GSA U.S General Services Administration

Electronic Personalization Test Procedure

VERSION 5.0.0

April Giles
Nabil Ghadiali

FIPS 201 EVALUATION PROGRAM

June 23, 2010

Office of Governmentwide Policy
Office of Technology Strategy
Identity Management Division
Washington, DC 20405

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	04/28/06	Document creation.	Limited
Draft	0.0.2	05/11/06	Document update.	Limited
Draft	0.1.0	05/11/06	Submitted to GSA for approval.	GSA
Draft	0.1.1	05/11/06	Changes made per GSA comment.	Limited
Approved	1.0.0	05/11/06	Approved by GSA.	Public
Revision	2.0.0	06/29/06	Updated based on feedback from GSA.	Public
Revision	3.0.0	07/03/07	Updated based on feedback from the Lab.	Public
Revision	4.0.0	10/16/09	Updated based on changes to the EP (Product) Approval Procedure v13.0.0.	Public
Revision	5.0.0	06/23/10	Updated to reflect the changes to EP (Product) Approval Procedure v14.0.0.	Public

Table of Contents

List of Tables

1 Overview

Homeland Security Presidential Directive-12 (HSPD-12) - "*Policy for a Common Identification Standard for Federal Employees and Contractors*" directed the promulgation of a new Federal standard for a secure and reliable form of identification issued by all Federal Agencies to their employees and contractors.

In addition to derived test requirements developed to test conformance to the NIST standard, GSA has established interoperability and performance metrics to further determine product suitability. Vendors whose products and services are deemed to be conformant with NIST standards and the GSA interoperability and performance criteria will be eligible to sell their products and services to the Federal Government.

1.1 Identification

This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the Electronic Personalization Product or Service against the subset of applicable requirements that need to be electronically tested for this category.

2 Testing Process

As previously mentioned, this document prescribes detailed test steps that need to be executed in order to test the requirements applicable for this category. Please note that conformance to the tests specified in this document will not result in the Product or Service being compliant to the applicable requirements of FIPS 201. The Product or Service must undergo an evaluation using all the evaluation criteria listed for that category prior to being deemed as compliant. Only products and services that have successfully completed the entire Approval Process will be designated as conformant to the Standard. To this effect, this document only provides details for the evaluation using the Lab Test Data Report approval mechanism.

A Lab Engineer follows the steps outlined below in order to test those requirements that have been identified to be electronically tested. The end result is a compilation of the observed behavior of the submitted PIV Card in the Lab Test Data Report.

Section 3 provides the test procedures that need to be executed for evaluating the Product or Service as conformant to the requirements of FIPS 201.

3 Test Procedure for Electronic Personalization

3.1 Requirements

The following table provides a reference to the requirements that need to be electronically tested within the Lab as outlined in the Approval Procedures document for the Product and Service. The test cases that are used to check compliance to the requirements are cross-referenced in the table below.

Identifier #	Requirement Description	Source	Test Case #
EP.8	{The personalized card shall be tested by the SP 800-85B test tool for data format compliance.}	Derived	EP-TP.1
EP.10	{The CCC shall contain the mandatory BER-TLV fields as specified in SP 800-73-3 Table 7.}	SP 800-73-3, Appendix A Para 7 pg.20	EP-TP.1
EP.11	{The registered} data model {value in} the CCC shall be 0x10.	SP 800-73-3, Section 3.1.1 Para 2 pg.4	EP-TP.1
EP.12	{The CHUID on a PIV card shall contain the mandatory BER-TLV fields as specified in SP 800-73-3 Table 8.}	SP 800-73-3, Appendix A Para 8 pg.20	EP-TP.1
EP.13	{The PIV Authentication Certificate on a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 9.}	SP 800-73-3, Appendix A Para 11 pg.21	EP-TP.1
EP.14	{The Cardholder Fingerprints element on a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 10.}	SP 800-73-3, Appendix A Para 12 pg.21	EP-TP.1
EP.15	{The Security Object on a PIV Card shall contain the mandatory BER-TLV fields as specified in SP 800-73-3 Table 11.}	SP 800-73-3, Appendix A Para 13 pg.21	EP-TP.1
EP.16	{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-TP.1
EP.17	{The facial image on a PIV Card shall contain the BER-TLV fields as	SP 800-73-3,	EP-TP.1

