#	Organization	Commentor	Type	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
C-1	CertiPath	Spencer	E	1	205 & 207	1.2	The document is referred to as a "recommendation" in two places here. I believe that this is a misnomer. These are not recommendations, rather they are requirements.	Replace the word recommendation with a more appropriate word: "document," "requirement," "publication" or a like term would appear to be more appropriate.	Resolved by capitalizing “Recommendation” in order to be consistent with other NIST Special Publications, such as SP 800-38B and SP 800-56A Revision 2.
C-2	CertiPath	Spencer	T	3	259-260	2	The PIV Secure Messaging key is not specified by FIPS 201. FIPS 201 actually defers to SP 800-78 and SP 800-73 to define this.	Recommend the reference to the PIV Secure Messaging key should not be a bullet under this paragraph, but defined separately. e.g. "In addition, SP 800-73-4 defines an asymmetric Card Validation Certificate (CVC) key, supporting the establishment of session keys for use with secure messaging."	Resolved by changing the sentence preceding the bulleted list to: “The PIV cryptographic keys specified in FIPS 201 and SP 800-73 are:”
C-3	CertiPath	Spencer	E	4	281-282	2	The sentence as written is misleading/incomplete.	Recommend the word "respectively" be added to the end of this sentence as follows: "FIPS 201 requires CAs and Online Certificate Status Protocol (OCSP) responders to generate and distribute digitally signed certificate revocation lists (CRL) and OCSP status messages, respectively."	Accept.
C-4	CertiPath	Spencer	T	4	283 & 285	2	The use of the term "revocation mechanisms" to describe CRLs and OCSP status messages is incorrect. This term is not used anywhere else and does not appear to be a term of art. In Section 4, these "mechanisms" are referred to as "formats for distribution of certificate status information." Which would appear to be a more accurate label	Recommend the term "revocation mechanisms" be replaced with a more accurate term. e.g. "These certificate status mechanisms support validation of the PIV Card, the PIV cardholder, the cardholder's digital signature key, and the cardholder's key management key. "The signed certificate status mechanisms specified in FIPS 201 are:"	Accept.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
C-5	CertiPath	Spencer	T	4	286	2	The statement "X.509 CRLs that specify the status of a group of X.509 certificates" is inaccurate. The CRL is a list of revoked certificates. It does not otherwise indicate a certificate's status (which could be expired, for example).	Revise this bullet to accurately reflect the function of a CRL. e.g. "X.509 CRLs that list the X.509 certificates that have been revoked. . ."	Declined. RFC 5280 notes that "Each CRL has a particular scope. The CRL scope is the set of certificates that could appear on a given CRL." While it is true that a CRL consists of a list of the serial numbers of the unexpired certificates within the scope of the CRL that have been revoked, a CRL provides the revocation status of all unexpired certificates within its scope. A CRL specifies that an unexpired certificate within its scope is revoked by listing its serial number and that it is not revoked by not listing its serial number.
C-6	CertiPath	Spencer	T	5	311	3.1	See comment #2. FIPS 201 does not define the keys for secure messaging. These are defined by SP 800-73 and this document. Rather the sixth class of keys is the optional PIV Card Application Administration Key, which is not mentioned here at all - by design? It is not for use by the PIV Cardholder. If so, then there are five credentials defined by FIPS 201 for use by the cardholder and an additional secure messaging key defined by SP 800-73.	Revise this listing to remove the secure messaging key to a separate paragraph following the list. e.g. "FIPS 201 specifies five different classes of cryptographic keys to be used as credentials by the PIV cardholder: + the mandatory PIV Authentication key; + the mandatory asymmetric Card Authentication key; + an optional symmetric Card Authentication key; + a conditionally mandatory digital signature key; and + a conditionally mandatory key management key In addition, SP 800-73-4 defines an optional asymmetric card verifiable certificate (CVC) key to establish session keys for secure messaging."	Resolved by changing the sentence at the beginning of Section 3.1 to "FIPS 201 and SP 800-73 specify specifies six different classes of cryptographic keys to be used as credentials by the PIV cardholder:"
C-7	CertiPath	Spencer	T	6	341	3.1 (Table 3-1)	The table does not include the "intermediate CVC" which is part of the secure messaging key function and is not limited to ECDH (according to the information below).	Recommend revising Table 3-1 to accurately portray the two components of the secure messaging key.	SP 800-78: Declined. The Intermediate CVC acts in a similar role as an X.509 CA certificate. So, it is not a component of the secure messaging key, but rather simply a signed data object that is stored on the card. As such, information about the Intermediate CVC is appropriately specified in Section 3.2.1. Table 3-1 only lists keys where the private (or secret) key is stored on the PIV Card.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change	NIST Response
IG-1	InfoGard	SWeymann	G	44	1090	A.5.2.1 of Revised Draft SP 800-73-4 Part 2	In existing validations, use of ECC CDH required the CAVP Component Validation List ECC CDH Shared Secret certificate. Assuming that NPIVP will require a CAVP Key Agreement Scheme SP 800-56A validation if the Secure Messaging option is supported, that validation is inclusive of the ECC CDH primitive. It should not be necessary for vendors to separately test the CVL ECC CDH primitive if the module has the appropriate complete EC DH key agreement scheme (KAS) validation. The current SP 800-73-4 draft does not address this point one way or ther other, but vendors preparing for compliance are already asking. This comment is intended to avoid future confusion.	Please include a statement in Part 2 covering this topic - Section A.5.2.1 may be the best choice. "All other procedures required to complete the key agreement are performed by the cardholder's client application and its associated cryptographic module. Cards that support ECC CDH with the PIV KMK shall obtain CAVP CVL ECC CDH or KAS EC DH validation."	Declined. The Cryptographic Algorithm Validation Program (CAVP) testing requirements in Section 7 of SP 800-78-4 is aligned with the functionality of each key that may be present within the PIV Card Application. Within CAVP testing for the SP 800-56A Section 5.7.1.2 ECC EDH primitive component is distinct from testing for the OnePassDH key agreement scheme using ECC. Similarly, the 186-4 RSASP1 component and SP 800-56B RSADP component are distinct from each other as well as from full RSA signature testing.
IG-2	InfoGard	SWeymann	T	43	1048	A.5.1 of Revised Draft SP 800-73-4 Part 2	The function of GENERAL AUTHENTICATE with the PIV KMK with an RSA key is the SP 800-56B Section 7.1.2 RSADP operation. This operation continues to be a source of misunderstanding by CMVP reviewers in the PIV card FIPS 140-2 validations, who in the recent past required this to be described as establishing a key into the module. The purpose of the operation is key decryption; it is NOT to establish a key into the module. Please identify this operation specifically as SP 800-56B Section 7.1.2 RSADP in A.5.1 or a subsection.	At approximately line 1059: "The role of the on-card KMK private RSA transport key is to decrypt the sender's symmetric key on behalf of the cardholder and provide it to the client application cryptographic module. This operation is the RSA decryption primitive (RSADP) as specified in SP 800-56B Section 7.1.2. The RSADP operation may be used in the Approved mode provided the implementation has a CAVP validated RSADP or RSA signature implementation." [Note that the primitive described by RSADP is part of the RSA signature process. CAVP validation of RSADP is now available but it should not be necessary to separately test if RSA signature is validated.]	Resolved by IG-1.