FIPS 201 Evaluation Program
Attestation Form for Electronic Personalization (Product)

This form serves to assert that the offering being submitted for FIPS 201 conformance evaluation is accurately meeting the requirements stated in the Standard.

Applicant Information

Company Name	

Product/Service Information

Name	
Part Number	
Hardware Version	
Software Version	
Firmware Version	

Lab Specific Information

Approval Procedure Version	12.0.0

Requirements being attested to:

Identifier #	Requirement Description	Source
EP.1	To activate the card for personalization or update, the Application Administrator shall be authenticated to the PIV Card using a challenge response protocol which requires the use of cryptographic keys stored on the card. The authentication procedure shall be in accordance with SP 800-73-1.	FIPS 201-1, Section 4.1.6.2 SP 800-73-1, Appendix B
EP.2	When cards are personalized, card management keys shall be set to be specific to each PIV Card.	FIPS 201-1, Section 4.1.6.2
EP.3	The PIV Card shall include the following objects as defined in SP 800-73-1: • Card Capabilities Container • CHUID • PIV Authentication Key Pair • Biometric Fingerprints • Security Object	FIPS 201-1, Section 4.2
EP.4	The PIV Card may include the following objects as defined in SP 800-73-1. • Biometric Facial Image • Printed Information • Digital Signature Key Pair • Key Management Key Pair • Card Management Key • Card Authentication Key Pair	Derived
EP.5	If the device generates cryptographic keys or performs signing operations, it shall be validated to FIPS 140-2 with an overall Security Level 2 (or higher).	FIPS 201-1, Section B.4

EP.6	Two fingerprint templates shall be stored on the PIV Card. These shall be prepared from images of the primary and secondary fingers as specified in FIPS 201.	SP 800-76-1, Section 3.3.1
EP.7	When facial imagery is stored on the PIV Card, only one image shall be stored. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-76-1, Section 5.2
EP.8	The personalized card shall be tested by the SP 800-85B test tool for data format compliance.	Derived
EP.9	Data objects populated on personalized PIV cards shall be stored in the appropriate containers according to SP 800-73-1, Appendix A, and should contain all appropriate tags and lengths for each element in the object.	Derived
EP.10	Part 3 conformant cards shall return all the Tag-Length-Value (TLV) elements of a container in the physical order listed for that container in this data model.	SP 800-73-1, Appendix A
EP.11	The CCC shall contain the mandatory BER-TLV fields as specified and identify the registered data model number 0x10.	SP 800-73-1, Appendix A
EP.12	The CHUID on a PIV card shall meet the following requirements: • The length of the CHUID is indicated in BER-TLV format, identified by tag 0xEE. • The Federal Agency Smart Credential Number (FASC-N) shall be consistent with the Technical Implementation Guidance Smart Card Enabled Physical Access Control System (TIG SCEPACS) Option for “System Code || Credential Number” to establish a credential number space of 9,999,999,999 credentials. • The Global Unique Identifier (GUID) field must be present, and may include either an issuer assigned IPv6 address or be coded as all zeros. • The Expiration Date is tagged 0x35 and value is within the next five years. This field shall be 8 bytes in length and shall be encoded as YYYYMMDD.	SP 800-73-1, Section 1.8.3
EP.13	The fingerprint buffer specifies the primary and secondary fingerprints within Tag value 0xBC.	SP 800-73-1, Appendix A
EP.14	The fingerprint template length shall not exceed 4,000 bytes.	SP 800-73-1, Appendix A
EP.15	The facial image is preceded with tag value 0xBC *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-73-1, Appendix A
EP.16	The facial image length shall not exceed 12,704 bytes *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-73-1, Appendix A

