Comment #	Part#	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change	Organization	Submitter/POC	NIST Disposition
1	1		iii	118	NPIVP Conformance Testing One year ago, there was a problem to verify and certify OPACITY's KDF that is based on SHA256 or SHA384 hash. Is it possible to verify and certify OPACITY using SHA256 or SHA384 as KDF?		*Giesecke and Devrient*	*Jatin Deshpande*	Noted - no changes requested and comment will be seperately answered (email).
2	1	References	28	1032	There's a reference to SP800-78-4 instead of SP800-78-5.		*Giesecke and Devrient*	*Jatin Deshpande*	Accepted
3	2	3., 3.2.2	14	407, 633	In table 2 the CHANGE REFERENCE DATA command is listed with command chaining. In the description of the command no command chaining is mentioned.		*Giesecke and Devrient*	*Jatin Deshpande*	Partially Accepted: Command chaining is not needed for changing PINs (global or local ones). So state that command chaining is only required if PIV Card Application supports OCC. Phrase note according to footnote 3.
4	2	3.2.2	14	591 to 595	Does this mean, that the PIV card may have additional PIN or OCC with key references others than described in part 1 table 4 that can be used for administration. This would be interesting, because some PKCS#11 middleware uses to have an admin PIN instead of the 9B key.		*Giesecke and Devrient*	*Jatin Deshpande*	Not Accepted.
5	2	A.1	40	1108 to 1119	The working example for General Authenticate with algorithm '08' (AES-128) uses length of 8 for random, whitness and calculated tokens.		*Giesecke and Devrient*	*Jatin Deshpande*	Accepted. Table has been updated to reflect 16 bytes rather than 8 bytes.
6	2	A.2	40	1120 to 1133	The working example for General Authenticate with algorithm '08' (AES-128) uses length of 8 for random, whitness and calculated tokens.		*Giesecke and Devrient*	*Jatin Deshpande*	Accepted. Table has been updated to reflect 16 rather than 8 bytes block authentication data.
7	1 and 2	4.1.5	25	790	**Missing possibility to personalize C_ICC** We suggest that there will be another container that can be written using PUT DATA, so the issuer is able to personalize the C_ICC in the field using PUT DATA command. Access condition shall be the same than the Secure Messaging Signer Certificate.		*Giesecke and Devrient*	*Jatin Deshpande*	Not accept - admin action is out of scope
1	Part 1	5.3	23	867	During the NIST Personal Identity Verification Webinar, it was said that RSA4096 key generation was very slow and unpractical. To check that statement, I did some benchmarks to compare RSA 2048 Key generation timing on the first PIV card validated by NPIVP (PIV 1.08 from Oberthur)with RSA 4096 key generation on the latest version of PIV cards (ID-One PIV 243 from IDEMIA. The result shows that today, it is faster to generate an RSA 4096 key than it was to generate an RSA 2048 key at the start of the PIV deployment 18 years ago. And since PQC migration is not before 2035 that leaves 12 years where RSA 4096 could still be used for no extra cost as it is only the key size that changes. I'll send you by email a chart that shows the probability distribution function based on Key generation time for both cards (with Mean, Standard Deviation and Variance). And RSA 4096 performances on the next generations of smart card chips to become available between now and 2035 is likely to increase by almost as much.	Add RSA 4096 in table 9 with algorithm identifier 16 (Algo ID=15 is already standardized by ANSI for ECC P-521 (see INCITS 504-1 - Table 23)	IDEMIA	*Christophe GOYET*	No changes - but defer to 800-78-5 - as is done in line 868-870. DoD tested 4K RSA algorithm to provide input for SP 800-78. It was determined that issuance is more than 90 sec per card per 4K key and that is too much time when considering the mass amount of issuance done today.

2	Part 2	3.2.2	14	600	Card Management Functions for the PUK may be out of scope for this specification, but nevertheless this specification shall not prohibit a behavior described by FIPS 201-3 that states that all commands available in contact can be available in contactless over the virtual contact interface (VCI).	Change the first sentence with "If key reference '81' is specified and the command is not submitted over the contact interface **(or the VCI)**, then the card command SHALL fail."	IDEMIA	*Christophe GOYET*		Not accepted - All commands ARE available in VCI. That does not mean, however, that all keys can be used with these commands. To allow the reset of PIN wirelessly (over VCI) is not security-wise.
