I would say for all LOA's, provided privacy controls are included in the use of the DC for L2 and lower. In fact, L2 or L1 credentials should be derived from a PIV.		Declined. Section 1.2 of Draft SP 800-157 states: "While the PIV Card may be used as the basis for issuing other types of derived credentials, the issuance of these other credentials is outside the scope of this document. Only derived credentials issued in accordance with this document are considered to be Derived PIV credentials." So, LOA-1 and LOA-2 credentials may be derived from a PIV Card, but the resulting credentials would not be considered to be Derived PIV credentials.
242	DHS	Paul Grassi	T	9	355	2.1	Can we get away with doing remote issuance of the L4 DC? Especially since the PIV was issued in-person. Isn't that the point?		Resolved by comment #27.
243	DHS	Matt Ambs	T	9	359-360	2.1	What is the rationale for retaining the biometric sample used to enroll for the derived credential? In cases where the same agency issues the PIV card and the derived credential, we would already be in possession of the biometric template.	Reconsider the need to collect a new biometric sample.	The requirement is derived from the common policy and it provides an audit trail for dispute resolution.
244	DHS	Levi Stamper	E	10-11		2.3, 2.4	Terminology and implications of a "terminated PIV card" vs. "revoked PIV Authentication Certificate" must be clarified. The implications of these two conditions in conjunction with derived credential lifecycle management is ambiguous.		NIST (157) Resolved by revision to Section 2.4 and the inclusion of a lifecycle section in 2.1. Section 2.3 also discusses the revocation relationship between the PIV Card and the Derived PIV Token
245	DHS	ICE	T	11		2.4	While linkage between the PIV and derived credential is discussed, there should also be a common linkage between both certificates and a user account in directory services.		Noted. This is an implementation detail that is out of scope of the technical specification for Derived PIV Credential. Note: The FICAM LAWG might be the place to further discuss and detail this.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
246	DHS	Levi Stamper	T	12		3.2	Suggest that certificate profiles corresponding to id-fpki-common-pivAuth-derived-hardware, id-fpki-common-pivAuth-derived, support attributes tying derived certificates to corresponding PIV-AUTH certificates without relying on external data sources such as BAE, IDMS, etc.		Declined. The external data sources are used in order to keep track of whether the Subscriber continues to be eligible to have a PIV Card. Including attributes in a Derived PIV Authentication certificate that tied it to the PIV Authentication certificate that happened to be current at the time the PIV Derived Authentication certificate was issued would do nothing to support this.
247	DHS	Mark Russell	T	15	557	3.4.1	The NISTIR specifically addresses devices that use hardware to protect keys in storage along with software cryptographic modules, including devices that use a Trusted Execution Environment (TEE) for private key storage. The NISTIR classes these solutions as "hybrid" (part hardware, part software) solutions. It would be helpful to discuss these solutions in 800-157, as there has been some confusion as to whether these would be deemed hardware or software tokens. Our impression is that they are software tokens and hence only good for LOA3.	Mention "hybrid" solutions in the 800-157 draft and explain whether they would be considered hardware or software tokens for LOA purposes.	Resolved by comment #204. See also resolution to comment # 111.
248	DHS	Mark Russell	T	16	588	3.4.2	Requiring an LOA-2 password to unlock a software PKI credential detracts from the user experience while adding little practical benefit. If the private key is removed from the device, an adversary has unlimited time to perform brute-force attacks (potentially many simultaneous attacks in parallel). Whether a PIN or password is used would seem to have minimal impact on the success of the attack; but it would have significant impact on the usability of the solution.	Consider allowing PIN authentication to activate a software credential.	NIST (157) Resolved by comment #147.
249	DHS	Mark Russell	T	18	622	B.1	The PIV-Derived Application specification is only required for removable hardware tokens. Why should this requirement not extend to embedded cryptographic tokens? While embedded tokens can't be moved from one device to another, they will still rely on compatible software implementations to use credentials on these tokens. Requiring embedded tokens to also use this interface would enable more software solutions to work with a wider range of tokens.	Consider making the PIV Derived Applet specification mandatory for both embedded and removable hardware tokens.	Declined. The specifications for removable hardware tokens are relevant to interoperability at the device driver level. The software interfaces that applications use will tend to be operating system specific.
250	DHS	Mark Russell	G	18	628	B.1	"the contactless interface is not supported by the PIV derived application" - there is significant interest at DHS in solutions that would use the wireless capabilities of mobile devices for workstation login and PACS access. The NISTIR mentions that one "could imagine" such a thing but must proceed cautiously, but there is no mention in 800-157 of this type of use case, except this clause her that the derived PIV applet has no contactless interface. An opportunity is being missed here to take advantage of the full capabilities of mobile device as access tokens.		NIST (157) Resolved by comment #15

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
251	Emergent LLC	Various ,POC : Venkat Sundaram			217-218	Executive	Limiting a derived credential to a PKI credential limits the number of devices that the Government can use Out of the box. Most popular operating systems including ioS and versions of Android do not have the capability to have a secure container for the PKI credential. The proposed standard loosely revolves around Micro SD cards, NFC & Bluetooth which are not a standard capability, open to man in the middle attacks and often pose usablity issues such as interference and battery drain. Additionally, we recommend that the authentication required on mobile devices include a trusted attribute as an anchor and a device certificate, not a end user certificate. To expand the scope of derived credentials, we request that a derived credential be defined as a " Credential issued based on a the validity of a PIV card". The interoperability mentioned works to the advantage of PKI providers and not mobile device solutions available in the market place today. This definition would put undue burden on the Government in cost and usability of mobile solutions available in the market place today.	Suggestion to expand the scope of a “derived credential to be a Credential that is based on a PIV issued credential”; whose interoperability is based on the validity of the PIV PKI credential. The definition proposed is Derived credentials are based on the validity of a PIV credential - not limited to a PKI credential implanted on a device.	Declined. OMB Memorandum M-11-11 states that “Agency processes must accept and electronically verify PIV credentials issued by other federal agencies.” Allowing the Derived PIV Credential to be something other than a PKI credential would either make this impossible or would put an undue burden on agencies that would have to be able to “accept and electronically verify” all of the different types of Derived PIV Credentials issued by other agencies.
252	Emergent LLC	Various ,POC : Venkat Sundaram			232-237	1.1	Cryptographic modules within commercial operating systems and its certified version for each release is not a feasible model. A certified cryptographic module can fit a certain form factor and OS version, however the adoption and development of mobile devices far exceeds the rate at which certifications is possible. OS vendors are trying to beat their release schedules , Android for instance has repeatedly beat their time-line expectations. Reliance on cryptographic modules to store private keys is going to put undue burden on the federal government, it will limit the number of devices or OS instances it can use. Many commercial form factors and manufactures do not have this in their product road map and will prove to be expensive to implement and enforce. This supports the background (section 1.1) and the overall sentiment of the ability to use PIV cards with mobile devices. Risk based Multi factor authentication dependent on USER ATTRIBUTES within a PIV must be an option the Government should consider. Our recommendation is to have multiple attributes that exist today to make a risk based decision for authintication - the attributes are bound to a users PIV.	Requesting update to " PKI language'. In response to the growing use of mobile devices within the federal Government, FIPS 201 was revised to permit the issuance of additional, derived PIV credentials, BASED ON THE USERS PIV CREDENTIAL, SP 800-157 PROVIDES PROVISIONS FOR ESTABLISHING A TRUST ANCHOR WITHIN THE USERS MOBILE DEVICE, THAT CAN BE USED FOR AUTHENTICATION WITH A HIGHER LEVEL OF ASSURANCE THROUGH PIV CERTIFICATE ATTRIBUTES, achieving substantial cost savings by leveraging the identity-proofing results that were already performed to issue PIV cards.	Declined. The scope of the document is HSPD-12/FIPS 201 with a mandate for 'common identification' across USG. As the PIV card has established PKI for logical access, the Derived PIV Credential leverages the same PKI infrastructure. Departments and agencies are free to leverage other technologies when HSPD-12/FIPS 201 (common identification across USG and OMB M-11-11) does not apply.
253	Emergent LLC	Various ,POC : Venkat Sundaram			245	1.1	This credential can validate user, the device and provide an infrastructure for attribute exchange within mobile application. This we believe will facilitate higher use, better interoperability at a lower cost ; with the added benefit of commercial software and hardware devices. This supports the following paragraph Line 246-253 & 254. The identity ecosystem is capable of securing credentials for all federal users with the ability to provision an their identity on a cloud based infrastructure following guidelines for issuance of a Derived PIV.	Request to add NSTIC & FCCX guidelines and best practices for management and use of the identity ecosystem.	Noted. The use of PKI as the basis of the Derived PIV Credential does not preclude its adoption and use in NSTIC pilots or adoption and use in cloud based federations such as FCCX. See also resolution to comment #252.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
254	Emergent LLC	Various ,POC : Venkat Sundaram			256	1.1	Over the air authentication wiill allow for one time passwords, knowledge based question and answers , advanced attribute exchanges, federation and cross domain single sign-on ; all on mobile devices, without the need for cryptographic containers carrying user credentials.	Request Addition " Or Over the air authintication" for cloud IDP's that provision users based on the PIV attributes.	Resolved by comments #251, #252, and #253.
255	Emergent LLC	Various ,POC : Venkat Sundaram			347-348	2.1	The trust anchor provides for additional authentication possibilities and use of additional commercial devices - providing Just in time access to resources with multi factor authentication. Eg: - An adjudicated user with a PIV can enroll for a derived credential by providing device attributes such as SIM attributes, Device IMIE, OS Status, Device serial number etc. These attributes are bound with the PIV validity (crl etc) and provisioned for access through a multi factor authentication infrastructure based on the user's organizational affiliation. This credential is derived from PIV but does not require crypt containers, MicroSD Cards slots , blue tooth capabilities or NFC functionalities. This simple implementation will allow the Government to use commercial technology securely , leverages existing infrastructure and provides for a simple - easy to use mobile infrastructure.	The credential resides on a hardware, software OR TRUST ANCHOR ON THE DEVICE WITH A BINDING TO PIV CREDENTIAL as a security token as illustrated in Table C-1.	Resolved by comments #251, #252, and #253.
256	Emergent LLC	Various ,POC : Venkat Sundaram			278-280	1.2	Additional requirements as suggested for Derived PIV. Recognizing that Mobile devices and its use within the federal government is an emerging domain, the specifications laid out will continue to evolve. Federal and commercial initiatives through NSTIC has evolved pilots like FCCX, are well positioned to promote the use of derived credentials and non-pki based single sign-on and attribute exchange infrastructure that can very-well support the use of derived credentials without the need for device bound technology to secure PKI certificates.	Request addition : Non PKI based derived credentials will enable authentication. Security controls will be consistent with Special Publication 800-53 Revision 4 AND further work in the areas of Situations Requiring Potential Baseline Supplementation (Page 37 , sp 800-53) & Security controls Incorporated into MP-7 within SP 800-53 R4.	Resolved by comments #251, #252, and #253.
257	Emergent LLC	Various ,POC : Venkat Sundaram			286-289	1.2	Additional requirements as suggested for Derived PIV.	Request addition : The derived credential is PIV derived authentication certificate or a credential provisioned based on the possession of a PIV credential. (In addition to COMMON)	Resolved by comments #251, #252, and #253.
258	Emergent LLC	Various ,POC : Venkat Sundaram			298	1.2	Additional requirements as suggested for Derived PIV.	Addition : FICAM Certified Non PKI baesd cloud IDP/SSO (currently in Pilot with USPS /FCCX) can be used in absence of PKI provisioned to a mobile device.	Resolved by comments #251, #252, and #253.
259	Emergent LLC	Various ,POC : Venkat Sundaram			346	2.1	This will enable use of Non PKI based derived credenials in mobile devices, since the recommendation that (Line 291 - 292) - Only derived credentials issued in accordance with this document are considered to be Derived PIV credentials Addition , Line 458, SECTION 3.2 : Trust anchor based multi factor authentication does not require storage of private keys on mobile devices. The authentication is performed with the multi factor authentication binding with user's organizational attributes on the PIV issued certificates.	Addition : The Non PKI derived crdential should be validated for each session with a out of band PIN or knowledge based question and answers actively and passively through means of known attributes on users mobile device sich as IMIE Number, OS Status, GeoLocation, Trust anchor and users PIV status following FIPS 201 guidelines. (for LOA 1,2 & 3)	Resolved by comments #251, #252, and #253.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
260	Emergent LLC	Various ,POC : Venkat Sundaram			273	1.2	Request addition to add other checks for higher assurance. Additionally implementation and usage of derived credentials in a seamless manner across multiple form-factors and operating system platforms can be facilitaed witih a standard middleware platform.	Mobile Management solutions will be used to enforce the integrity of the device trust anchor bound to the mobile identity provider. Any tampering of the device or credential will de-provision the device, user and revoke access.	Resolved by comments #251, #252, and #253.
261	Emergent LLC	Various ,POC : Venkat Sundaram			Add new section 3.3.3.3	3.3.1.3	The authentication in this case is done consistently , following NSTIC and FCCX principles , architecture guidelines, framework, protocols and attribute definitions. The trust anchor based authentication for mobile devices will be based on a trusted identity provider , where identities are created based on the existing PIV relationship.	Trust Anchor Based Multi Factor Authentication. Users PIV credentials as a trust anchor can be used to deploy a multi factor authentication token , software token or mobile device management device controller to a device. Controls to verify integrity of the device and the agent can be enforced with COTS today that can enable use of commercial mobile devices in a secure manner, consistent with the definition of derived credentials. This allows for use of devices that otherwise will not have provisions for a cryptographic container to secure the PKI certificates.	Resolved by comments #251, #252, and #253.
