#	Organization	Commentor	Type	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	Resolution/Response
1	Oberthur	C. Goyet	T	14		Table 7-1	This table lists some minimum CAVP validation requirements for signature generation that cannot be met by the PIV card alone because neither hashing nor message formatting for signature is performed by the card. According to SP800-73-4 part 2 line 606, "data to be signed is expected to be hashed off card".	Separate the CAVP requirements applicable to the PIV card from the ones applicable to the PIV client application programming interface.	Noted. For signature generation, Section 7 of SP800-78-4 specifies “186-4 RSASP1 component” for RSA and “186-4 ECDSA Signature Generation component” for ECDSA. The specified component testing aligns with the functionality of the PIV Card Application and does not involve hashing or padding.
2	Oberthur	C. Goyet	t	13		Table 6.2	SP800-73-4 took the ANSI 504 secure messaging CS4 but replaced AES 192 with AES 256 because AES 192 is not in the NSA suite B. Following the same logic shouldn't algorithm)A (i.e. AES 192) be removed from 800-78-4 ? This algorithm makes the key management more complex because the size of the key is not a multiple a 16, and form a performance standpoint, AES128, AES192 and AES 256 take about the same time in a smart card (difference is less than 10%)	Remove AES192 that is not in the NSA Suite B	Declined. In SP 800-78-4, AES 192 is only permitted for use for symmetric Card Authentication key and the PIV Card Application Administration key, neither of which is intended to provide interagency interoperability. There is no requirement for PIV Cards, Card Management Systems, or relying parties to be able to process this algorithm, except at agencies that have particularly chosen to use this algorithm and key size. Removing this key size option would create an unnecessary burden for any agency that may have already deployed PIV Cards that use AES 192 for one of these keys.