#	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.