262	G&D	A.Summerer	G	9	356	2.1	The following sentence requires that an applicant has to be idenfied by biometrics for each transactions: "If there are two or more transactions during the issuance process, the Applicant shall identity himself/herself using a biometric sample..."	Under the assumption that the last transaction of issuance process is the download of the derived credential to the mobile device (in a server connection initiated by a mobile device application). How shall the applicant identify himself/herself with biometrics on the mobile device in order to download the credential? Potentially mobile devices with fingerprint reader could be used. However, does it mean that LOA4 derived PIV credentials can only be downloaded with those devices?	Noted. At LOA-4 all steps in the issuance process must be performed in person, so any biometric sample that needs to be collected would be collected using a biometric reader under the control of the issuer, not a biometric reader on the mobile device. This requirement only applies, however, for the process of issuing the credential. There is no requirement that a biometric comparison be performed before the credential (which is a public-key certificate) is loaded onto the device.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
263	Intercede	Andy Atyeo, Ben Arnold		9	349	2.1	The statement that "A LOA-3 Derived PIV Credential may be issued remotely or in person *in accordance* with SP800-63"/An LOA-4 ...shall be issued in person *in accordance* with SP-800-63." is making me wonder: (1) Is the intent to indicate that (as sp800-63 indicates) a LOA-3 derived credential can be issued remotely or in person, and a LOA-4 derived credential can be issued only in person. Or (2) Is the intent to direct the reader of sp800-157 to sp800-63-2 Table 2, which introduces requirements over and above what is specified in sp800-157 for the issuance of LOA3/LOA4 derived credentials? For example, reading sp800-157 in isolation, issuance of the LOA3 derived credential requires the PKI-AUTH check to demonstrate possession and control of the PIV credential, but sp800-63-2 Table 2 (page 34) also indicates additional requirement : "RA inspects photo ID / RA verifies info provided including ID number/account number... checks DoB ... checks ID number and account number conforms to name and address of applicant ... confirms ability of applicant to receive mail". I believe the intent is that sp800-157 is stating the requirements (e.g. PKI-AUTH check for LOA3) and this over-rides what is stated in sp800-63-2, in which case rewording the sentence with 'in accordance' might help clear this up. If however the intent is that all additional requirements of sp800-63-2 should also be met then it should be reworded to make that more obvious.	*As required by sp800-63* , a LOA-3 Derived PIV Credential may be issued remotely or in person. in accordance with SP800-63 / *As required by sp800-63* an LOA-4 ...shall be issued in only in person. in accordance with SP800-63 .	Declined. Draft SP 800-157 is not overriding the requirements of SP 800-63-2. Table 3 in Section 5.3.1 of SP 800-63-2 specifies identity proofing requirements. However, the final paragraph of Section 5.3.1 states that "If a valid credential has already been issued, the CSP may issue another credential of equivalent or lower assurance. In this case, proof of possession and control of the original token may be substituted for repeating the identity proofing steps. (This is a special case of a derived credential. See Section 5.3.5 for procedures when the derived credential is issued by a different CSP.)" SP 800-157 is following this procedure for derived credentials of substituting proof of possession of the PIV Card for repeating the identity proofing steps (from Table 3).
264	Intercede	Andy Atyeo		16	592	3.4.2	sp800-157 states "…for software LOA3: ...Lockout mechanisms for repeated unsuccessful activation attempts are not required for software cryptographic modules.". Sp800-63-2 table 6 discusses password requirements for tokens, and discusses 'throttling' (referring to prevention of too many password submissions within a time period), rather than 'lockout' (disabling of a credential due to too many incorrect attempts.) Therefore the question is : whether lockout and throttling are not required for software LOA3, or whether lockout is not required but throttling is required for software LOA3. I believe the intend is to not require lockout or throttling but this is not clear to me.	Depending on intent either "Lockout **and throttling** mechanisms for repeated unsuccessful activation attempts are not required for software cryptographic modules." …or… "Lockout mechanisms for repeated unsuccessful activation attempts are not required for software cryptographic modules, **but a throttling mechanism as identified in sp800-63-2 is required.**"	Resolved by comments #4 and #127
265	Intercede	Chris Edwards		13	475	3.3.1	In the list of removeable hardware cryptographic tokens, there is no mention of bluetooth connected secure-elements (secure elements that might exist outside of the mobile, inserted into a bluetooth connected cardreader, connecting to the mobile. This is one of the few secure element types available today with FIPS140-2 accreditation, so therefore an attractive option for deployment in the near future). Are these permitted for (LOA4) derived credentials?		Resolved by resolution of comment #56 and 193.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
266	Intercede	Chris Edwards		10	386	2.2	386 states that PIV derived credential is unaffected by revocation of original PIV auth cert. However we know from 345 that revocation status of PIV auth cert must be checked 7 days after issuance of the derived credential. So the intent of 386 is to indicate that *after the initial 7 day check* , revocation of original PIV auth will cause the derived credential to be revoked.	Similarly, the Derived PIV 385 Credential is unaffected by the revocation of the PIV Authentication certificate ...**unless the revocation takes place within 7 days of the derived credential being issued**	Resolved by comment #197.
267	Intercede	Chris Edwards		10	419	2.4	417 describes how there will be a linkage between the derived credential issuer and the original PIV issuing agencies IDMS. In many cases there will be a separate IDMS and CMS (Card Management System) - where the IDMS is effectively a backend enrollment system/user database, which communicates with a seperate CMS (Card Management System) system to facilitate the management of PIV credentials. As such there are some cases where it is more appropriate for the linkage to be between the derived credential issuing system and the CMS that issued the original PIV card. Therefore the linkage should be allowed to either the IDMS or the CMS, in order to accomodate different setups that different agencies use.	If the Derived PIV Credential is issued by the same agency that issued the Subscriber's PIV Card, the linkage between the two credentials may be maintained through the common Identity Management System (IDMS) or **Card Management System (CMS)** database implemented by the issuing agency.	Noted. This text depicts an example of how the linkage could be maintained between the termination status of the PIV Card and the Derived PIV Credential. There are multiple possible solutions.
268	Intercede	Chris Edwards, Ben Arnold		15	575	3.4.1	360 indicates that when issuing a LOA4 derived PIV credential, a biometric shall be collected and retained for future reference to validate the applicant. Biometric validation of the applicant is required for multi-stage issuance (to verify it is the same person), and also for a future LOA4 unlock. It is unclear why the choice is made to enforce that the biometric captured from the subscriber at the point of issuing the derived credential should be stored for future reuse (e.g. during the unlock described in 575.) This seems to have some negative consequences - it means only a single biometric is available, and it also means that the quality of the retained biometric sample is determined by the biometric captured during the issuance of the derived credential, which may be inferior to the biometrics enrolled for the PIV card. Rather than limiting the derived credential issuing system to using the biometric captured for verification purposes during the issuance of the derived credential it would be beneficial to allow the derived credential issuing system the ability to keep the biometrics read from the PIV card, or if the issuing system of the derived credential is the same as the issuing system of the original PIV card, the original enrolled biometrics.	A 1:1 biometric match shall be performed against **either** the biometric sample retained during 575 initial issuance of the Derived PIV Credential, **or the biometric samples from the original PIV card, or the biometric samples from the enrolment system that issued the PIV card.**	Accept by amending the affected text.
269	AF PKI SPO	Mr. Kit Howell	S	6	280	1.2	LOA 4 not yet available, (the infrastructure) has not met requirements for LOA 4. Coordinator Justification: validity and clarity		Declined. LOA-4 credentials are currently available. The PIV Authentication certificates on PIV Card are LOA-4 credentials, and Derived PIV Credentials will use the same infrastructure as PIV Authentication certificates use.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
270	AF PKI SPO	Mr. Ling Lock	S	7	287	1.2	In the sentence, “The Derived PIV Credential is a PIV Derived Authentication Certificate” is the term, PIV Derived Authentication Certificate a name or a description? Coordinator Justification: clarity		Resolved by comment #346. The full sentence states: “The Derived PIV Credential is a PIV Derived Authentication certificate, which is an X.509 public key certificate that has been issued in accordance with the requirements of this document and the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework [COMMON].” So the referenced sentence already includes additional text clarifying what a PIV Derived Authentication certificate is.
271	AF PKI SPO	Mr. Ling Lock	S	7	291	1.2	Clarify if there is only one type of derived credential (derived signature, derived encryption, etc…) Coordinator Justification: clarity		Resolved by comments #270, and #5.
272	AF PKI SPO	Mr. Kit Howell	S	9	347	2.1	LOA 4 not yet available Coordinator Justification: validity and clarity		Resolved by comment #269.
273	AF PKI SPO	Mr. Kit Howell	S	9	356	2.1	Coordinator Comment: It is unclear what is meant by biometric sample. Coordinator Justification: clarity		Noted. The Biometrics Glossary (http://biometrics.gov/Documents/Glossary.pdf) defines biometric sample as follows: “Information or computer data obtained from a biometric sensor device. Examples are images of a face or fingerprint.”
274	AF PKI SPO	Mr. Kit Howell	S	9	367	2.1	Coordinator Comment: “Re-key” should not be permitted. All derived credentials should be reissued based on the PIV certificate. Coordinator Justification: validity		Declined. The Common Policy states that “Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject.” The term “reissue” does not appear in the Common Policy. A PIV Card may be reissued, but this term does not apply to certificates.
275	AF PKI SPO	Mr. Kit Howell	C	10	378	2.2	Coordinator Comment: “re-key” does not work. This would effectively make the derived credential equal to the original PIV. Coordinator Justification: validity		Resolved by Comment #274.
276	AF PKI SPO	Mr. Ling Lock	C	7	379-386	1.2	Coordinator Comment: Apparent conflict. If the PIV card is lost or compromised, the derived certificate should also be revoked. Coordinator Justification: validity		Resolved by comment #178.
277	AF PKI SPO	Mr. Kit Howell	S	10	401	2.3	Coordinator Comment: Change sentence, “In all other cases, termination….” to “Termination always requires revocation of the PIV Derived Authentication certificate.” Coordinator Justification: clarity		Declined. As with the PIV Authentication certificate, if the PIV Derived Authentication private key has been zeroized or the token in which the key is stored has been destroyed, and there are no other copies of the key, then the key can no longer be used to authenticate to a remote system and so revocation of the certificate is not necessary.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
278	AF PKI SPO	Mr. Kit Howell	C	11	430-432	2.4	Coordinator Comment: Re-write this sentence. There will be no linkage between the existing derived credential and the new PIV card. A new derived certificate must be issued based on the new PIV card. Coordinator Justification: validity and clarity		Declined. There is no requirement to issue a new PIV Derived Authentication certificate whenever a new PIV Card is issued. The PIV Card is used to identify the Applicant for a Derived PIV Credential as an alternative to repeating the identity proofing steps that were performed when the PIV Card was issued, but the Derived PIV Credential is not “based on” the particular PIV Card that was used to perform the identity proofing.
279	AF PKI SPO	Mr. Kit Howell	C	12	444-446	3.1	Coordinator Comment: the derived certificate and the source certificate on the PIV card should be tied together. If one is revoked, the other should also be revoked.		Resolved by comments #178 and #278.
280	AF PKI SPO	Mr. Kit Howell	C	12	445	3.1	Coordinator Comment: Change, “need not” to “must”. Coordinator Justification: the derived credential should be linked to the valid PIV Card.		Resolved by comments #178 and #278.
281	AF PKI SPO	Mr. Kit Howell	S	12	451-455	3.2	Coordinator Comment: Indicate in the paragraph this description is equivalent to LOA 4. Coordinator Justification: clarity		Accept.
282	AF PKI SPO	Mr. Kit Howell	S	12	456-458	3.2	Coordinator Comment: Indicate in the paragraph this description is equivalent to LOA 3. Coordinator Justification: clarity		Accept.
283	Not applicable	Sam Wilke		16	562	3.4.1	Regarding mininum PIN length of six bytes, is there a recommended maximum?	Recommend maximum PIN length or include reference to relevant SP/IR regarding PIN use.	Declined. For removable hardware cryptographic modules the maximum password length is 8 bytes by reference to the VERIFY command in Appendix B.2. For embedded hardware cryptographic modules, there is no reason to specify a maximum password length.
284	Not applicable	Sam Wilke		9	359, 360	2.1	With reference to: "The issuer shall retain for future reference the biometric sample used to validate the Applicant." Is it prudent to include a reference to authority on retaining biometric information? Would this hold true with more complex biometric samples in the future?	Include footnote to reference regarding biometric sample oversight, management, retention, etc.	Resolved by resolution to comments #171 and #243.