EP.17	The message digest produced as a result of a hash function on the contents of a data object buffer shall be identical to that data object's message digest contained in the security object.	Derived
EP.18	The CBEFF structure must comply with SP 800-76 Table 7, "Simple CBEFF Structure". Lengths of the biometric data must be less than 4,000 and 12,704 bytes for the fingerprint and facial image, respectively.	SP 800-76-1, Section 6
EP.19	Data objects populated on personalized PIV cards shall be stored in the appropriate containers according to SP 800-73-1, Appendix A, and should contain all appropriate tags and lengths for each element in the object.	SP 800-76-1, Section 6
EP.20	The Patron Header Version of the CBEFF Patron Format shall be 0x03.	SP 800-76-1, Section 6
EP.21	The biometric data block is digitally signed but not encrypted, and this shall be reflected by setting the value of the Signature Block Header (SBH) security options field to b00001101.	SP 800-76-1, Section 6
EP.22	For fingerprint and facial records, the Biometric Data Block (BDB) Format Owner shall be 0x001B denoting M1, the INCITS Technical Committee on Biometrics.	SP 800-76-1, Section 6
EP.23	For the mandatory fingerprint template on the PIV card, the BDB Format Type value shall be 0x0201. For the optional facial image on the PIV card, the BDB Format Type value shall be 0x0501.	SP 800-76-1, Section 6
EP.24	The Creation Date in the PIV Patron Format (see Row 7 in Table 8 of SP 800-76-1) shall be the date of acquisition of the parent sample, encoded in eight bytes using a binary representation of "YYYYMMDDhhmmssZ". Each pair of characters (for example, "DD") is coded in 8 bits as an unsigned integer where the last byte is the binary representation of the ASCII character Z which is included to indicate that the time is represented in Coordinated Universal Time (UTC). The field "hh" shall code a 24 hour clock value.	SP 800-76-1, Section 6
EP.25	The Validity Period in the PIV Patron Format (Row 8 in Table 8 of SP 800-76-1) contains two dates.	SP 800-76-1, Section 6
EP.26	Biometric Type field within the PIV Patron Format shall be 0x000008 for fingerprint template and shall be 0x000002 for facial images. The value for other biometric modalities shall be that given in CBEFF, 5.2.1.5. For modalities not listed there the value shall be 0x00.	SP 800-76-1, Section 6
EP.27	For the mandatory fingerprint template on the PIV card, the CBEFF Biometric Data Type encoding value shall be b100xxxxx, which corresponds to biometric data that has been processed. For the optional facial image on the PIV card, the CBEFF Biometric Data Type encoding value shall be b001xxxxx.	SP 800-76-1, Section 6
EP.28	For all biometric data whether stored on a PIV card or otherwise retained by agencies the quality value shall be a signed integer between -2 and 100 per the text of INCITS 358. A value of -2 shall denote that assignment was not supported by the implementation; a value of -1 shall indicate that an attempt to compute a quality value	SP 800-76-1, Section 6

	failed. Values from 0 to 100 shall indicate an increased expectation that the sample will ultimately lead to a successful match. The zero value required by FACESTD shall be coded in this CBEFF field as -2.	
EP.29	The Creator field in the PIV Patron Format contains 18 bytes of which the first K <= 17 bytes shall be ASCII characters, and the first of the remaining 18-K shall be a null terminator (zero).	SP 800-76-1, Section 6
EP.30	The Data Type Encoding field in the PIV Patron Format shall contain the 25 bytes of the FASC-N component of the CHUID identifier.	SP 800-76-1, Section 6
EP.31	The “Reserved for future use” field in the PIV Patron Format shall contain 0x00000000.	SP 800-76-1, Section 6
EP.32	Both finger’s template records shall be wrapped in a single CBEFF structure prior to storage on the PIV card.	FIPS 201-1, Section 4.4.2
EP.33	The fingerprint templates stored on the card are compliant to the MINUSTD profile specified in SP 800-76-1, Table 3.	SP 800-76-1, Section 3.3.2
EP.34	The Format Identifier of the General Header Record shall be 0x464D5200.	SP 800-76-1, Section 3.3.2
EP.35	The Version Number of the General Header Record shall be 0x20323000.	SP 800-76-1, Section 3.3.2
EP.36	The length of the entire CBEFF wrapped record shall fit within the container size limits specified in SP 800-73-1.	Derived
EP.37	Both of the two fields ("Owner" and "Type") of the CBEFF Product Identifier shall be non-zero.	SP 800-76-1, Section 3.3.2
EP.38	The two most significant bytes of each of the two fields ("Owner" and "Type") of the CBEFF Product Identifier shall identify the vendor, and the two least significant bytes shall identify the version number of that supplier's minutiae detection algorithm.	SP 800-76-1, Section 3.3.2
EP.9	The Capture Equipment Compliance of the General Record Header shall be 1000b.	SP 800-76-1, Section 3.3.2
EP.40	The Capture Equipment ID of the General Record Header is greater than zero.	SP 800-76-1, Section 3.3.2
EP.41	The width on Size of Scanned Image in X Direction shall be the larger of the widths of the two input images. Similarly, the height on Size of Scanned Image in Y Direction shall be the larger of the heights of the two input images.	SP 800-76-1, Section 3.3.2
EP.42	The Number of Views of the General Header Record shall be 2.	SP 800-76-1, Section 3.3.2
EP.43	The Reserved Byte of the General Header Record shall be 0.	SP 800-76-1, Section 3.3.2
EP.44	The View Number of the Single Finger View Record shall be 0.	SP 800-76-1, Section 3.3.2
EP.45	The Impression Type of the Single Finger View Record shall be either 0 or 2.	SP 800-76-1, Section 3.3.2