	specified in SP 800-73-3 Table 12.} *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	Appendix A Para 14 pg.21	
EP.18	{The Printed Information element implemented in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 13.} *(This requirement will be evaluated only if the printed information is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 15 pg.22	EP-TP.1
EP.19	{The Digital Signature Certificate in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 14.} *(This requirement will be evaluated only if the digital signature key is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 16 pg.22	EP-TP.1
EP.20	{The Key Management Certificate in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 15.} *(This requirement will be evaluated only if the key management key is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 17 pg.22	EP-TP.1
EP.21	{The Card Authentication Certificate in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 16.} *(This requirement will be evaluated only if the card authentication key is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 18 pg.23	EP-TP.1
EP.22	{The Discovery Object in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 17.} *(This requirement will be evaluated only if the Discovery Object is implemented in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 19 pg.23	EP-TP.1
EP.23	{The CBEFF structure must comply with SP 800-76-1} 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 Para 2 pg.17	EP-TP.1

EP.24	{The Patron Header Version of the CBEFF Patron Format shall be 0x03.}	SP 800-76-1, Section 6 Para 14 pg.17	EP-TP.1
EP.25	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 Para 3 pg.18	EP-TP.1
EP.26	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 Para 3 pg.18	EP-TP.1
EP.27	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 Para 3 pg.18	EP-TP.1
EP.28	{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 Para 3 pg.18	EP-TP.1
EP.29	The Validity Period {in the PIV Patron Format (see Row 8 in Table 8 of SP 800-76-1) shall} consist of two dates.	SP 800-76-1, Section 6 Para 3 pg.18	EP-TP.1
EP.30	{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	SP 800-76-1, Section 6 Para 3 pg.18	EP-TP.1

	modalities not listed there the value shall be 0x00.		
EP.31	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 Para 3 pg.18	EP-TP.1
EP.32	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 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.	SP 800-76-1, Section 6 Para 3 pg.18	EP-TP.1
EP.33	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 Para 3 pg.19	EP-TP.1
EP.34	{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 Para 3 pg.19	EP-TP.1
EP.35	{The “Reserved for future use” field in the PIV Patron Format shall contain 0x00000000.}	SP 800-76-1, Section 6 Para 3 pg.17	EP-TP.1
EP.36	{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 Para 1 pg.35	EP-TP.1

EP.37	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 3.4.3 Para 3 pg.7	EP-TP.1
EP.38	{The Format Identifier of the General Header Record shall be 0x464D5200.}	SP 800-76-1, Section 3.4.3 Para 3 pg.8	EP-TP.1
EP.39	{The Version Number of the General Header Record shall be 0x20323000.}	SP 800-76-1, Section 3.4.3 Para 3 pg.8	EP-TP.1
EP.40	{The length of the entire CBEFF wrapped fingerprint record shall fit within the container size limits specified in SP 800-73-3.[1]}	SP 800-73-3, Appendix A Para 12 pg.21	EP-TP.1
EP.41	Both {of the two} fields ("Owner" and "Type") of the CBEFF Product Identifier shall be non-zero.	SP 800-76-1, Section 3.4.3 Para 3 pg.9	EP-TP.1
EP.42	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 3.4.3 Para 3 pg.9	EP-TP.1
EP.43	{The Capture Equipment Compliance of the General Record Header shall be 1000b.}	SP 800-76-1, Section 3.4.3 Para 3 pg.8	EP-TP.1
EP.44	{The Capture Equipment ID of the General Record Header shall be greater than zero.}	SP 800-76-1, Section 3.4.3 Para 3 pg.8	EP-TP.1
EP.45	{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 3.4.3 Para 3 pg.8	EP-TP.1
EP.46	{The resolution of the X (horizontal)	SP 800-76-1,	EP-TP.1

[1] The size of the CBEFF wrapped fingerprint record can exceed the size limit (4000 bytes) if the data element signer certificate is stored in the Fingerprint I and II data element itself.