285	Secure Access Technologies	Aaron Ashfield		5	254	1.1	This section did not discuss the followings: 2FA Soft Tokens that use (Internet) to communicate with the data terminal were not discussed as part of new technologies. iBeacon LE Soft Tokens. iBeacon LE Hard Tokens. RE: iBeacon / Bluetooth LE / Bluetooth Low Energy: This technology is different from Bluetooth 2.0 and is available on ALL major-brand mobile devices today. It can be set to provide all security functions of NFC on new iOS/Android and BB devices without any extra hardware.	2FA Soft Tokens (internet comm.), 2FA Bluetooth LE Tokens and BT LE Hard Tokens are commercially available today, and offer a low cost replacement for PIV cards.	Resolved by comment #56.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
286	Secure Access Technologies	Aaron Ashfield		6	281	1.2	The current figure1-1 illustrates a user putting the PIV Certificate on a mobile device, and gaining access to a portal using that mobile device and a password. 1- From a security perspective, anybody that gets the password can walk to the user device and have access to data. Moreover, a device left un-attended with an open session provides direct access to data. Finally, this architecture will encourage device snatching (while a user is logged) and blackmail, and will create a culture of fear 2- From a user experience, we will have users that type complex passwords everytime a mobile device locks... 20-50 times a day... While people have a bad user experience, these passwords cannot provide the same security as passwords on PCs. Password sharing, password camera recording, etc. become a problem Figure1-1 implies that 2FA is not important, and that it can be replaced with MDM or a certificate on the device. One industry players are talking about putting PIV-Cert in the cloud. Please note that whille 2FA is a Security Standard, MDM is a Management Standard with reduced security functions such as a) enforcing passwords which causes password problems b) remote wipe which is not reliable. Secure Access Technologies Inc. is very worried about this	The figure needs to be updated with a data terminal that is physically separate from the mobile device carrying the Derived PIV Credentials.	Resolved by comment #57.
287	NorkaTech	Sarra Harty		6	281	1.2	We are very concerned about this draft proposal that removes 2FA security and replaces it with a PIV certificate on the device. A certificate on a Mobile device provides minimal security and forces users to type passwords too often, thus the password becomes the weakest link... This draft would unfairly put two-factor and multi-factor authentication companies at an economic disadvantage as they will loose business with the government. This draft would give and unfair advantage to MDM companies with inferior security and higher costs to do business with the government.	Add a Terminal (PC or tablet) physically separate from the Mobile Device (with Derived PIV) to connect to the website or portal	Declined. Draft SP 800-157 does not remove two-factor authentication security. Even the LOA-3 embedded software credential provides two-factor authentication as it is a “Multi-factor (MF) Software Cryptographic Token” as defined in SP 800-63-2. The scope of SP 800-157 is “is to provide PIV-enabled authentication services on the mobile device to authenticate the credential holder to remote system.” SP 800-157 does not address mobile device management.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
288	NorkaTech	Sarra Harty		12	459	3.3	This section is missing information about Bluetooth proximity tokens (iBeacon) that provide similar function to NFC and more, and that is available on most mobile devices.	Add section: Proximity Tokens Description: Proximity tokens are either a) hardware Bluetooth LE tokens that store the keys or b) Soft tokens that store the keys in a keychain or SE, and on a devices physically separate from the data terminal. To break this security, one must have the data terminal device, the proximity token device and the user PIN. This is equivalent to PIV security where an attacker must obtain the data terminal, the PIV card and the user PIN. Proximity tokens are always physically separate from the data terminal, act as a second factor and also act as a proximity monitor. Communication with the data terminal is through encrypted communication over the Bluetooth LE channel. Availability: High: All major mobile platforms support Bluetooth LE Benefits: Always on device. User does not do any action except keep the proximity token in the pocket. Proximity security locks data and alarms when left unattended	Resolved by resolution of comment #56.
289	NorkaTech	Sarra Harty		23	789	Appendix B-B2	PIV Derived Authentication Certificate: Add a row: Token Type=Proximity Token Assurance Level=Very High	PIV Derived Authentication Certificate: Add a row: Proximity Token: Very High	Resolved by comment #56.
290	Security Architects	Alfonso Mendes		6	281	Figure	There are concerns about: 1- Password-Based security on mobile devices: What guarantees that the person is not an attacker? 2- Removing PIV cards security and reducing security to a mere Password (and a certificate on the device) while attacks are increasing in sophistication: Heartbleed, Snowden, device snatcing... 3- Increased device snatching, session attacks and physical attacks. We need some studies to evaluate the risk.	Enforce 2FA	Resolved by comment #287.
291	ICAMSC		T	N/A	N/A	General	SP 800-157 allows for storage and use of credentials on a large variety of mobile and non-mobile platforms. Yet it relies on the credential containers defined in SP 800-63-2, which were last updated in 2011 in SP 800-63-1. SP 800-157 does not reevaluate these containers when utilized in a different risk environment (introduced by use of mobile devices and by changes in security environment and attacks in the last 3 years) as would be expected per OMB-04-04.	Particularly, the appropriateness of utilization of MF software cryptographic tokens for storing PIV derived credentials should be addressed in SP 800-157 or by accompanying guidance. A detailed issue analysis has been generated and is available in a separate technical analysis write-up. Suggest a technical discussion with the authors of SP 800-157 and for GSA to develop the best practices guidance for implementation.	Resolved by comment #111. The PIV team had a technical discussion with GSA about this comment.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
292	ICAMSC		T	N/A	N/A	General	Under certain configurations allowed by SP 800-157, derived PIV credentials can be created without authorization of the subscriber. For example, malware on a PIV-enabled laptop can capture the PIV PIN using a keylogger and then covertly initiate a derivation process.	SP 800-157 or accompanying guidance should address the issue of verifying intent. Suggest a technical discussion with the authors of SP 800-157 and for GSA to develop the best practices guidance for implementation.	Verifying intent is addressed in SP 800-79-2 with issuer control # SP (DC)-1 for Derived PIV Credentials.
293	ICAMSC		T	N/A	N/A	General	The increase in the number of credentials held by the individual may lead to insider risk since a subscriber can now share a credential without exposing that he/she has given it away.	SP 800-157 or the accompanying guidance should address how the association of multiple credentials with the same individual should be communicated to the relying party in addition to the verifier. Suggest a technical discussion with the authors of SP 800-157 and for GSA to develop the best practices guidance for implementation. A detailed issue analysis has also been generated and is available in a separate technical analysis write-up.	Noted. Technical discussion was conducted with GSA.
294	ICAMSC		T	N/A	N/A	General	Details of the entire derived PIV credential lifecycle should be expanded upon in SP 800-157 or the accompanying guidance. It should address issues of revocation of the associated key management key and communication between the derived PIV credential CSP and the PIV card CSP.	Suggest a technical discussion with the authors of SP 800-157 and for GSA to develop the best practices guidance for implementation. A detailed issue analysis has also been generated and is available in a separate technical analysis write-up.	Noted. Technical discussion was conducted with GSA.
295	ICAMSC		T	N/A	N/A	General	Additional considerations.	A detailed issue analysis has been generated and is available in a separate technical analysis write-up. Suggest a technical discussion with the authors of SP 800-157 and for GSA to develop the best practices guidance for implementation.	Resolved by resolution of comment # 293.
296	ICAMSC		E	2nd cover	46	General	This page lists William Burr with Dakota Consulting and on line 133 William Burr is listed as being part of NIST.	Accurately and consistently list William Burr's affiliation.	Resolved by changing William Burr's affiliation to Dakota Consulting, Inc. on line 133 (line 135 in final document).
297	ICAMSC		E	iii	168	Table of Content	The spacing between each word on line 168 does not match the formatting of the Table of Contents. The test on line 168 reads as follows: "Appendix B - Data Model and Interfaces for Removable (Non-Embedded) Hardware Cryptographic Tokens (normative)."	Please update the spacing between each word on line 168.	Accept.
298	ICAMSC		G	iv	200 - 210	Executive Summary	The text in the Executive Summary provides great information about how mobile devices lack integrated smart card readers, but it will be beneficial if the publication also identifies and discusses the core usability issues that has led to the need for Derived PIV Credentials.	Please add language about the evolution of PIV credential usage and the core usability issue with the use of PIV Cards, similar to the language in the Introduction section of Draft NIST IR 7981, lines 139 - 148.	Noted. The language in Draft NIST IR 7981 is closely aligned with the text in line 200 -210 of Draft SP 800-157.
299	ICAMSC		G	iv	207 - 208	Executive Summary	It is unclear which cases are considered to be impractical for use of the PIV Card, in the following sentence: "SP 800-157 does not address use of the PIV Card with mobile devices, but instead provides an alternative to the PIV Card in cases in which it would be impractical to use the PIV Card."	Please add clarification language and/or provide examples that agencies can leverage when determining if the use of a PIV Card is impractical.	Resolved by comment #41.
300	ICAMSC		E	iv	213	Executive Summary	Text that reads "of derived credential."	Please update to either "of a derived credential" or "of derived credentials."	Accept.
301	ICAMSC		E	5	259	1.1	Text that reads "contactless antenna."	Please update to either "contactless interface" like on line 261 or "contactless interface antenna" (preferred).	Accept.
302	ICAMSC		E	6	279	1.2	Text that reads "PKI based."	Please update to "PKI-based."	Accept.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
303	ICAMSC		G	7	306 - 322	1.4	"Normative" and "Informative" are not defined. If certain sections of this publication are mandatory for compliance, then additional language may be beneficial.	Please define "Normative" and "Informative" in this publication. For example, language similar to what is provided in SP 800-73-4: "All sections in this document are normative (i.e., mandatory for compliance) unless specified as informative (i.e., non-mandatory)."	Accept
304	ICAMSC		T	9	344	2.1	Sentence reads, "The revocation status of the Applicant's PIV Authentication certificate shall be rechecked seven (7) calendar days following issuance of the Derived PIV Credential – this step protects against the use of a compromised PIV Card to obtain a Derived PIV Credential." What is the purpose of this? Wouldn't checking the revocation status of the PIV credential at issuance and then checking the revocation status of the derived credential at each use be sufficient? Also what action is expected if it is discovered that the PIV is revoked seven days later? How is this action recorded or tracked?	Clarify what the intent of this action is and the expectations for the derived credential issuer.	Declined. The revocation check is done by the Derived Credential issuer, so that the issuer can revoke the Derived Credential, if needed. There are two options Departments and Agencies have when the PIV Authentication certificate validation check returns a revoked certificate status: 1) Immediately revoke the Derived PIV Credential, 2) Investigate why the PIV Credential was revoked and revoke the Derived PIV Credential if there is a risk that the Derived PIV Credential was issued fraudulently.
305	ICAMSC		E	9	351	2.1	Text that reads "using TLS."	Please update to "using Transport Layer Security (TLS)." Spell out acronyms the first time they are used.	Accept.
306	ICAMSC		T	10	382 - 389	2.1	Section 2.1 Initial Issuance states that a Derived PIV Credential shall be issued following verification of the applicant's identity using the PIV Authentication key on his or her existing PIV Card. However, this section does not provide information about how the Derived PIV Credential is generated after the verification.	Please add additional language in Section 2.1 Initial Issuance of the publication that describes how the Derived PIV Credential is generated/created in association with the PIV Card after the applicant's identity is verified.	Resolved by resolution of comment # 83.
307	ICAMSC		T	10	385	2.1	Section 2.2 Maintenance reads, "Similarly, the Derived PIV Credential is unaffected by the revocation of the PIV Authentication certificate." But if the PIV credential is revoked then shouldn't all derived credentials associated with the PIV credential also be revoked? In this scenario an individual could be fired and have the PIV revoked, but the individual could continue to access federal systems with their derived credential from a mobile device.	Clarify the wording to reflect when the associated Derived PIV Credential should be revoked if the PIV credential is revoked. Based on recent briefings from NIST, an agency would not need to revoke the Derived PIV Credential if it is being reissued but would when an individual no longer has a need for a PIV (e.g., got fired).	Resolved by making the underlined changes: The ability to use the Derived PIV Credential is especially useful in such circumstances because the PIV Card is unavailable, yet (while waiting to be issued a new PIV Card) the Subscriber is able to use the Derived PIV Credential to gain logical access to remote Federally controlled information systems from his/her mobile device. And by replacing the first sentence of the paragraph as follows: The Derived PIV Credential is unaffected when the Subscriber replaces his/her PIV Card (re-issuance) with a new PIV Card, including when PIV Card is lost, stolen or damaged.
308	ICAMSC		T	10	401	2.3	Section 2.3 Termination reads, "In all other cases, termination shall be performed by revoking the PIV Derived Authentication certificate." Revoking should occur in ALL cases regardless of any other action taken with the tokens.	Correct so that revocation is the primary action taken for derived credentials regardless of the action taken with the token.	Decline. As indicated by FIPS 201-2 comments, revocation of certificates when associated private key can be zerorized is not a desired. See comments DoD-20, SIA-28 in Revised FIPS 201-2 (among others) at http://csrc.nist.gov/publications/fips/fips201-2/fips201_2_2012_draft_comments_and_dispositions.pdf

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
309	ICAMSC		T	11	422	2.4	Section 2.4 Linkage with PIV Card reads, "The Backend Attribute Exchange [BAE] can be queried for the termination status of the PIV Card, if an attribute providing this information is defined and the issuer of the PIV Card maintains this attribute for the Subscriber." The BAE does not maintain revocation information for PIV Credentials, but only maintains metadata on attributes affiliated with an identity. There are no attributes reflecting termination status of the PIV Card in existence today or planned.	Please clarify how BAE maintains revocation information for PIV Credentials.	Noted. NIST has been in contact with GSA regarding the issue and acknowledges that a new attribute would need to be created to support this functionality.