3	Part 2	A.2	41	1133	Table 23 second row provides the following response: '7C 0A 80 **08** 88 77 66 55 44 33 22 11 90 00'.But the length of the encrypted nonce depends on the cipher block size of the algorithm of the 9B key. 16 for AES keys. (was 08 for TDES and that 08 was not changed when this example was updated with an AES key (9B 08)	change the second row response with '7C 0A 80 **10** 88 77 66 55 44 33 22 11 90 00'	IDEMIA	*Christophe GOYET*		Accept
4	Part 2	A.3	41	1138	(i.e., key reference '9A' or '9E'): 9E is not PIN protected, so a sucess will authenticate only the card , and not the PIV card holder as stated in the header of this A.3 section.	change (i.e., key reference '9A' or '9E') with (i.e., key reference '9A')	IDEMIA	*Christophe GOYET*		NOT ACCEPT
5	Part 2	4.1.4	25	789	To allow the use of the PIV Secure Messaging for card management operations that need 256 bit channel strength (like card personalization and remote post issuance update), could you please allow the cipher suite CS6 that is the same as CS7 but with a ECC P-521 Secure Messaging Key Establishement Key. Algo ID for ECC P-521 is already standardized to 0x15 by ANSI 5004-1 (to which NIST contributed in the past) as well as CS6.	Add a column in table 14 to offer a PIV Secure messaging with 256 bit channel strength to allow post issuance update of Digital Signature Key and or Key Management Key with ECC P-384	IDEMIA	*Christophe GOYET*		Not Accepted. See Table 14. The secure channel already supports 192-bit channel strength, which is enough for ECC P384. We do not intend to add ECC P521.
1	1	3.1.6	8	493	Switch order to "BIO-A or BIO" to match the order in the statement.	Modify: "The facial image data object is used for automated facial authentication in attended and unattended modes (e.g., BIO or BIO-A), as well as automated facial authentication for PIV reissuance and verification data reset." To: "The facial image data object is used for automated facial authentication in attended and unattended modes (e.g., **BIO-A or BIO**), as well as automated facial authentication for PIV reissuance and verification data reset."	Google	Rachelle Summers		Accept
2	1	3.1.6	8	493	Automated facial authentication is specified to work in attended and unattended modes for facial image data objects, but that level of specificity is not indicated for PIV reissuance and verification data reset.	Clarify if automated facial authentication for PIV reissuance and verification data reset is for attended, unattended or both.	Google	Rachelle Summers		Partial accept. Reissuance requires BIO-A, reset can be done via OCC-AUTH remotely. Hence, the request cannot be simply stated. So add "according to FIPS 201-3"

3	1	5.1.1	22	824	Modify sentence to explain that the fingerprints used for OCC should be imaged separately.	Modify: "The fingerprints used for OCC MAY be taken from the full set of fingerprints collected for PIV background investigations and SHOULD be imaged from fingers not imaged for off-card one-to-one comparison." To: "The fingerprints used for OCC MAY be taken from the full set of fingerprints collected for PIV background investigations and SHOULD be imaged from fingers ~~**not imaged for off-card one-to-one comparison**~~. **The fingerprints used for OCC should be imaged separately from that for off-card one-to-one comparison**."	Google	Rachelle Summers		Not accept
4	1	REF	26	1003	Please provide a link to the specific document being referenced as written OR update the [MRTD] reference contents to reflect the 9303 document series from the link below. No Eighth Edition 9303 series document exists with a title that is under the [MRTD] reference as currently written. See: https://www.icao.int/publications/pages/publication.aspx?docnum=9303). Part 3 of the Machine Readable Travel Documents is "Part 3: Specifications Common to all MRTDs".	Include accurate title and URL to specific document for [MRTD] reference OR modify reference to reflect the documents available at https://www.icao.int/publications/pages/publication.aspx?docnum=9303.	Google	Rachelle Summers		Accept
5	1	B.1.2	44	1202	"Signed Nonce" implies both the nonce and its signature when all that is returned is the signature.	Modify: "Signed Nonce Returned" To: "**Nonce Signature** Returned"	Google	Rachelle Summers		not accept -- No changes needed. Microsoft and yubico have the same 'understanding' of signed nonce – https://www.yubico.com/resources/glossary/what-is-certificate-based-authentication/ https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/how-it-works-authentication
6	1	B.1.3	44	1202	"Signed Nonce" implies both the nonce and its signature when all that is returned is the signature.	Modify: "Signed Nonce Returned" To: "**Nonce Signature** Returned"	Google	Rachelle Summers		Disagree -- see previous resolution.
7	2	3.2.2	14	633	Modify "Command Syntax" table to match "Command Syntax" table on line 582 in order to support chaining for OCC.	Modify: "'00' or '0C' for secure messaging" To: "**'00' or '10' indicating command chaining"** [new line] "**'0C' or '1C' for secure messaging**"	Google	Rachelle Summers		Noted. No changes. OCC reset is not specified because it is a card management operation. All other key refs (PIN, Global PIN, PUK) fit in one command - no chaining needed.