EP.46	The quality value of captured fingerprint images shall be computed using NFIQ and reported as Q = 20(6-NFIQ).	SP 800-76-1, Section 3.3.2
EP.47	The Number of Minutiae of Single Finger View Record is between 0 and 128.	SP 800-76-1, Section 3.3.2
EP.48	Fingerprint templates shall be limited to minutiae of types "ridge ending" and "ridge bifurcation" unless it is not possible to reliably distinguish between a ridge ending and a bifurcation, in which case the category of "other" shall be assigned and encoded as 00b.	SP 800-76-1, Section 3.3.2
EP.49	If used by the Product, the integrated template generator shall be certified by NIST as conformant to FIPS 201 and related documents.	Derived
EP.50	The mandatory value for Extended Data Block Length for MINUSTD template shall be zero.	SP 800-76-1, Section 3.3.2
EP.51	All facial images must conform to the requirements in SP 800-76-1 Table 6, "INCITS 385 Profile for PIV Facial Images." *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-76-1, Section 5.2
EP.52	If facial imagery is stored on the PIV card, the length of the entire record shall fit within the container size limits specified in SP 800-73. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	Derived
EP.53	The spatial resolution of the facial image shall be such that the width of the head shall be at least 240 pixels in width and the total width of the image at least 420 pixels in width as defined in the Normative Note #7 of Section 5.2 in SP 800-76-1. Widths exceeding the minimum requirements for spatial resolution should conform to the Image Width: Head Width ration of 7:4 defined in Section 8.3.4 of INCITS 385. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-76-1, Section 5.2 INCITS 385, Section 8.3.4
EP.54	Facial image data shall be formatted in one of the two compression formats enumerated in Section 6.2 of FACESTD. Both whole-image and single-region-of-interest (ROI) compression are permitted. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-76-1, Section 5.2
EP.55	Facial images shall be compressed using a compression ratio no higher than 15:1. However, when facial images are stored on PIV cards, JPEG 2000 shall be used with ROI compression in which the innermost region shall be centered on the face and compressed at no more than 24:1. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-76-1, Section 5.2
EP.56	The CHUID buffer shall contain an Asymmetric digital signature of the CHUID object, which has been encoded as a Cryptographic Message Syntax external digital signature as defined in RFC 3852.	FIPS 201-1, Section 4.2.2