310	ICAMSC		T	12	444	3.1	Section 3.1 Certificate Policies reads, "The expiration date of the PIV Derived Authentication certificate is based on the certificate policy of the issuer and need not be related to the expiration date of the PIV Authentication certificate or the expiration of the PIV Card." This doesn't appear to be consistent with section 2.4 Linkage with PIV Card. Should the Derived PIV credential expire when the PIV Card that was used to issue the Derived PIV credential expires?	Please add clarification language in Section 2.4 Linkage with PIV Card and 3.1 Certificate Policies to reflect under which circumstances the Derived PIV credential expires in relation to expiration of PIV Card or PIV Authentication certificate.	Resolved by comment #107.
311	ICAMSC		G	13	471 - 472	3.3	Section 3.3 Cryptographic Token Types states that, "Although software tokens are considered embedded tokens for this reason, as a practical matter it will often be impossible to prevent users from making copies of software tokens or porting them to other devices." This statement does not include any security controls or mitigation strategies that can be referenced.	Please include references to existing security controls or guidance in order to provide agencies with methods to mitigate risk.	Resolved by comment #111.
312	ICAMSC		T	13	479 - 481	3.3.1	Section 3.3.1 Removable (Non-Embedded) Hardware Cryptographic Tokens introduces the concept of a PIV Derived Application, but lacks supporting background information around its usage and associated capabilities.	While Appendix B references NIST SP 800-73 for PIV Derived Application requirements, please include additional background information about a PIV Derived Application, its usage and associated capabilities.	Resolved by adding the following descriptive text to section 3.3.1 at the end of the first paragraph. "The use of this data model and its interface supports interoperability and ensures the Derived PIV Credential interface is aligned with the interface of the PIV Card."
313	ICAMSC		G	13	485 - 488	3.3.1	Section 3.3.1 Removable (Non-Embedded) Hardware Cryptographic Tokens directs the reader to Appendix B - Data Model and Interfaces for Removable (Non-Embedded) Hardware Cryptographic Tokens (Normative) for a definition of Application Protocol Data Unit (APDU); however, Appendix B does not provide a definition or mention the term.	Please provide a definition for APDU in this publication.	Resolved by adding a definition in Appendix E. The Application Protocol Data Units (APDU) are part of the application layer in the OSI Reference Model and are used for communication between two separate device's application. In the context of smart cards, an application protocol data unit (APDU) is the communication unit between a smart card reader and a smart card. The structure of the APDU is defined by ISO/IEC 7816-4 Organization, security and commands for interchange.
314	ICAMSC		T	15	561	3.4.1	Section 3.4.1 Hardware Implementations reads, "The required PIN length shall be a minimum of six bytes." A byte is defined as eight (8) bits. How does this equate to a minimum number of characters/digits for the PIN?	Please update to "six digits" or "six characters" - not sure if bytes is proper term here depending on word size of OS.	Resolved by comment #123.
315	ICAMSC		E	15	563	3.4.1	Text that reads "LoA-4."	Please update to "LOA-4" - correct capitalization.	Accept.
316	ICAMSC		T	16	590 - 591	3.4.2	Section 3.4.2 Software Implementations states that password reset is not supported for software cryptographic modules, but it doesn't provide reasoning or justification.	Please provide explanation of why password reset is not supported for software cryptographic modules.	Resolved by comments #4 and #127.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
317	ICAMSC		T	16	592 - 593	3.4.2	It is unclear why a lockout mechanism for repeated unsuccessful activation attempts is not required in software cryptographic modules.	Please provide explanation of why a lockout mechanism for repeated unsuccessful activation attempts is not required in software cryptographic modules.	Resolved by comment #4.
318	ICAMSC		T	16	588 - 593	3.4.2	Section 3.4.2 Software Implementations states that, "The password shall meet the requirements of an LOA-2 memorized secret token as specified in Table 6, Token Requirements per Assurance Level, in [SP800-63-2]" and "Lockout mechanisms for repeated unsuccessful activation attempts are not required for software cryptographic modules." However, Level 2 Memorized Secret Token in Table 6 of SP 800-63-2 states that, "The Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on the Subscriber's account to 100 or fewer in any 30-day period." This implies that a protection against brute force is required. The content in SP 800-63-2 does not align with the guidance in SP 800-157.	The Verifier Requirements in Table 6 of SP 800-63-2 provides guidance for brute force attacks. The guidance in 3.4.2 Software Implementations seems to conflict with the information from Table 6 of SP 800-63-2. If this is an intentional difference, please explain.	Resolved by imposing the same activation requirements for software and hardware.
319									Duplicate removed.
320	Directive Health	Dr. Scott Jenkins		6	281	1.2	This figure depicts a 1-Factor authentication method. It is not equivalent to PIV + data terminal. Any attacker can login from the user's terminal with a PIN. The figure needs another input/output device (tablet, PC, phone) that is different from the mobile device with the derived PIV Credential.	Add an input/output device (tablet, PC, phone) physically separate from the mobile device (with Derived PIV) to connect to the website or portal	NIST (157) Resolved by comment #57.
321	Directive Health	Dr. Scott Jenkins		12	459	3.3	This section is missing information about proximity tokens (soft tokens or hard tokens). This technology is available on the market today, is low cost and provides much improved user experience and security compare to passwords or MDM. - Proximity tokens work with all major mobile device brands - Proximity tokens are low cost (less than 50% of cost for MDM) - Proximity tokens dramatically reduce the number of password entry thus enhancing user experience, and securing the passwords from over-user, eavesdropping and attacks - Proximity tokens secure the user session with continuous authentication, and protect data and device in real-time Source: www.SecureAccessTechnologies.com	Add section: Proximity Tokens Description: Proximity tokens are either a) hardware Bluetooth LE tokens that store the keys or b) Soft tokens that store the keys in the keychain or SE. The proximity tokens are physically separate from the data terminal and act as a second factore. Communication with the data terminal is through encrypted communication over the Bluetooth LE channel. Availability: High: All major mobile platforms support Bluetooth LE Benefits: Always on device. User does not do any action except keep the proximity token in the pocket. Proximity security locks data and alarms when left unattended	Resolved by resolution of comment # 56.
322	Directive Health	Dr. Scott Jenkins		23	789	Appendix B-B2	PIV Derived Authentication Certificate: Add a row: Proximity Token: Very High	PIV Derived Authentication Certificate: Add a row: Proximity Token: Very High	Resolved by comment #56.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
323	42TEK, Inc.	David Snyder	T	6	281	Figure	Figure 1-1 Use of Derived PIV Credential illustrates a device with a derived PIV, equivalent to an MDM-enrolled device, where the MDM certificate is appended/substituted with the derived PIV. This figure does not maintain the 2FA function of PIV where the cert never goes on the data terminal. This figure implies that the user is authenticated simply with a pass code, instead of the current requirement of a pass code + PIV card (2FA). This model is not secure as any user that types the passcode on the "mobile" platform will get access to the website or portal. An internal attacker that gets user's password can use that password to gain access to the web service from the user's mobile device while the user is way, WITHOUT EVER BEING DETECTED. Modern 2FA Soft Tokens hold the derived PIV certs separately so that the 2FA value of the PIV card is not compromised. These tokens store the derived PIV in the Keychain or Secure Element and ensure that the derived PIV never comes in contact with the data terminal, thus maintaining 2FA at all times. Modern 2FA Soft Tokens use HTTP or Bluetooth LE to communicate with other devices. These Modern 2FA Soft Tokens are very cheap and cost the same, if not less, than MDM, while providing a much higher security value, equivalent to PIV cards, much better user	Change Figure 1-1. Add a mobile device that is separate from the data terminal. The mobile device holds the derived PIV and acts as 2FA soft token. The data terminal is physically separate from the 2FA soft token. (Figure attached) ** See email for graphics	Resolved by comment #57.
324	42TEK, Inc.	David Snyder	T	23	790	Appendix C	Table C-1, “Token types and Relation to OMB’s Electronic Authentication Guidelines,” assigns five of the options a “Very High” PIV Assurance Level and Comparable OMB E-Authentication Level of 4 (“Very high confidence in the asserted identity’s validity”), but only “High” and Level 3 (“High confidence in the asserted identity’s validity”) for Software Token. While the document acknowledges at lines 781-784 that the OMB is expected to issue future guidance, I believe that 2FA Software Tokens should be rated at a “Very High” PIV Assurance Level and a OMB E-Authentication Level of 4 when there is a private key on a smartphone or wireless key fob. (See www.secureaccesstechnlogies.com or www.secureauth.com)	Add a new row "2FA Software Token" to Table C-1 Software Token PIV Assurance Level and Comparable OMB E-Authentication Level ratings that says, "Very High" and "4" for Software Token solutions that employ two-factor authentication with a smartphone or wireless key fob that communicates with the first device." (See attached figure) ** See email for graphics	Resolved by resolution to comment #56 and #57.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
325	CDC	Roger Johnson, CDC	Critical	6	266 - 300	1.2	Scope is limited to only mobile devices: • All devices should be managed the same—there should be no artificial distinction created between mobile devices, PCs, etc. If someone has a need for a user to be able to log on to their workstation when they don't have their PIV card (e.g. mission critical people like doctors), this could easily be supported by the use of the Trusted Platform Module and the (future?) Mobile Trusted Module. This might also be more secure that attempting to have an out-of-band process to issue the user temporary credentials when they leave their PIV card at home (obviously an eAuth Level 3 or 4 PIV-derived credential is more secure than a temporary password, and probably better than mapping any type of temporary card to the user's account and then dealing with removal later—we'd expect a lot of exceptions in trying to manage this). • There will be other special cases in which a PIV alternative is needed. In particular, the case of admin accounts. We absolutely need admin tokens to leverage the PIV identity proofing and revocation processes (i.e. strongly tied to the PIV card's status). However, we need the cards to be separate, so that a PIV card inserted into a compromised system (which end users are going to encounter periodically, particularly when remotely accessly the enterprise from a non-GFE computer) cannot be utilized by an attacker to access admin accounts after the user enters the PIV's PIN. Even if the cards enforced PIN entry for each authentication attempt, the user will likely become accustomed to entering the PIN anytime they are	The scope limitation should be removed.	Resolved by comment #15.
326	Hunphrey Chen	Bancgroup		6	281	Figure	This figure removes the PIV card, and substitutes it with a code on the phone... Where is the security piece? Does it mean that anybody that has my device can get in? Does it mean that anybody that steals my pass code can get in?	This figure needs to incorporate a Physical Substiture for the PIV Card. For example, a Bluetooth hard token, a Soft Token running on a second mobile device…	Resolved by comment #57.
327	Hunphrey Chen	Bancgroup		23	790	Appendix C	Table C-1, needs to mention two factor authentication hard tokens and two factor authentication soft tokens that have Very High Assurance Level.	Add a row for Two Factor Authentication hard tokens and soft tokens	Resolved by resolution of comment #56.
328	Fed Contractor	Anis Amro		6	281	Figure	The illustration enables anybody with a mobile device (on MDM) and a PIN to connect to government networks. What guarantees that the person is not an attacker? We are seeing an increasing number of internal attacks on systems (Snowden) and Facilities (Navy Yard shooting). Is it time to remove PIV cards and reduce security to a mere PIN (and a certificate on the device)? Are there any studies on the potential increase on device snatching, session attacks and physical attacks?	Incorporate 2FA	Resolved by comments #57 and #287.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
329	FPKI	CPWG	G	iv	193-195	Executive Summary	The PIV Card is neither used government-wide nor as intended. It is not used government-wide for physical access, and potentially requires having PIV/CAC credentials from that network for logical access as well as requiring the user to have a valid account on the network for local access.	Revise to state "….known as the Personal Identity Verification (PIV) Card, which is currently required for use government-wide for both physical access..."	Resolved by comment #158.
330	FPKI	CPWG	G	iv	197-198	Executive Summary	PIV Card readers are neither ubiquitous nor integrated. It is still most commonly used as a flash pass for physical access; is not fully deployed within all agencies; and, it not necessarily interoperable across agencies.	Reword to read: "...where the PIV Card can provide for common authentication ... across the federal government when fully implemented for both logical and physical access."	Resolved by comment #159.
331	FPKI	CPWG	T	5	234-235	1.1	It is the PKI infrastructure that supports electronic authentication rather than the PIV infrastructure. PIV is only an identity verification process utilizing specific PKI keys and credentials.	Reword to read: "...investment in the PKI and PIV infrastructure for electronic authentication..."	Resolved by comment #161.
332	FPKI	CPWG	T	7	292-293	1.2	It would be useful to make it clear throughout the document that Derived PIV credentials may only be issued by PIV Issuers	Reword to read: "Only derived credentials issued in accordance with this document are considered to be Derived PIV credentials. Derived PIV credentials shall be issued by an accreditited PIV Card Issuer or a Derived PIV credential issuer.	Declined. The purpose of the statement is to clarify while other types of credentials can be derived from the PIV Card, only the credentials specified in SP 800-157 are PIV credentials. Note: The 2nd paragraph of Section 2 covers accreditation, while the 1st paragraph of section 1 specifies that Derived PIV Credentials are issued by federal department and/or agencies.
