Comment #	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change	NIST Resolution
IDEMIA						
1	3.1	5	301	It is stated that "All cryptographic algorithms employed shall provide at least 112 bits of security strength." However tables 9 and Table 10 both list RSA 1024 as supported cryptographic algorithms for Retired Key Management Keys even after 2030. RSA 1024 provides only 80 bits of security. Is RSA 1024 currently used by Federal Agencies ? Can it be removed from the list of supported algorithms?	Remove RSA 1024 throughout the document	Not accept. The algorithm is associated with retired key management keys and, as such, is needed to decrypt older cybertexts that have been previously encrypted with the key/algorithm combo.
2	3.2.1	7	354	the Probabilistic Signature Scheme (PSS) padding is defined in [PKCS1]. However PIV Test Runner Version 5.0.1 - 20200212-0308 (the latest one) reject the PSS signatures with the the cryptic message below. Could NIST specifies any additional requirements for RSA PSS on top of PKCS1 to ensure better interoperability: Message from Test Runner: Signature verification returned: false Digital signature not verified. Test failed. Note to card vendors: Signature verification can fail if the original signature was not generated using Encoded Signed Attributes that were DER encoded. The order of the on card ESA attributes does not determine the order used by the tester signature generation. Reading of the ESA attributes into a DER format may change the order. For compatibility with all systems the on card ESA ordering should match the DER ordering.	Provide additional references for RSA PSS on top of PKCS1 to address the issue of DER Ordering.	Noted. This will be further resolved in SP 800-85A-5.
3	6.2, table 9	13	438	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)	Noted. We have collaborated with DoD on the performance of 4K RSA . The key generation time is 90 seconds, which is too much when considering the large population of PIV cards to be issued/re-issued on a daily basis. 4K RSA may be reconsidered in a later version of 800-73, but more importantly, PQ algorithms take precedence.
4	7	20	476	For Cipher Suite 7, Encryption and Decryption is said to use AES CBC 256. This is correct but could be misleading the user into thinking the encryption provides 256 bit of channel strength. Only 192 bit of channel strength are provided even if the algorithm itself is AES-256. This is because of the size of the PIV Secure Messaging Key Establishment KEy (ECC P-384 intead of P-521). Achieving a true 256 bit of channel strength is very easy without changing the way the PIV Secure Messaging is established, or the session keys established. You just need to use an ECC P-521 as the PIV Secure Messaging Key Establishement Key. Performances are the same and security significantly higher, for no extra cost as most smart card chip these days do support ECC P-521. PIV Secure Messaging with ECC P-521 has been sucessfully supported for Card Management Operations for over 5 years by some PIV cards widely deployed to US Federal Agencies (including to NIST) for instance by the US Access Program.	Add ECC P-521 in Table 9 as an option to provide a real 256 bit strengh in the PIV secure Messaging at no extra cost. Use Algo ID=15 as already standardized by ANSI for ECC P-521 (see INCITS 504-1 - Table 23)	Not accepted. The secure channel strength is 192 bit per Table 18 of part 2 in SP 800-73-5. This is equivalent to ECC P-384. SP 800-73 states: If the PIV Card Application supports the VCI and either the digital signature key ('9C'), the key management key ('9D'), or one of the retired key management keys ('82' – '95') is an ECC (Curve P-384) key, then PIV Card Application SHALL only support cipher suite CS7. See also SP800-57 Part 1 Table 2 for comparable security strength, which this document is aligned with. There is also no plan to include ECC P-521.
HID						
1	6.2	13	438	Table 9 should include an algorithm identifier for RSA 4096-bits as table 2 mentions this algorithm as allowed. This would help PIV Card implementers integrate the right identifier if they intend to support this key size in addition to others. It would prevent interoperability issues in the future	Table 9: Add a line '04' : RSA 4096 bit modulus, 65537 ≤ exponent ≤ 2256 - 1. (04 is provided as an example).	See previous resolution in cell 6G
Canonical (Dimitri Ledkov						

				Ed25519 is now featured in FIPS 186-5, but is not present in the PIV Standards hence PIV smartcards cannot implement it over the protocol (despite having hardware support). For example Yubikey offers Ed22519 over FIDO2 and OpenPGP smartcard interfaces, but not over PIV. Adding to Ed25519 for the PIV Standards would help a lot the wider public, as hardware compliant with PIV Standards is widely used for generic purposes (storing CA certificates by vendors for TLS, UEFI SecureBoot, and any other keys securing software supply chain).	Please consider updating PIV Standards to include Ed25519.	Not accept. We keep the current set of algorithms. Newer ones, like Ed22519, take time to build support. Rather than focus Ed22519, the next update will be for PQ-based algotihms.
Jason Stone DoD PKI portfolia managerment office						
			Table 1 and 9	The reason for my concern is that PfMO has had inquiries to approve tokens using PIV applets. SIPRNet is pushing for RSA-4096 user key lengths. I understand that the Homeland Security and NIST are concerned with Unclassified Federal implementations, although the conditions referenced above are excluding this capability as a possibility from use in other applications. How can we as Federal partners allow for expanded use of the same products and build stronger solutions? Many of the FIPS 140 chip certifications (or Common Criteria) verify the greater algorithm capabilities are available at the chip level.		Not accept - see G6.