EP.57	The digital signature is implemented as a SignedData Type.	FIPS 201-1, Section 4.2.2
EP.58	The value of the version field of the SignedData content type shall be v3.	FIPS 201-1, Section 4.2.2
EP.59	The digestAlgorithms field of the SignedData content type shall be in accordance with Table 3-3 of SP 800-78-1.	FIPS 201-1, Section 4.2.2
EP.60	The eContentType of the encapContentInfo shall be id-PIV-CHUIDSecurityObject (OID = 2.16.840.1.101.3.6.1).	FIPS 201-1, Section 4.2.2
EP.61	The encapContentInfo of the SignedData content type shall omit the eContent field.	FIPS 201-1, Section 4.2.2
EP.62	The certificates field shall include only a single X.509 certificate which is used to verify the signature in the SignerInfo field.	FIPS 201-1, Section 4.2.2
EP.63	The crls field from the SignedData content type shall be omitted.	FIPS 201-1, Section 4.2.2
EP.64	The SignerInfos in the SignedData content type shall contain only a single SignerInfo type.	FIPS 201-1, Section 4.2.2
EP.65	The SignerInfo type shall use the issuerAndSerialNumber choice for the sid and this shall correspond to the issuer and serialNumber fields found in the X.509 certificate for the entity that signed the CHUID.	FIPS 201-1, Section 4.2.2
EP.66	The SignerInfo type shall specify a digestAlgorithm in accordance with Table 3-3 of SP 800-78-1.	SP 800-78-1, Section 3.2.1
EP.67	The signedAttrs of the SignerInfo shall include the MessageDigest (OID = 1.2.840.113549.1.9.4) attribute containing the hash computed over the concatenated content of the CHUID, excluding the asymmetric signature field.	FIPS 201-1, Section 4.2.2
EP.68	The signedAttrs of the SignerInfo shall include the pivSigner-DN (OID = 2.16.840.1.101.3.6.5) attribute containing the subject name that appears in the X.509 certificate for the entity that signed the CHUID.	FIPS 201-1, Section 4.2.2
EP.69	The signatureAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-4 of SP 800-78-1 and based on the PIV card expiration date in accordance with Table 3-3 of SP 800-78-1.	SP 800-78-1, Section 3.2.1
EP.70	The SignedData content type shall include the digital signature.	FIPS 201-1, Section 4.2.2
EP.71	The digital signature certificate used to sign the CHUID shall in the extKeyUsage assert id-PIV-content-signing (OID = 2.16.840.1.101.3.6.7).	FIPS 201-1, Section 4.2.2
EP.72	The size of the public key for digital signature certificate used to sign the CHUID shall be determined by the expiration of the Card in accordance with Table 3-3 of SP 800-78-1.	SP 800-78-1, Section 3.2.1
EP.73	The CBEFF_SIGNATURE_BLOCK shall be encoded as a Cryptographic Message Syntax external digital signature as defined in RFC 3852.	FIPS 201-1, Section 4.4.2

EP.74	The digital signature is implemented as a SignedData Type.	FIPS 201-1, Section 4.4.2
EP.75	The value of the version field of the SignedData content type shall be v1 or v3 based on whether the certificates field is omitted or not.	FIPS 201-1, Section 4.4.2
EP.76	The digestAlgorithms field of the SignedData content type shall be in accordance with Table 3-3 of SP 800-78-1.	FIPS 201-1, Section 4.4.2
EP.77	The eContentType of the encapContentInfo shall be id-PIV-biometricObject (OID = 2.16.840.1.101.3.6.2).	FIPS 201-1, Section 4.4.2
EP.78	The encapContentInfo of the SignedData content type shall omit the eContent field.	FIPS 201-1, Section 4.4.2
EP.79	If the signature on the fingerprint biometric was generated with a different key as the signature on the CHUID, the certificates field shall include only a single certificate in the SignerInfo field which can be used to verify the signature; else the certificates field shall be omitted.	FIPS 201-1, Section 4.4.2
EP.80	The crls field from the SignedData content type shall be omitted.	FIPS 201-1, Section 4.4.2
EP.81	The signerInfos in the SignedData content type shall contain only a single SignerInfo type.	FIPS 201-1, Section 4.4.2
EP.82	The SignerInfo type shall use the issuerAndSerialNumber choice for the sid and this shall correspond to the issuer and serialNumber fields found in the X.509 certificate for the entity that signed the biometric data.	FIPS 201-1, Section 4.4.2
EP.83	The SignerInfo type shall specify a digestAlgorithm in accordance with Table 3-3 of SP 800-78-1.	SP 800-78-1, Section 3.2.1
EP.84	The signedAttrs of the SignerInfo shall include the MessageDigest (OID = 1.2.840.113549.1.9.4) attribute containing the hash of the concatenated CBEFF_HEADER and the STD_BIOMETRIC_RECORD.	FIPS 201-1, Section 4.4.2
EP.85	The signedAttrs of the SignerInfo shall include the pivSigner-DN (OID = 2.16.840.1.101.3.6.5) attribute containing the subject name that appears in the X.509 certificate for the entity that signed the fingerprint biometric data.	FIPS 201-1, Section 4.4.2
EP.86	The signedAttrs of the SignerInfo shall include the pivFASC-N (OID = 2.16.840.1.101.3.6.6) attribute containing the FASC-N of the PIV card.	FIPS 201-1, Section 4.4.2
EP.87	The signatureAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-4 of SP 800-78-1 and based on the signature generation date of the object, in accordance with Table 3-3 of SP 800-78-1.	SP 800-78-1, Section 3.2.1
EP.88	The SignedData content type shall include the digital signature.	FIPS 201-1, Section 4.4.2
EP.89	The digital signature certificate used to sign PIV fingerprint biometric shall in the extKeyUsage assert id-PIV-content-signing (OID = 2.16.840.1.101.3.6.7).	FIPS 201-1, Section 4.4.2