333	FPKI	CPWG	T	9	333-336	2	This statement ignores the facts that the characteristics and configuration of the certificates, and the operations and security of the issuing CA are also subject to an annual PKI compliance audit in accordance with the FCPCA CP that is separate from the identified "independent assessment."	Reword to read: "In accordance with [HSPD-12], the reliability of the Derived PIV Credential issuer shall be established through an official accreditation process. The processes, as outlined in [SP800-79] and the Federal Common Policy Certification Authority (FCPCA) Certificate Policy (CP), shall include an independent (third-party) assessment."	Resolved by resolution to comment # 166.
334	FPKI	CPWG	T	9	342	2.1	If the document means "valid" then this should say that—active has no meaning in this sense.	Reword to read: "The PIV Authentication certificate shall be validated as being and not revoked prior to issuance of a Derived PIV Credential, and..."	Resolved by comment #167.
335	FPKI	CPWG	T	9	344-346	2.1	This requirement is unclear; who performs this check and how? The 7‑days exactly reflects the exemplar language in SP 800-63 ["(e.g., after a week)"]; however, the RA for the Derived Credential issuing CA can (should) check the status of the certificate immediately—the FCPCA CP requires that revoked credentials be posted within 6 hours.	Reword to read: "The revocation status of the Applicant's PIV Authentication certificate shall be checked immediately and rechecked seven (7) calendar days following issuance of the Derived PIV Credential – this step protects against the use of a compromised PIV Card to obtain a Derived PIV Credential."	Resolved by comment #168.
336	FPKI	CPWG	T	9	344-346	2.1	Need clarification on what happens if the PIV Auth cert is revoked	Suggest adding: "If the revocation status of the PIV Authentication certificate reveals that the certificate has been revoked, the Derived PIV Issuer must revalidate the Subscriber linkage to the Derived PIV Credential or revoke the Derived PIV credential."	Resolved by comment #304.
337	FPKI	CPWG	T	9	359-360	2.1	Retention of biometric samples has PII considerations; SP 800-157 should clearly make reference to protecting them in accordance with the Privacy Act.	Reword to read: "...used to validate the Applicant in accordance with the Privacy Act [PRIVACT]."	Resolved by comment #171.
338	FPKI	CPWG	T	9 & 10	368-369	2.2	This statement is unnecessarily vague—the only CP applicable to PIV certificates is the FCPCA CP.	Reword to read: "…in accordance with the Federal Common Policy Certification Authority (FCPCA) Certificate Policy."	Resolved by comment #95.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
339	FPKI	CPWG	T	11-Jan	414-432	2.4	At this time, D-PIV only appears to be associated with the parent PIV-Card Issuer. Is this the intent of the standard? Should another agency or issuer be allowed to issue D-PIV creds based on a PIV card issued by another issuer?	Strong binding between D-PIV and the PIV issuer is highly recommended. Additional guidelines, in terms of when D-PIV needs to be revoked (based on PIV lifespan, revocation status, etc.), need to be developed. Information is needed on the circumstances when a D-PIV needs to be revoked because the PIV card has been revoked or terminated (in alignment with the guidelines of the assiciated NISTR 7981) as well as mechansims for enforcing this requirement.	Resolved by comment 174.
340	FPKI	CPWG	T		695	B.1.21	D-PIV mentions that the container used for D-PIV will be different from the PIV container	More details are needed around what containers would be used in relationship to D-PIV and the other contents and how that content is linked back to the parent PIV credential.	Resolved by comment #175.
341	FPKI	CPWG	G	General	General	N/A	Can D-PIV be issued by Non-Federal issuers?	Suggest adding a requirement that states only PIV Issuers may issue D-PIV	Noted. Draft SP 800-157 already states in multiple places that Derived PIV Credentials are issued by Federal departments and agencies.
342	FPKI	CPWG	T	10	379-381	2.2	These provisions must be consistent with the FCPCA CP. Given that PIV is only covered by the Federal Common Policy, the vague reference to an unnamed certificate policy, as well as the inclusion of a policy directive, is inappropriate. In addition, a damaged PIV Card is not cause for revocation of the certificates housed therein, therefore there is no reason to presume that a damaged mobile device should require revocation of the associated certificate.	Reword to read: "...Credential is lost, stolen, or compromised, the PIV ... revoked in accordance with the Federal Common Policy Certification Authority (FCPCA) Certificate Policy (CP)."	Resolved by comment #177.
343	FPKI	CPWG	T	11	409-411	2.4	This statement is inconsistent with the first sentence in this subparagraph; and, it is inconsistent with the provisions of FIPS 201 and the FCPCA CP, which state, respectively: "(§2.9.4) A PIV card is terminated when the department or agency that issued the card determines that the cardholder is no longer eligible to have a PIV Card. The PIV Card shall be terminated… " Similar to the situation in which the card or a credential is compromised, normal termination procedures must be in place as to ensure the following: ● The PIV Card itself is revoked: ● The PIV Card shall be collected and destroyed, if possible. ● Any databases maintained by the PIV Card issuer that indicate current valid (or invalid) FASC-N or UUID values must be updated to reflect the change in status.	Reword to read: "The issuer of the Derived PIV Credential shall not solely rely on tracking the revocation status of the PIV Card certificate as a means of tracking the termination status of the PIV Authentication certificate. This is because there are scenarios where the card's PIV Authentication certificate is not revoked even though the PIV Card has been terminated."	Resolved by comment #181.
344	FPKI	CPWG		12	442-443	3.1 (and globally)	Text should not reference specific worksheet numbers in the Cert Profile	Remove references to Worksheets throughout the doc and simply reference the cert profile document	Declined. Referencing the specific worksheet within the profile document helps to avoid confusion for the reader.
345	FPKI	CPWG	T	12	444-446	3.1	There should be only one certificate policy related to any PIV certificate—the FCPCA CP. Further, there are existing conditions in the FCPCA CP regarding the expiry relationships between certificates and the PIV card (i.e., the former cannot exceed the latter).	Reword to read: "The expiration date of the PIV Derived Authentication certificate is based on the Federal Common Policy Certification Authority (FCPCA) Certificate Policy (CP)."	Resolved by comment #183.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
346	FPKI	CPWG	G	12	435-458	3.2, 3.3	3.1 and 3.2 use the term "PIV Derived" instead of Derived PIV like the rest of the document. Does the use of the term PIV Derived mean that the credential was derived from PIV, the Derived credential is a PIV credential or the policy was derived from the Common-Auth policy?	Review the use of the terms "PIV Derived" and "Derived PIV" to ensure the use is consistent and appropriate throughout the document. Also, consider replacing the term Derived PIV with "Mobile PIV"	NIST (157). Resolved by using "Derived PIV Credential" throughout the document and removing "PIV Derived."
347	FPKI	CPWG	G	24	792-808	Glossary	A definition of "PIV Derived" and "Derived PIV" is needed BTW, It took 8 hours in CPWG meetings, but we were able to ascertain that the term Derived PIV is used 96 times and PIV Derived is use 111 times. Note that FIPS 201 uses both terms as well.	Suggest defining the terms "PIV Derived" and "Derived PIV" in the glossary We believe that "PIV Derived" implies the creation of a credential that could be issued by any issuer based on presentation of a PIV Card and "Derived PIV" implies that a PIV Issuer has issued a credential that can be used as a PIV credential (e.g., on a mobile device).	Resolved by comment #346. The term “PIV derived credentials” appears only one time in FIPS 201-2, in the Abstract, and it is a typographical error. It should have said “derived PIV credentials,” just as it does in similar text in Section 1.4 of FIPS 201-2.
348	G&D	A.Summerer	T	6	269	1.2	A hardware token could be also embedded in the sleeve of a mobile device.	Is it allowed to use sleeve solutions at all? If yes, an embedded token in a sleeve should also be mentioned in the list of possible options. If not, this specification shall explicitly disallow the usage of a sleeve solution.	Noted. A “sleeve solution” would be a removable hardware cryptographic module. Section 3.3.1 of Draft SP 800-157 lists the types of permitted removable hardware cryptographic modules. All others are explicitly disallowed. While a “sleeve solution” would presumably not be a UICC or an SD card, it would be allowed if “sleeve” connected to the device via USB in accordance with Section 3.3.1.3.
349	G&D	A.Summerer	T	6	269	1.2	A hardwarre token could also be a bluetooth HW token (a HW token which is connected with the device via bluetooth).	Is it allowed to use bluetooth HW token? If yes, bluetooth HW token should also be mentioned in the list of possible options. If not, this specification shall explicitly disallow the usage of bluetooth HW tokens.	Resolved by resolution of comments # 193 and #56.
350	G&D	A.Summerer	E	13	480	3.3.1	"the PIV Derived Application shall be implemented" is not in line with the GlobalPlatform terminologies and could be misunderstood. The same applies to line 525 in chapter 3.3.1.3 on page 14.	"installed" is better than "implemented"	Accept.
351	G&D	A.Summerer	T	14	507-515	3.3.1.1	In this section ASSD is declared as mandatory for the APDU communication. However, ASSD is rarely implemented in mobile devices today. The integration of ASSD in mobile device requires modifications in the OS kernel. On the other hand, some vendors of smart µSD cards provide special proprietary driver solutions for the APDU transfer which can be installed as mobile app without root permissions and firmware modifications. Such kind of drivers are not compatible to ASSD but allow the usage of smart µSD cards on many devices today without firmware modifications.	Please mention ASSD only as a recommended option beside of other APDU transfer options for secure µSD cards. The compliance of APDU transport on device level should rather be focused on application interface level and not on SE drivers level. See comment #4 in terms of device compliance.	Resolved by comment #11.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
352	G&D	A.Summerer	T	13-15		3.3.1, 3.3.2	The device comliance requirements for the different hardware tokens are too much focused on SE drivers level. E.g. for smart µSD ASSD is mandatory. However, for UICC and eSE no requirements exist. But technically all these different SEs require communication driver interfaces for the APDU communication. Today different approaches exist to realise an APDU communication with a certain SE. This kind of approaches are irrelevant for the mobile apps as long as an abstraction layer on application level exist which can be used to access all these SEs with a common API.	The SIMalliance has standardized an API ('OpenMobileAPI') for accessing Secure Elements in Mobile Devices. Today, many devices support this API for UICC, eSE and secure µSD card access. The intention of this API is to provide mobile apps a common interface for APDU transfer towards SEs, no matter which kind of SE. The OpenMobileAPI provides a common set of functions for the APDU transfer and hides the details of the communication drivers for the different SEs. OpenMobileAPI drivers are either integrated in the mobile OS or can be installed as mobile app. The OpenMobileAPI framework reduces complexibilty and assures flexbility. The SIMalliance has already released a test specification and the industry is currently working on an OpenMobileAPI qualification program for devices. Therefore it is recommended to refer to this API rather than low level protocols in terms of device compliance.	Resolved by comment #11.
353	G&D	A.Summerer	T	22	744	B.2	Why does the ICC only represent the removable hardware token and not the embedded hardware token?	Please change "...that represents the removable hardware cryptographic token" to "...that represents the hardware cryptographic token". Between embedded ICC or removable ICC there is no difference. Both require this APDU interface.	Declined. As noted in Section 3.3 an embedded hardware cryptographic module may implement the APDU-based Derived PIV Credential, but it is not required to.
354	G&D	A.Summerer	G	iv	218	Executive Summary	Some sections in this paper indicate that the PIV derived credential (i.e. X509 authentication certificate) are created on issuers side remotely and transfered securily to the SE in the mobile device. The corresponding key pair seems to be generated prior in the token on client side. Section 3.2 mentions that for LOA4 the derived authentication keys has to be generate in a FIPS140 crypto. module (i.e. none exportable in the target SE). Must the keys always be generated in the token on client side, even LOA3? It seems that the issuance process always requires a prior PIV card authentication by the applicant before the derived credential is created and loaded.	The issuance process seems to consist of following steps: 1) Request of derived credentials which requires a PIV Card auth. towards server 2) Generation of derived key pair in module of mobile device 3) Upload of public key 4) Creation of derived certificate 5) Download of derived certificate into module of mobile device If this is the expected issuance process it would be helpful to have a clear flow description with figures in this paper. Otherwise it is difficult to get the picture of the whole concept with the information in the different sections.	Resolved by comment #83.
355	G&D	A.Summerer	G	iv	218	Executive Summary	Obviously the derived credentials and the original credentials on the PIV card have no link in a mathematical sense. The derived authentication keys are randomly generated and the derived certificate is signed by the issuer.	It would be helpful to mention explicitly in the paper that the derived credential and the original credentials on the PIV Card have no link in a mathematical sense. The linkage between original and derived credential is entirely based on life-cycle status sync. by the issuers.	Declined. As noted it is obvious that there is no such link, so there is no need for SP 800-157 to say that. Any text explicitly stating that there is no link between the certificates “in a mathematical sense” would be very confusing for many of the readers.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
356	G&D	A.Summerer	G	iv	212	Executive Summary	Following sentence implies that derived credentials may only be used with the mobile device: "The use of a different type of token greatly improves the usability of electronic authentication from mobile devices to remote IT resources."	Derived credentials in a mobile device can technically also be used on the PC (i.e. laptop or desktop). The mobile device could be securely paired with the PC via e.g. WIFI, USB or Bluetooth. The benefits: - No Smart Card reader needed - Simplifies work on PC - Less wear and tear for PIV cards Therefore it might be worthwile to allow the usage of derived credentials also on the PC. Is it allowed to store the credentials also in the PC (i.e. in a TPM). Or what is about HW dongles? How can the server prohibit this if this is not allowed?	Resolved by Comment #15.