8	2	3.2.2	14	634	Specify which parameter(s) are needed for change OCC in P2 section of "Command Syntax" table.	Explicitly indicate in P2 section of table which parameter(s) should be used for change OCC.	Google	Rachelle Summers		Noted. No changes. OCC reset is not specified because it is a card management operation.

9	2	3.2.4	18	701	Include additional best practice information on Exponentiation below Table 7.	Add note below Table 7: "**Exponentiation SHALL NOT be allowed on keys 9A, 9C and 9E. These are essentially all authentication keys and in no case is it valid to use exponentiation for in lieu of a digital signature for authentication**."	Google	Rachelle Summers		Agree to add 1st sentence only.
10	2	3.2.4	18	705	Expand Challenge and Response tag data object descriptions to cover symmetric and asymmetric key use cases.	Modify: "The Challenge (tag '81') contains clear data (byte sequence), which is encrypted by the card." To: "**When symmetric keys are used, the Challenge (tag '81') contains clear data (byte sequence) which is encrypted by the card and the Response (tag '82') contains either the decrypted data from tag '80' or the encrypted data from tag '81'.**"	Google	Rachelle Summers		Not accept. In addition, we are deprecating SYM-CAK and it does not make sense to specifically call it out now, when it will be retired soon because of low/non use in federal government.
11	2	3.2.4	18	706	Expand Challenge and Response tag data object descriptions to cover symmetric and asymmetric key use cases.	Modify: "The Response (tag '82') contains either the decrypted data from tag '80' or the encrypted data from tag '81'." To: "**When asymmetric keys are used, the Challenge (tag '81') contains data objects in the dynamic authentication template (tag 7C) and the Response (tag '82') contains the signature of the data objects in the dynamic authentication template as described in section A.4 'Signature Generation With the Digital Signature Key'..**"	Google	Rachelle Summers		Not Accept. to decline. In addition, we are deprecating SYM-CAK and it does not make sense to specifically call it out, when it will be retired soon because of low/non use in federal government.
12	2	REF	39	1085	The link for reference [SECG] is missing.	Add link to [SECG] reference: https://www.secg.org/sec1-v2.pdf.	Google	Rachelle Summers		Accepted
1	1	3.4	26	701	The term "persistent" is realtive, this publication would seem to mean it persists for the lifetime of the PIV card, but other organizations could use a UUID to identify a human subscriber for the subcriber's lifetime	Recommend including the type of persistence referenced (e.g., persistent over the life of a single card issuance)	GSA FPKI	FPKIPA Team		see comment below.
2	1	3.4.2	27	722	Cardholder UUID acronym is only one letter off from CHUID	Recommend changing verbiage to be more differentiating such as using "Subscriber UUID" as opposed to "cardholder UUID"	GSA FPKI	FPKIPA Team		No changes. These terms are well understood and have been used extensively in NIST and other publications.

										cardholder UUID is not in TIG SCEPACS, so proposed resolution is not applicable. Instead:Noted, but add footnote (see next para). The CHUID historically has an Person Identifier (PI) field, which is being used by some department/agencies. The cardholder UUID has been ask for by department/agencies in prior revision of FIPS 201. It has been marked as optional so that departments/agencies who feel the scope of the identifier is a risk thus can choose not to implement it. Add the following footnote: The identifier should only be scoped to identify a given cardholder over the lifetime of the PIV card and Derived PIV credential issued during the cardholder's piv eligibility. The identifier should not be scoped for any other purposes.
3	1	3.4.2	27	723	It may not be recommended to place the cardholder UUID in the CHUID as it is a free-read element and may result in the lost of an identifer that could be considered PII, or it could be an identifier assoiciated with a sensitive persona	Recommend disallowing inclusion of cardholder UUID in CHUID object	GSA FPKI	FPKIPA Team		
4	1	3.4.2	27	725	FPKI is interested in a lifetime (persistent) subscriber UUID (per issuer) that is interoperable between agencies and would have enough uniqueness to account for all federal employees and contractors.	Recommend potentially mandating cardholder UUID (or subscriber UUID) as an element to be included in the PIV-auth certificate (FPKI profiles can be updated as such), and also recommend standardizing on a version 4 UUID from RFC 4122 as it provides enough uniquness for all Federal human resources and limits the potential for collisions	GSA FPKI	FPKIPA Team		Accept in part: The identifier should be optional and scoped to identify a PIV credential holder during the cardholder's PIV eligibility. The identifier should not be scoped for any other purposes.