EP.90	The size of the public key for digital signature certificate used to sign the biometrics shall be determined by the signature generation date of the object, in accordance with Table 3-3 of SP 800-78-1.	SP 800-78-1, Section 3.2.1
EP.91	The CBEFF_SIGNATURE_BLOCK shall be encoded as a Cryptographic Message Syntax external digital signature as defined in RFC 3852. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2
EP.92	The digital signature is implemented as a SignedData Type. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2
EP.93	The value of the version field of the SignedData content type shall be v3. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2
EP.94	The digestAlgorithms field of the SignedData content type shall be in accordance with Table 3-3 of SP 800-78-1. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-78-1, Section 3.2.1
EP.95	The eContentType of the encapContentInfo shall be id-PIV-biometricObject (OID = 2.16.840.1.101.3.6.2). *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2
EP.96	The encapContentInfo of the SignedData content type shall omit the eContent field. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2
EP.97	If the signature on the facial image biometric was generated with a different key as the signature on the CHUID, the certificates field shall include only a single certificate in the SignerInfo field which can be used to verify the signature; else the certificates field shall be omitted. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2
EP.98	The crls field from the SignedData content type shall be omitted. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2
EP.99	The signerInfos in the SignedData content type shall contain only a single SignerInfo type. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2
EP.100	The SignerInfo type shall use the issuerAndSerialNumber choice for the sid and this shall correspond to the issuer and serialNumber	FIPS 201-1, Section 4.4.2

	fields found in the X.509 certificate for the entity that signed the biometric data. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	
EP.101	The SignerInfo type shall specify a digestAlgorithm in accordance with Table 3-3 of SP 800-78-1. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-78-1, Section 3.2.1
EP.102	The signedAttrs of the SignerInfo shall include the MessageDigest (OID = 1.2.840.113549.1.9.4) attribute containing the hash of the concatenated CBEFF_HEADER and the STD_BIOMETRIC_RECORD. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2
EP.103	The signedAttrs of the SignerInfo shall include the pivSigner-DN (OID = 2.16.840.1.101.3.6.5) attribute containing the subject name that appears in the X.509 certificate for the entity that signed the biometric data. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2
EP.104	The signedAttrs of the SignerInfo shall include the pivFASC-N (OID = 2.16.840.1.101.3.6.6) attribute containing the FASC-N of the PIV card. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2
EP.105	The signatureAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-4 of SP 800-78-1 and based on the signature generation date of the object, in accordance with Table 3-3 of SP 800-78-1. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-78-1, Section 3.2.1
EP.106	The SignedData content type shall include the digital signature. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2
EP.107	The digital signature certificate used to sign PIV facial image biometric shall in the extKeyUsage assert id-PIV-content-signing (OID = 2.16.840.1.101.3.6.7). *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2
EP.108	The size of the public key for digital signature certificate used to sign the biometrics shall be determined by the expiration of the card in accordance with Table 3-3 of SP 800-78-1. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-78-1, Section 3.2.1

EP.109	Data objects populated on personalized PIV cards shall be stored in the appropriate containers according to SP 800-73-1, Appendix A, and should contain all appropriate tags and lengths for each element in the object.	Derived
EP.110	The security object buffer shall contain an asymmetric digital signature as specified in RFC (3852).	FIPS 201-1, Section 4.4.2
EP.111	The digital signature is implemented as a SignedData Type.	FIPS 201-1, Section 4.4.2
EP.112	The value of the version field of the SignedData content type shall be v3.	FIPS 201-1, Section 4.4.2
EP.113	The digestAlgorithms field of the SignedData content type shall be in accordance with Table 3-7 of SP 800-78.	SP 800-78, Section 3.2.3
EP.114	The eContentType of the encapContentInfo shall be id-icao-ldsSecurityObject (OID = 1.3.27.1.1.1).	FIPS 201-1, Section 4.4.2
EP.115	The eContent of the encapContentsInfo field shall contain the encoded contents of the ldsSecurity object.	PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version - 1.1, Annex C
EP.116	The certificates field shall be omitted since it is included in the CHUID.	SP 800-73-1-1, Section 1.8.5
EP.117	The digestAlgorithm field specified in the SignerInfo field is in accordance with Table 3-7 of SP 800-78.	SP 800-78, Section 3.2.3
EP.118	The signatureAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-4 of SP 800-78 and based on the PIV card expiration date in accordance with Table 3-3 of SP 800-78.	SP 800-78, Section 3.2.1
EP.119	The SignedData content type shall include the digital signature.	Derived
EP.120	The card issuer's digital signature key used to sign the CHUID shall also be used to sign the security object.	SP 800-73-1-1, Section 1.8.5
EP.121	The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78 and based on the certificate expiration date in accordance with Table 3-3 of SP 800-78. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.2.1
EP.122	If Rivest Shamir Adleman (RSA) with Probabilistic Signature Scheme (PSS) padding is used, the parameters field of the AlgorithmIdentifier type shall assert Secure Hash Algorithm (SHA) 256 (OID = 2.16.840.1.101.3.4.2.1). For the other RSA algorithms, the parameters field is populated with NULL. For Elliptic Curve Digital Signature Algorithm (ECDSA), the parameters field is absent.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006,