357	G&D	A.Summerer	G	8	276	1.2	The PIV derived credentials on mobile device platforms leverage a number of new use cases. E.g. encypted voice communication or encrypted cloud storage.	It would be interesting to outline also potential new use cases leveraged by PIV derived credentials on mobile device. Derived credentials could be potentially used for new use cases like secure cloud storage access, secure voice, email encryption/decryption, email signature, Windows Logon, VPN connection.	Resolved by Comment #15.
358	G&D	A.Summerer	G	9	340	2.1	For remote issuance the PIV card holder has to proof its identity by a PIV card authentication before the PIV derived credentials are issued on the mobile device. Technically this PIV card authentication can be performed with the PC (with smart card reader) and with the mobile device (e.g. via NFC) as well. The latter approach has the benefit that the whole issuance process can be performed within a single transaction with the mobile device. However, this paper does not describe these different options and if all these options are allowed.	It would be helpful if this paper outlines possible remote issuance scenarios with different PIV card authentication approaches. E.g. Scenario 1: PIV card authentication on the mobile device combined with key generation and download of the derived credential in the same transaction. Scenario 2: PIV card authentication on the PC. Generation of keys and download of the derived credential with the mobile device in a second step. This scenario could potentially outline the concept how the temporary secret can be used to link the different transactions.	Resolved by comment #83.
359	G&D	A.Summerer	G	18	628	B.1	This section mentions that the contactless interface shall not be supported by the PIV Derived Application. However, NFC card emulation mode would technically allow to use the PIV Derived Application on the UICC or eSE via NFC. E.g. for PACS	The possibility to use the PIV Derived Application via NFC (e.g. for PACS) is not mentioned in the whole document. But it would be worthwile to allow this option in this paper.	Resolved by comment #15.
360	G&D	A.Summerer	G	12	453	3.2	3.2 requires hardware tokens validated to FIPS140 L2 or higher. However, FIPS140 L2 validation for UICCs might be an issue since UICC specific performance requirements might potentially conflict with the FIPS140-2 self test requirements which are mandatory for L1, L2, L3 and L4.	A special FIPS140 scheme for UICCs should be developed which improves the concept of self tests in terms of performance.	Noted. This would be an issue for the Cryptographic Module Validation Program, not for SP 800-157.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
361	G&D	A.Summerer	G	12	463	3.3	What is exactly a hardware token? A tamper proof ICC? Or can a TEE (like in GlobalPlatform defined) also be an embedded hardware token (not tamper proof but trusted)? However, chapter 3.2 mandates for LOA4 derived credentials the key pair has to be generated in a crypto module [FIPS140] Level 2 or higher that provides Level 3 physical security. Does it mean a hardware token has to have these levels or higher?	The document shall explicitly define what a hardware token is. Is it always a crypto module [FIPS140] Level 2 or higher that provides Level 3 physical security?	Noted. The text clearly specifies FIPS 140-2 Security Level 2 (Overall) and Physical Security equivalent to Security Level 3. See also NIST IR 7981 for hybrid approach, which TEE may be part of. While dedicated (e.g. embedded) hardware solutions, are not commercially available at this time, many mobile devices on the market do provide hardware-backed features that can protect keys of credentials that are stored on mobile devices. Typically these features can protect keys using hardware-based mechanisms, but a software cryptographic module uses the key during an authentication operation. This hybrid approach provides many security benefits over software-only approaches, and should be used whenever supported by mobile devices and applications. See also resolution to comment # 247.
362	Intercede	Andy Atyeo, Chris Edwards		10	371	2.2	The standard case for a certificate re-key of derived credential will be a key generation inside the derived credential hardware (for LOA4), followed by the construction of a certificate request (PKCS10), which requires a signature operation, since certificate requests are self-signed for 'proof of possession'. To perform this, according to sp800-73 will require entry of the cardholder PIN. When there is a secure channel between the crypto-module on the (CMS) server and the derived-credential crypto-module, in order to supply the cardholder PIN to the chip would require the cardholder PIN to be submitted to the (CMS) server, in order it could be encrypted into the secure channel. It is clearly undesirable to require the cardholder PIN to be required to be sent to the server, as this introduces unnecessary risk. The current statement (line 371) saying a secure channel must be used when the PIV derived authentication key is "Stored" is ambiguous. Does "Stored" mean "Imported", or does "Stored" also include a key generation on the chip (since in a key generation, the key is stored, even though it never leaves the boundary of the derived credential crypto-module). If "Stored" includes on-card key generation, then it forces the cardholder PIN to be sent to the server causing unnecessary risk. Therefore if this can be clarified to indicate that the secure channel applies to key "import" rather than key being "stored" this will remove the risk. In this way, the philosophy would be to protect *secret* data from the server to the chip, but still allow cardholder instigated operations (which involve PIN entry) on the client even if these are part of the post issuance. (Incidentally this	Communication between the issuer and the cryptographic module in which the PIV Derived 371 Authentication private key is stored **imported** shall occur only over mutually authenticated secure sessions 372 between tested and validated cryptographic modules.	Declined. Section 3.2 states that at LOA-4 "the PIV Derived Authentication key pair shall be generated with a hardware cryptographic module … that does not permit exportation of the private key." So, "stored" cannot mean "imported," as the key can never be imported at LOA-4. The location where the key is stored and where it was generated must be the same. The reason for requiring a mutually authenticated secure channel is not to protect the private key, it is to ensure that the issuer knows where the private key was generated and is stored. If the GENERATE ASYMMETRIC KEY PAIR command is sent over a mutually authenticated secure session and the public key that is provided in the response over that same secure session is placed in the certificate then the issuer has assurance that the private key corresponding to the key in the certificate was generated in the same cryptographic module as was the key that appeared in the certificate that was created during initial issuance. The text in lines 371-373 only requires a mutually authenticated secure session for communication between the issuer and the cryptographic module. If the PIN needs to be entered, it could be sent directly by the cardholder to the cryptographic module, in which case it would not have to be sent over a secure

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
363	CertiPath	Spencer	G			General	"Derived PIV" suggests that the credential is a PIV as defined in FIPS 201-2, as opposed to being a credential "derived from" a PIV (as would be the case if the credential were called "PIV-derived"). As such, this suggests that the credential carries all the weight of a PIV, the primary differentiator of which is the *suitability* determination. By basing the Derived PIV on a PIV (rather than doing independent identity proofing and suitability determination), the Derived PIV seemingly inherits not only the identity but also the suitability. Since suitability is more variable than identity (one's suitability can change over time, but can also be adjudicated differently across different organizations during the same instance in time), some discussion of the implications of Derived PIV to suitability should be included.	Discuss the suitability aspects of the Derived PIV credential. For example: Does it inherit the suitability of the 'parent' PIV? Or, should an independent suitability determination be made? This is particularly important if issuers different from the 'parent' PIV issuer are going to be permitted to issue Derived PIV credentials. Also consider whether these are "Derived PIV" or "PIV-Derived". In other words, do they carry the same weight as the parent PIV?	Noted. As per NIST 800, the Derived PIV Credential is a PIV credential. As a valid PIV Card is required to be issued a Derived PIV Credential, and as the Derived PIV Credential must be terminated if the PIV Card is terminated, there is no reason to believe that there are any special implications of Derived PIV Credentials to suitability. Suitability for the PIV card and the Derived PIV Credential is topic in NIST SP 800-79.
364	CertiPath	Spencer	G			General	In several places, the current draft refers to the issuer's certificate policy. This is incorrect. The Federal PKI mandates a single certificate policy for PIV - the COMMON Policy Framework. This is where the policy changes to incorporate Derived PIV policy OIDs will be made. All issuers must subordinate under COMMON. Also review statements made in SP 800-157 concerning these certificates to ensure they do not contradict Federal COMMON Policy requirements concerning PKI components and their containers (software or hardware).	Reference the fact that the "Derived PIV" gets its policies from the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework and cite this document throughout whenever references are made to the Derived PIV Authentication Certificate or keys. Update policy statements concerning certificates and keys to conform to the COMMON Policy Framework.	Resolved by comment #95.
365	CertiPath	Spencer	G			General	If the Derived PIV is to carry identity and suitability (see previous comment) weight similar to its parent PIV, it is counter-intuitive that this Derived PIV could be issued by an entity other than the issuer of the 'parent' PIV. Further, consider requiring some reference to the 'parent' PIVAuthN certificate in the Derived PIV AuthN certificate. Finally, synch expiration of the Derived PIVAuthN to the parent PIV AuthN certificate. This will ensure maintenance of the highest level of integrity through close linkage of the 'chain of identity' in the derived credential and will prevent overuse.	Revise the document to ensure closer linkage of PIV/Derived PIV relationship.	Resolved by comment #107. Use of Derived PIV Credentials if the underlying PIV Card is lost or stolen is a use case requested by the FICAM LAWG. The capability of external issuers to issue Derived PIV Credentials allows these organizations to support other Agency employees on detail. Departments and Agencies are free to include a reference linking Derived PIV Credentials to their PIV credentials.
366	CertiPath	Spencer	E	iv	202	Exec	"department" should be plural	Make "department" plural	Accept.
367	CertiPath	Spencer	E	5	253	1.1	"these type of readers" is grammatically incorrect	"this type of reader" or "these types of readers"	Resolved by replacing phrase "these type of readers" with "these types of readers"
368	CertiPath	Spencer	E	Gen	Gen	General	Page numbering goes from iv to 5.	Restart numbering at 1 following page iv.	Accept.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
369	CertiPath	Spencer	E	5	254	1.1	Word Choice. The word "could" in this opening sentence seems awkward and inappropriate in the context of the paragraph. Suggest amore assertive statement of fact.	Recommend rewriting this paragraph to suggest that "Emerging technology associated with the mobile device that takes advantage of NFC can be used to communicate with the PIV card."	Resolved by replacing: "Newer technology could take advantage of mobile devices that can directly communicate with and use PIV Cards over a wireless interface using Near Field Communication (NFC)" with: "Newer technology on mobile devices can directly communicate with and use PIV Cards over a wireless interface using Near Field Communication (NFC)"
370	CertiPath	Spencer	E	5	260	1.1	The sentence that begins "The user would need. . ." is unnecessary.	Delete the referenced sentence.	Noted. The intent of this section is to provide a technology overview. The sentence is needed to clarify how NFC would be used with mobile devices.
371	CertiPath	Spencer	T	6	271	1.2	Cryptographic modules must be FIPS 140 approved	Revise this sentence to reference FIPS 140 in association with the crypto modules.	Resolved by resolution to comment # 163.
372	CertiPath	Spencer	E	7	293	1.2	"The document. . ." reads better as "This document. . ." Otherwise, a reader may wonder if this is something other than this document	Replace opening "the" with "this"	Accept.
373	CertiPath	Spencer	E	7	299	1.2	"The publication. . ." reads better as "this publication". Otherwise, a reader may wonder if this is something other than this document - (and on another note, why change to "publication" here? This may be a point of confusion).	Replace the opening 'the' with 'this'. Consider changing "publication" to "document."	Accept.
374	CertiPath	Spencer	T	9	335	2	The citation to SP 800-79 is too limited. This covers the issuance process only. Does not take into account the Derived PIV Authentication Certificate must be issued under COMMON Policy Framework or that the provider must be subordinated under COMMON. SP 800-78 also has a voice here.	Recommend this language is revised to either cite FIPS 201-2 directly or include the Federal Common Policy Framework as a reference.	Resolved by comment #166.
375	CertiPath	Spencer	E	9	342	2.1	What does "active PIV" mean?	Revise this sentence as follows: "The PIV Authentication certificate's validity (i.e. not expired or revoked) shall be verified prior to issuance of a Derived PIV Credential, . . ."	Resolved by comment #167.
376	CertiPath	Spencer	T	9	344	2.1	What is the reasoning behind checking validity after 7 days? How does this protect against a compromised PIV? It assumes too much and seems unnecessary, especially since there is supposed to be continual monitoring of the PIV credentials for termination - would it not be better to flag compromised PIV credentials and do an exception check?	Revise this section to remove the 7 day waiting period.	Resolved by comment #150.
377	CertiPath	Spencer	T	9	344	2.1	If a routine check reveals the PIV Authentication certificate was revoked for key compromise what then?	Revise this section to include next steps if the PIV AuthN certificate is revoked for key compromise - regardless of when this revocation takes place.	Resolved by comment #304.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
378	CertiPath	Spencer	T	9	352	2.1	If the PIV authentication key is being used to prove identity, why is a temporary shared secret needed? Can the PIV credential not be used to reassert identity in subsequent sessions?	Revise this section to cite use of PIV for identity assertion.	Declined. The issuance process may require that Applicant to authenticate himself/herself from the mobile device on which the PIV Derived Authentication private key will be stored. If the Applicant cannot use the PIV Card with the mobile device (a likely scenario) then some other form of authentication will need to be used (a temporary secret). The Applicant may authenticate from a different device (e.g., a desktop computer) using the PIV Card in order to obtain the temporary secret.
379	CertiPath	Spencer	T	11	355	2.1	The LOA 4 private key must be generated in and remain in a hardware cryptographic module?	Recommend adding this clarification - since you have included others.	Noted. Section 3.2 titled cryptographic specification includes the details of the cryptographic module.