	(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)	Worksheet 9
EP.123	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.2.2
EP.124	If the public key algorithm is Elliptic Curve, then the EcpkParameters field uses either the namedCurve field populated with the appropriate OID from Table 3-6 of SP 800-78 or the implicitlyCA choice. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.2.2
EP.125	The keyUsage extension shall assert only the digitalSignature bit. No other bits shall be asserted. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9
EP.126	The policyIdentifier field in the certificatePolicies must assert id-fpki-common-authentication (OID = 2.16.840.1.101.3.2.1.3.13). *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9
EP.127	The authorityInfoAccess field shall contain an id-ad-ocsp accessMethod. The access location uses the Uniform Resource Identifier (URI) name form to specify the location of an Hypertext Transfer Protocol (HTTP) accessible Online Certificate Status Protocol (OCSP) Server distributing status information for this certificate. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9
EP.128	The FASC-N shall be populated in the subjectAltName extension using the pivFASC-N attribute (OID = 2.16.840.1.101.3.6.6). *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	FIPS 201-1, Section 4.3
EP.129	The piv-interim extension (OID = 2.16.840.1.101.3.6.9.1) shall be present and contain an interim_indicator field which is populated with a Boolean value. This extension is not critical. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006,

		Worksheet 9
EP.130	The size of the public key for PIV authentication shall be determined by the expiration of the certificate in accordance with Table 3-1 of SP 800-78. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.1
EP.131	The public key present in the PIV authentication certificate correspond to the PIV authentication private key. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	FIPS 201-1, Section 4.3
EP.132	The FASC-N in the subjectAltName field in the PIV authentication certificate is the same as the FASC-N present in the CHUID. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	Derived
EP.133	The expiration of the PIV authentication certificate is not beyond the expiration of the CHUID. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	FIPS 201-1, Section 4.3
EP.134	If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.1
EP.135	The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78 and based on the certificate expiration date in accordance with Table 3-3 of SP 800-78. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.1
EP.136	If RSA with PSS padding is used, the parameters field of the AlgorithmIdentifier type shall assert SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For the other RSA algorithms, the parameters field is populated with NULL. For ECDSA, the parameters field is absent. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5
EP.137	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.2.2
EP.138	If the public key algorithm is Elliptic Curve, then the EcpkParameters field uses either the namedCurve field populated with the appropriate OID from Table 3-6 of SP 800-78 or the implicitlyCA	SP 800-78, Section 3.2.2 X.509

	choice. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5
EP.19	The keyUsage extension shall assert both the digitalSignature and nonRepudiation bits. No other bits shall be asserted. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5
EP.140	The size of the public key for digital signature shall be determined by the expiration of the certificate in accordance with Table 3-1 of SP 800-78. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.1
EP.141	The public key present in the digital signature certificate corresponds to the digital signature private key. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	FIPS 201-1, Section 4.3
EP.142	The expiration of the digital signature certificate is not beyond the expiration of the CHUID. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.1
EP.143	If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.1
EP.144	The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78 and based on the certificate expiration date in accordance with Table 3-3 of SP 800-78. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.2.1
EP.145	If RSA with PSS padding is used, the parameters field of the AlgorithmIdentifier type shall assert SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For the other RSA algorithms, the parameters field is populated with NULL. For ECDSA, the parameters field is absent. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5