380	CertiPath	Spencer	T	9	361	2.1	This final paragraph suggests there is a threat when multiple Derived PIVs are issued but does not provide any corrective action. It also fails to account for the chaos of multiple Derived PIVs associated with the same 'parent'. This problem can be mitigated, at least partially, by only allowing Derived PIV issuance by the issuer of the 'parent' PIV.	Recommend this paragraph be expanded to include protection mechanisms.	Resolved by comment #172.
381	CertiPath	Spencer	T	9&10	368	2.2	There is an inference that Derived PIV credentials may be issued under some Certificate Policy other than COMMON. Is this the intent? If not, there should be an explicit statement that Derived PIV credentials shall be issued under the U.S. Federal COMMON Policy Framework	Revise sentence beginning on line 368 as follows: "These operations may be performed either remotely or in-person and shall be performed in accordance with the X.509 Certificate Policy for the U.S. Federal PKI COMMON Policy Framework."	Resolved by comment #95.
382	CertiPath	Spencer	T	10	380	2.2	See comment #2 above	Revise this to cite the COMMON Policy Framework.	Resolved by comment #95.
383	CertiPath	Spencer	T	10	382	2.2	Derived credentials should become invalid when the PIV Authentication credential from which they are derived becomes invalid. Where is the chain of custody for a LOA 4 credential whose 'parent' was revoked? This is particularly true for a PIV authentication credential that is revoked for cause (key compromise) even if the right to hold a PIV is not terminated.	Recommend requiring replacement of derived credentials when the 'parent' PIVAuthN credential is replaced - no matter the reason. The derived credential should not outlive its 'parent'.	Resolved by comment #97.
384	CertiPath	Spencer	T	10	393	2.3	This statement should be more assertive. If the Derived PIV is no longer needed it SHALL be revoked regardless of the status of its parent.	Replace "may" with "shall" in this sentence.	Accept. Also see comment #197.
385	CertiPath	Spencer	T	10	398	2.3	This is the definition of LOA 4 - why not say so?	Include reference to LOA 4 in this statement.	Declined. A PIV Authentication private key may be created and stored on a hardware cryptographic token that does not permit the user to export the private key even if the corresponding certificate was issued at LOA-3.
386	CertiPath	Spencer	T	13	417	2.4	Since this is a 'derived' credential, it should be issued by the same entity that issued the parent credential. How do you maintain chain of custody if you allow distance between the PIV credential and its derivative(s)?	Change the concept to require a derived credential be issued by the same issuer as the PIV credential.	Resolved by comment #97.
387	CertiPath	Spencer	T	11	421	2.4	This distance from the PIV card issuer lowers the integrity of the derived credential. You are relying on something other than the issuer to verify validity of the linkage.	Reconsider allowing derived credentials to be issued by an entity other than the PIV card issuer.	Resolved by comment #97.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
388	CertiPath	Spencer	T	11	430	2.4	How is linkage updated? There is a PIV against which the Derived PIV was issued. Now this PIV is replaced? Where is the chain of identity back to the original PIV. Is the PIV and its successor compared - are the biometrics on the two evaluated for LOA4? Why would a Derived PIV ever outlive its parent?	Reconsider the notion that Derived PIV are not linked to the parent PIV.	Resolved by comment #97.
389	CertiPath	Spencer	G	12	444	3.1	Why would the derived credential not be in synch with the 'parent' credential? The Authentication credential has specific requirements for repeating intial identity proofing, in person appearances etc. Chain of identity suggests the derived credential has to be linked to the 'parent'. Recommend rethinking this. Also, the Derived PIV must be under COMMON. Therefore, any reference to the CP of the Issuer is in error.	Link the expiration date of the derived authentication certificate to the expiration date of the PIV authentication credential. Remove reference to the "CP of the Issuer"	Resolved by comments #95 and #107
390	CertiPath	Spencer	E	13	471	3.3	This sentence is badly constructed. The phrase "for this reason" should be separated from the preceding text by a comma - unless you think there's a reason in the preceding text - and the comma following "for this reason" should be removed.	Check grammar/sentence construction to ensure it is conveying the message you intend.	Resolved by removing sentence.
391	CertiPath	Spencer	T	13	471	3.3	The premise of allowing the copying of software keys by the subscriber is covered in the Federal COMMON Policy Framework. It is permissable provided certain security measures are observed. This would seem to be a good thing for derived PIV - derive once, use on multiple devices.	Recommend reviewing U.S. Federal Common Policy Framework Section 6.2.4.2 and revising this section accordingly.	Resolved by removing referenced sentence.
392	CertiPath	Spencer	T	13	479	3.3.1	Footnote 7 refers to smart cards, should reference hardware modules	Reword footnote 7.	Resolved by changing "smart card" to "UICC".
393	CertiPath	Spencer	E	15	562	3.4.1	Bytes' does not seem to be the correct term here.	Replace 'bytes' with 'digits'.	Resolved by comment #123.
394	CertiPath	Spencer	E	15	564	3.4.1	Use of the word "authentication" in this sentence may confuse entities. Failed authentication attempts suggests failure of the Derived PIV authentication credential to be accepted by a relying party, not that the owner of the Derived PIV failed to enter the correct activation PIN (as described in the previous paragraph).	Recommend replacing "authentication" with "activation".	Accept.
395	CertiPath	Spencer	T	16	592	3.4.2	What happens to the private key when password is forgotten and new key issued? It is still subject to a brute force password attack. Is it revoked? No lockout mechanism means an infinite number of password guesses. This is not the case for any other LOA 3 PKI policy	Rethink this. Seems to be a logistical nightmare on the one hand and a loosening of requirements on the other.	Resolved by comments #4 and #127.
396	CertiPath	Spencer	T	17	607	Appendix A	Do not cite id-fpki-common-policy here. Rather cite U.S. Federal Common Policy Framework.	Reword this statement as follows: "Note that this means that in order to be able to use a copy of the key management private key in [FIPS140] Level 1 software cryptographic module, the corresponding certificate would have to be issued under a certificate policy as defined in the U.S. Federal Common Policy Framework that does not require the use of a [FIPS140] Level 2 hardware cryptographic module."	Declined. There is no requirement for key management certificates to be issued under the common policy.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
397	CertiPath	Spencer	G			Appendix B	Biometrics? Biometrics are not just for PACS. Biometrics can now be used to activate the PIVAuthN. Many mobile devices are incorporating biometric readers. There should be a provision for including biometrics containers on the Derived PIV app.	Consider the inclusion of biometrics - at least for hardware based modules.	Resolved by comment #13.
398	CertiPath	Spencer	G			Appendix B	Does the derived PIV contain any reference to the PIV from which it was derived? If not, how is the relationship between the two identified? What links them?	Document needs more detail on the technical aspects of the linkage.	Noted. Linkage is discussed in Section 2.4.
399	Hunphrey Cheng	Verizon	T	6	281	Figure	This figure removes the PIV card, and substitutes it with a code on the phone... Where is the security piece? Does it mean that anybody that has my device can get in? Does it mean that anybody that steals my pass code can get in? The idea of derives certificates is really good... Moving with the times, and getting rid of costly PIV readers is an imperative... However, one must not compromise his/her own security... as that is the foundation of business... and there are a lot of security innovations that provides better security than PIV cards, better user experience, and most importantly, better security. A combintation of iBeacon, 2FA and proximity monitoring is definately the solution of choice: 1) Store the Derived Credentials in the keychain/SE of a first mobile device. 2) Have a security layer on a second mobile device that collects the user Password, a Token Key from the first mobile device... Those are forwardedto Active Directory for authentication. This solution maintains 2FA. An attacker needs the first mobile device, the second mobile device and the user password to gain access.	This figure needs to incorporate a second factor to compensate for the PIV Card. For example, a mobile phone with Derived PIV Credentials can act as a second factor for a PC, tablet or door reader	Resolved by comment #57.
400	Hunphrey Cheng	Verizon	T	13	475	3.3.1	Need a section on: Non-Removable, Non-Embedded Hardware Cryptographic Tokens 1- Any mobile phone can be a token for a second mobile device 2- 2FA Soft Tokens 3- 2FA Proximity Tokens (iBeacon) 4- 2FA Hard Tokens (iBeacon)	Need a section on: Non-Removable, Non-Embedded Hardware Cryptographic Tokens 1- Any mobile phone can be a token for a second mobile device 2- 2FA Soft Tokens 3- 2FA Proximity Tokens (iBeacon) 4- 2FA Hard Tokens (iBeacon)	Resolved by comment #56.
401	Hunphrey Cheng	Verizon	T	23	790	Appendix C	Table C-1, does not mention two factor authentication hard tokens and two factor authentication soft tokens that have Very High Assurance Level.	This table needs to have a row for Two Factor Authentication soft tokens	Resolved by comment #56.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
402	Tyfone Inc.	Drew Thomas				General	SD memory card implementation restriction and Wireless Token with Cryptographic Module	Suggested that publication should not restrict SD memory card implementation to ASSD. It should allow for other methods as long as APDUs and Smart Cards are supported and the API to access them is made available. Provided language for Section 3.3.1.1 and also suggested addition to Section 3.3 which will include Section 3.3.3- Smart Card tokens that will connect wirelessly to any device.[Provided language section for the draft.]	Resolved by comment #56. See also comment #11.
403	Tyfone Inc.	Drew Thomas				3.3	Suggest that Section 3.3.3 be added to support Smart Card tokens that will connect wirelessly to any device.	Suggested language for consideration. See an email for attachment to see suggested language.	Resolved by resolution of comment #56.
404	PrimeKey AB	A. R.				General	Use of SIM-cards	Added text: present major costs and hasseles not to mention limited integration in mobile phone applications like the browser	Noted NISTIR 7981 covers the pros and cons of UICCs.
405	PrimeKey AB	A.R.				General	Use of uSD cards	Added text: not generally supported, limited integration in mobile phone applications like the browser	Noted NISTIR 7981 covers the pros and cons of uSD cards.
406	PrimeKey AB	A.R.					FIPS-certified mobile software crypto modules	Have very limited assurance in the commercial world	Noted.
407	PrimeKey AB	A.R.					The need for physical presence is incorrect	Google's U2F shows the way: hardware assisted attesting crypto modules can use a PIV as "bootstrap" credential in an self-serive on-line process as well as optionally be verified as FIPS compliant	Noted.
408	PrimeKey AB	A.R.					Virtual environments like https://www.samsungknox.com/en/solutions/knox/technical is needed	The next step for MDM	Noted.
409	National Security Agency - Information Assurance Directorate		T	13	472-473	3.3	Many mobile OSes make it impossible for users to make copies of software tokens and prevent porting them to other devices; stating that the opposite is often true is misleading given the current state of mobile technology.	Either strike or amend the sentence to encourage agencies to use Mobile Devices which provide protections to keys stored by the OS in a "software token."	Resolved by deleting sentence.
410	National Security Agency - Information Assurance Directorate		T	13	482	3.3.1	While a carrier may offer a security domain on a UICC that is separate from other domains, that security domain will never be fully under the explicit control of the issuing agency. The carrier, in order to perform network operations, will control the card management key, which will allow (possibly undetected) modification of the card, the card's firmware, and security domains on the card.	UICC Cryptographic Modules should be removed as an acceptable solution.	Noted. There may need to be an SLA and level of trust involved when using an MNO's UICC.
411	National Security Agency - Information Assurance Directorate		E	15	549-550	3.3.2	The certificate policy requirement is redundant to 3.2 and was not included in any section of 3.3.1.	Remove sentence	Declined. The requirement is repeated so the reader understands the applicable policy requirements for embedded cryptographic tokens.
412	National Security Agency - Information Assurance Directorate		E	15	562	3.4.1	6 bytes is a very long PIN.	"bytes" should probably be "digits" or "characters"	Resolved by comment #123.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
413	National Security Agency - Information Assurance Directorate		T	16	588	3.4.2	An 8 character/6 digit password is unnecessarily long for a mobile device that uses a hardware-backed key store, and not nearly sufficient for a fully software (for example, PKCS#12) implementation. Users will attempt to bypass security mechanisms that are not appropriate to mobile technology.	Additional nuance in the description of embedded tokens will allow for a more nuanced discussion of password-based mechanims.	NIST (157) Resolved by comment #147.
414	National Security Agency - Information Assurance Directorate		T	16	590	3.4.2	Modern commercial mobile devices that are enrolled in enterprise management have support for password reset. Keys that are stored in the Mobile OS will be subject to this password reset. Every modern mobile OS cryptographically ties the device unlock passcode to the OS key storage and authorizes access to the OS key storage, so an additional password is unnecessary. If "software tokens" are exclusively PKKCS#12 files (which don't have this capability), then the description should make that clear.	A more nuanced treatment of embedded tokens will alleviate descriptions that seem incompatible with today's mobile technology. Issuing agencies should be required to implement password reset for OS key storage.	Resolved by comment #127.
415	National Security Agency - Information Assurance Directorate		T	16	592-593	3.4.2	Modern commercial mobile devices support lockout mechanism for repeated unsuccessful unlock attempts. Every modern mobile OS cryptographically ties the device unlock passcode to the OS key storage and authorizes access to the OS key storage, so an additional password is unnecessary.	A more nuanced treatment of embedded tokens will alleviate descriptions that seem incompatible with today's mobile technology. Lockout mechanisms should be required for OS key storage.	Resolved by comment #4.
416	National Security Agency - Information Assurance Directorate		T	23	780	Appendix C	Of late, mobile devices have become larger to accommodate larger screens. They are getting narrower.		Resolved by changing "smaller" to "thinner."
417	National Security Agency - Information Assurance Directorate		G				Overall, we are concerned by the amount of attention paid to various removable hardware token solutions compared to the level of discussion surrounding the embedded tokens. We believe that due to the costs, usability, lack of commercial market viability, and incompatibility of using hardware tokens, most agencies are going to opt for an embedded solution, and the comparative lack of guidance in this area will make this solution more difficult to implement. We recommend solutions be usable, commercially sustainable, and secure.	The publication should focus more on the commercial market-leading solutions of embedded cryptographic tokens. See next comment for recommended additions to the embedded token description.	Resolved by comment #418.
418	National Security Agency - Information Assurance Directorate		G				We believe that the embedded token description does not contain enough nuance regarding variations in solutions. The two discussed options for embedded tokens are hardware cryptographic modules and software cryptographic modules. We believe that many mobile products offer a middle ground with hardware-backed cryptographic modules which implement roots of trust compatible with much of the draft SP800-164.	Additional exposition could be added to 3.3.2: including references to the draft SP800-164, additional nuance regarding hardware-backed cryptographic modules (see comment #2), renewal mechanisms, relative security of tokens stored in the OS/kernel to application-based tokens, methods of key authorization (user-based and app-based), exportability requirements, role of management systems, and behavior upon failed device access attempts.	Resolved by adding some additional text regarding security controls for mobile devices.
419	Global Platform	Gil Bernabeu				3.3	GlobalPlatform is supporting deployment of smart card application in different form factor such as UICC or SIM , secure memory card and embedded SEs. Different Smartphone available in the market are currently equipped with an embedded SE. A specific sub section on 3.3.2 (similar to § 3.3.1.2) will be useful		Noted. These technologies are sufficiently covered within the Embedded Cryptographic Module section.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
420	Global Platform	Gil Bernabeu				3.3.2	GlobalPlatform is also supporting deployment of Trusted Execution Environment (TEE). The TEE is a secure area that resides in the main processor of a mobile device and ensures that sensitive data is stored, processed and protected in a trusted environment. The TEE offers the safe execution of authorized security software, known as 'trusted applications' enabling it to provide end-to-end security by enforcing protection, confidentiality, integrity and data access rights. This environment requires secure hardware capabilities associated with a APIs and specific behavior This environment is a good solution to store application managing the derived credential. A specific section at the end of 3.3 will be adequate to introduce this potential solution . TEE fully supports the section 3.4.1 regarding to Hardware implementations		Resolved by comment #419.
421	Global Platform	Gil Bernabeu				3.4.2	One specific feature of the TEE is to provides with a Trusted UI. A 'trusted user interface' (trusted UI) is defined as a specific mode in which a mobile device is controlled by the TEE, enabling it to check that the information displayed on the screen comes from an approved trusted application (TA) and is isolated from the rich OS. The trusted UI enables the information to be securely configured by the end user and securely controlled by the TEE by verifying the user interface of a mobile device.		Noted.
422	Exponent						The document states: "It may be noted that this guideline doesn't preclude the issuance of multiple Derived PIV Credentials to the same Applicant on the basis of the same PIV Card. Issuing several Derived PIV Credentials to an individual, however, could increase the risk that one of the tokens will be lost/stolen without the loss being reported, or that the subscriber will inappropriately provide one of the tokens to someone else." To limit the risk associated with multiple credentials, consider limiting the total number of derived credentials given to a single individual to make fraud detection easier and limit the scope of potential insider threat attacks (where a user intentionally provides one or more derived credentials to unauthorized users.)	No action. The note in the document informs the agencies of the risk. Because the Agency must approve all issued derived credentials, the ID Management System (IDMS) at the Agency will need to be able to keep track of the number of credentials issued and take action if they so desire. 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).	Noted.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
423	Exponent						Remote derivation of credentials presents the opportunity for a credential to be generated without the PIV Card holder's knowledge (e.g., malware on a computer with a PIV card inserted into it) or derivation using a stolen credential before the credential is reported stolen. Consider either limiting the validity period of remotely derived credentials (to limit the potential exposure time) or provide an out-of-band notification to the PIV Card holder that a new credential was derived using their credential. (Note: Out-of-band communication (letter, email, SMS, etc.) is used for LOA-3 credentials in SP800-63-2. See Table 3 on Page 34.)	No action. Computer security measures and the fact that the Applicant must demonstrate possession of the PIV Card via the PIV-AUTH authentication mechanism limit the exposure to this type of attack. The IDMS will also have a record of the derived credentials.	Noted.
424	Exponent						The publication allows the storage of LOA-3 derived credentials in both hardware cryptographic tokens as well as software. SP800-63 currently allows LOA-3 credentials to be stored in software, as long as appropriate authentication measures are taken. However, modern attack techniques on computers and mobile phones can give attackers access to these tokens without needing multiple authentication factors and thus they may not meet the requirements for LOA-3. Consider evaluating the security of software-stored credentials in light of SP-800-63 and SP-800-124 and current technology to determine if software tokens meet the requirements of LOA-3. This is especially important for tokens to be stored on mobile devices, which to-date have had difficulty meeting the same security standards as traditional, non-mobile computing devices and the standards described in SP800-124.	No action. NIST will rely on SP800-63 and SP800-124 to specify the required security for the devices on which the derived credentials will be stored. App vetting will also be more important. Software tokens will be LOA-3 as opposed to LOA-4 (a lower level of assurance) and this may be appropriate for use in many applications and will be better than the existing systems that rely on username and password.	Noted.
32	DOJ	Jesse Henderson		15	563	3.4.1	"At LoA-4, …" - Standardize Acronym	"At LOA-4, …"	Accept.
33	DOJ	Jesse Henderson		15	572	3.4.1	"… per section 6.2.3.1 of [FIPS 201]) prior…" - Standardize Document Reference	"… per section 6.2.3.1 of [FIPS201]) prior…"	Accept.
34	DOJ	Jesse Henderson		16	580	3.4.1	"...[FIPS 201]) prior to PIN reset." - Standardize Document Reference	"...[FIPS201]) prior to PIN reset."	Accept.
35	DOJ	Jesse Henderson		16	586	3.4.2	"For software implementations (LOA-3) of…" - Using LOA-3 as an adjective, should be place in front like other LOA references	"For LOA-3 software implementations of …"	Noted. The referenced text has been deleted from the document.
36	DOJ	Jesse Henderson		17	596	Appendix A	"...Authentication key, [FIPS 201] also requires…" - Standardize Document Reference	"...Authentication key, [FIPS201] also requires…"	Accept.
37	DOJ	Jesse Henderson		17	602	Appendix A	"...Card. Neither [FIPS 201] nor [COMMON] precludes…" - Standardize Document Reference	"...Card. Neither [FIPS201] nor [COMMON] precludes…"	Accept.
38	DOJ	Jesse Henderson		18	644	B.1.2	"Section 3.1.3 of [SP 800-73Part1]." - Standardize Document Reference	"Section 3.1.3 of [SP800-73Part1]."	Accept.
39	DOJ	Jesse Henderson		19	685	B.1.2	"...in Section 4.2.1 of [FIPS 201]." - Standardize Document Reference	"...in Section 4.2.1 of [FIPS201]."	Accept.
40	DOJ	Jesse Henderson		24	808	Appendix D	"...including [FIPS201], [SP800-63] and [SP 800-73]." - Standardize Document Reference	"...including [FIPS201], [SP800-63] and [SP800-73]."	Accept.

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
43	DOJ	Edward Siewick	semantics	10	379..381	2.2	The object "the token corresponding to the Derived PIV Credential" may be misconstrued as the PIV Card. The first sentence in the subsequent paragraph, *"The Derived PIV Credential is unaffected by loss, theft or damage to the Subscriber's PIV Card,"* does perhaps correct such a mis-reading. However, a simple word change prevents it all together.	Modify the *"If the token corresponding..."* sentence to read: *"If the token containing..."*	Resolved by changing the text to read "The token containing the private key corresponding to the Derived PIV Credential...."
44	DOJ	Edward Siewick	nit	10	394	2.3	Use of terminology should be consistent.	Change "Subscriber no longer requires a derived credential" to "Subscriber no longer requires a Derived PIV Credential".	Resolved by comment #188.
45	DOJ	Edward Siewick	nit	23	782	Appendix C	Table C-1 lists PIV-specific types of Derived PIV Credentials.	Change *"Derived Credentials"* to *"Derived PIV Credentials"*.	Accept.
46	DOJ	Edward Siewick	semantics	10	398..402	2.3	The clause regarding export of private keys should be generalized to consider all methods. As written, it only pertains to methods available to the end user through the user interface. Section 3.3 (471..473) say it is practically "impossible to prevent users from making copies of software tokens or porting them to other devices." It may also be impractical to verify or prove the the private key zeroized or destroyed was actually the one issued. So there may be a need for a more absolutist statement here, that termination always requires revokation.	Change "...hardware cryptographic token *that does not permit the user to export the private key*..." to "...hardware cryptographic token *that does not permit export of the private key*..."	Resolved by changing "...hardware cryptographic token that does not permit the user to export the private key..." to "...hardware cryptographic token that does not permit export of the private key..." It can easily be verified that the private key zeroized or destroyed was actually the one issued by performing a challenge/response with the hardware token prior to zeroization or destruction. The quoted text from Section 3.3 is not relevant here since the option to not revoke if the token has been zeroized or destroyed is limited to hardware tokens. See also comment #49.
47	DOJ	Edward Siewick	semantics	11	404	2.4	This is a complex sentence. When properly parsed, it doesn't actually say what the authors intended. The objects are the records, not the tokens.	Change *"...a process that maintains a link between the Subscriber's PIV Card and the Derived PIV Credential to enable..."* to *"...a process that maintains a link between the status of the Subscriber's PIV Card and that of* the Derived PIV *Credential to enable..."*	Resolved by deleting the referenced sentence.
48	DOJ	Edward Siewick	semantics	11	414..415	2.4	Same rationale as for line 404.	Change: *"Additional methods must be employed for maintaining a linkage between the current PIV Card and the corresponding Derived PIV Credential."* to: *"Additional methods must be employed for maintaining a linkage between the status of the current PIV Card and that of the corresponding Derived PIV Credential."*	Resolved by changing the referenced sentence to "Additional methods must be employed for obtaining information about the PIV Card from the PIV Card issuer."
50	DOJ	Edward Siewick	N.B.	11	417..419	2.4	The objective of the example should be to recommend arranging an automatic referral to the authoritative data store for the PIV Card's status information. As written, the example only suggests keeping the status records for both credentials on the one database. This would require modifying the database, and modifications to the system to serve both credential management processes.	Change: *"...the linkage between the two credentials may be maintained through the common Identity Management System (IDMS) database implemented by the issuing agency."* to: *"...the linkage between the two credentials may be maintained within the Identity Management System (IDMS) database implemented by the issuing agency, or via a reference to the IDMS record."*	Resolved by changing the referenced sentence to "If the Derived PIV Credential is issued by the same agency or issuer that issued the Subscriber's PIV Card, then the Derived PIV Credential issuer may have direct access to the Identity Management System (IDMS) database implemented by the issuing agency that contains the relevant information about the Subscriber."

#	Organizatio	Commenter	Type	Page	Line	Section	Comment(Include rationale for comment)	Suggested change	NIST
54	DOJ	Edward Siewick	nit	12	467	3.3	missing word	Adjust: *"nothing here is intended to either require or prohibit emulation of PIV Card or the removable token software interface."* to: *"nothing here is intended to either require or prohibit emulation of a PIV Card or a removable token software interface."*	Accept
141	USDA Mobility PMO	Peter Cox		11-12	367-369	2.2	I believe the we need to add LOA-3 to this paragraph to be consistent with the language in section 2.1, which requires that all communications be authenticated for LOA-3.	Add the following verbiage "a LOA-3 and" Change "an" to "a"	Noted. The text in lines 367-369 already apply to certificates issued at both LOA-3 and LOA-4. It is only the text that begins “When certificate re-key or modification is performed remotely for an LOA-4 Derived PIV Credential” that does not apply at LOA-3.
142	USDA Mobility PMO	Peter Cox		12	389	2.2	To preserve the chain of trust between the PIV card and the ensure that the identity proofing and identity information stays consistent across both PIV and the derived credential, I recommend that this should be "shall" rather then "may". Which ones are required?	I recommend that this should be "shall" rather than "may" Which ones are required?	Resolved by comments #153 and #216.
143	USDA Mobility PMO	Peter Cox		12	400	2.3	Insert number 2) since you have a 1)	", or 2)"	Resolved by rewording of the sentence.
144	USDA Mobility PMO	Peter Cox		12	400	2.3	Should state "and" instead of "or"	Replace to read "destroying the token and"	Resolved by comment #277.
145	USDA Mobility PMO	Peter Cox		12	401	2.3	Insert number 3) rather than 2)	"3)"	Resolved by comment #143.
146	USDA Mobility PMO	Peter Cox		13	407	2.4	add the language: "and to maintain the chain of trust."	add the language: "and to maintain the chain of trust."	Declined. The goal in maintaining the linkage is to ensure that an individual who becomes ineligible to have a PIV Card does not continue to possess a valid Derived PIV Credential. It has nothing to do with maintaining a chain-of-trust, as chain-of-trust is defined in FIPS 201-2.