EP.146	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.2.2
EP.147	If the public key algorithm is Elliptic Curve, then the EcpkParameters field uses either the namedCurve field populated with the appropriate OID from Table 3-6 of SP 800-78 or the implicitlyCA choice. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.2.2
EP.148	If the public key algorithm is RSA, then the keyUsage extension shall only assert the keyEncipherment bit. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5
EP.149	If the public key algorithm is Elliptic Curve, then the keyUsage extension shall only assert the keyAgreement bit. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5
EP.150	The size of the public key for key management shall be determined by the expiration of the certificate in accordance with Table 3-1 of SP 800-78. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.1
EP.151	The public key present in the key management certificate corresponds to the key management private key. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	FIPS 201-1, Section 4.3
EP.152	If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.1
EP.153	The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78 and based on the certificate expiration date in accordance with Table 3-3 of SP 800-78. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.2.1

EP.154	If RSA with PSS padding is used, the parameters field of the AlgorithmIdentifier type shall assert SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For the other RSA algorithms, the parameters field is populated with NULL. For ECDSA, the parameters field is absent. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6
EP.155	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	SP 800-76, Section 3.2.2
EP.156	If the public key algorithm is Elliptic Curve, then the EcpkParameters field uses either the namedCurve field populated with the appropriate OID from Table 3-6 of SP 800-78 or the implicitlyCA choice. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.2.2 X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6
EP.157	The keyUsage extension shall assert only the digitalSignature bit. No other bits shall be asserted. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6
EP.158	The policyIdentifier field in the certificatePolicies must assert id-fpki-common-cardAuth (OID = 2.16.840.1.101.3.2.1.3.17). *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6
EP.159	The extKeyUsage extension shall assert id-PIV-cardAuth (OID = 2.16.840.1.101.3.6.8). This extension is critical. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6
EP.160	The authorityInfoAccess field shall contain an id-ad-ocsp accessMethod. The access location uses the URI name form to	X.509 Certificate and

	specify the location of an HTTP accessible OCSP Server distributing status information for this certificate. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	CRL Profile for the Common Policy, February 6, 2006, Worksheet 6
EP.161	The FASC-N shall be populated in the subjectAltName extension using the pivFASC-N attribute OID = 2.16.840.1.101.3.6.6). *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6
EP.162	The piv-interim extension (OID = 2.16.840.1.101.3.6.9.1) shall be present contain an interim_indicator field which is populated with a Boolean value. This extension is not critical. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6
EP.163	The size of the public key for card authentication shall be determined by the expiration of the certificate in accordance with Table 3-1 of SP 800-78. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	SP 800-76, Section 3.1
EP.164	The public key present in the card authentication certificate correspond to the card authentication private key. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	FIPS 201-1, Section 4.3
EP.165	The FASC-N in the subjectAltName field in the card authentication certificate is the same as the FASC-N present in the CHUID. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	Derived
EP.166	If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.1
EP.167	If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	SP 800-78, Section 3.1
EP.168	If the public key size of the certificate that signs the CHUID, Biometrics and Security Object is 2048 bits or greater, then the hash	Derived

	algorithm asserted in the digestAlgorithm of the SignerInfo shall be SHA256 (1.2.840.113549.1.1.11 [PKCS v1.5 padding scheme] or 1.2.840.113549.1.1.10. [PSS padding scheme])	
EP.169	If the public key size of the PIV Authentication, Digital Signature, Key Management or Card Management certificate is 2048 bits or greater, then the hash algorithm asserted in the AlgorithmIdentifier of the signature shall be SHA256 (1.2.840.113549.1.1.11 [PKCS v1.5 padding scheme] or 1.2.840.113549.1.1.10. [PSS padding scheme]) *(This requirement will be evaluated only if the above listed certificates are issued by an authorized Certification Authority)*	Derived

Signature

I hereby claim that I am authorized to sign this form on behalf of the above specified company. I acknowledge that I have am aware of the requirements of FIPS 201 and its related publications that my Product needs to comply with and that the Product that has been submitted to the Lab is, to the best of my knowledge, complete and accurately meeting these requirements. Furthermore, by signing below, I attest that the Product/Service is being submitted under each category for which this Product/Service applies. I am also aware that any false claims to this statement could result in a penalty as defined by the Federal Acquisition Regulation (FAR).

Signature		Date	
Name			
Title			