	and Y (vertical) minutiae coordinates shall be 197.}	Section 3.4.3 Para 3 pg.8	
EP.47	{The Number of Views of the General Header Record shall be 2.}	SP 800-76-1, Section 3.4.3 Para 3 pg.8	EP-TP.1
EP.48	{The Reserved Byte of the General Header Record shall be 0.}	SP 800-76-1, Section 3.4.3 Para 3 pg.8	EP-TP.1
EP.49	{The Finger Position value shall be between 0 and 10.}	SP 800-76-1, Section 3.4.3 Para 3 pg.8	EP-TP.1
EP.50	{The View Number of the Single Finger View Record shall be 0.}	SP 800-76-1, Section 3.4.3 Para 3 pg.8	EP-TP.1
EP.51	{The Impression Type of the Single Finger View Record shall be either 0 or 2.}	SP 800-76-1, Section 3.4.3 Para 3 pg.8	EP-TP.1
EP.52	{The quality value of captured fingerprint images computed using NFIQ and reported as Q = 20(6-NFIQ) shall be 60, 80 or 100.[2]}	SP 800-76-1, Section 3.4.3 Para 3 pg.8	EP-TP.1
EP.53	{The Number of Minutiae of Single Finger View Record shall be between 0 and 128.}	SP 800-76-1, Section 3.4.3 Para 3 pg.8	EP-TP.1
EP.54	{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 3.4.3 Para 3 pg.8	EP-TP.1
EP.55	{The X coordinate value of the minutia shall not exceed image width value and Y coordinate value of the minutia shall not exceed image height value.}	SP 800-76-1, Section 3.4.3 Para 3 pg.8	EP-TP.1
EP.56	{The Minutia Angle shall be between	SP 800-76-1,	EP-TP.1

[2] The SP 800-85B Data Conformance Test Tool is set to pass Finger Quality values (Q) 60, 80 and 100 to ensure only the fingerprints with best quality are imported in to PIV Cards. However, according to NIST SP 800-76-1 Table 3 Q values 20 and 40 are considered acceptable in addition to those listed above.

	0 and 179.}	Section 3.4.3 Para 3 pg.8	
EP.57	{The Minutiae Quality shall be between 0 and 100.}	SP 800-76-1, Section 3.4.3 Para 3 pg.8	EP-TP.1
EP.59	{The mandatory value for Extended Data Block Length for MINUSTD template shall be zero.}	SP 800-76-1, Section 3.4.3 Para 3 pg.8	EP-TP.1
EP.60	{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 Para 1 pg.14	EP-TP.1
EP.61	{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 800-73-3.} *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 12 pg.21	EP-TP.1
EP.62	{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 Para 3 pg.16 INCITS 385, Section 8.3.4	EP-TP.1
EP.65	{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 Para 1 pg.30	EP-TP.1

EP.66	{The digital} signature {shall be} implemented as a SignedData Type.	FIPS 201-1, Section 4.2.2 Para 2 pg.31	EP-TP.1
EP.67	{The value of the} version field {of the SignedData content type shall be} v3.	FIPS 201-1, Section 4.2.2 Para 2 pg.31	EP-TP.1
EP.68	The digestAlgorithms field {of the SignedData content type shall be in accordance with Table 3-3 of} SP 800-78-2.	FIPS 201-1, Section 4.2.2 Para 2 pg.31	EP-TP.1
EP.69	{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 Para 2 pg.31	EP-TP.1
EP.70	{The} encapContentInfo {of the SignedData content type shall} omit the eContent field.	FIPS 201-1, Section 4.2.2 Para 2 pg.31	EP-TP.1
EP.71	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 Para 2 pg.31	EP-TP.1
EP.72	The crls field {from the SignedData content type} shall be omitted.	FIPS 201-1, Section 4.2.2 Para 2 pg.31	EP-TP.1
EP.73	The SignerInfos {in the SignedData content type} shall {contain only a} single SignerInfo {type}.	FIPS 201-1, Section 4.2.2 Para 2 pg.31	EP-TP.1
EP.74	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 Para 2 pg.31	EP-TP.1
EP.75	{The SignerInfo type shall specify a digestAlgorithm in accordance with Table 3-3 of SP 800-78-2.}	SP 800-78-2, Section 3.2.1 Para 2 pg.5	EP-TP.1
EP.76	{The signedAttrs of the SignerInfo shall include the} MessageDigest {(OID = 1.2.840.113549.1.9.4)} attribute containing the hash	FIPS 201-1, Section 4.2.2 Para 2 pg.31	EP-TP.1

	computed over the concatenated content of the CHUID, excluding the asymmetric signature field.		
EP.77	{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 Para 2 pg.31	EP-TP.1
EP.78	{The signatureAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-4 of SP 800-78-2 and based on the PIV card expiration date in accordance with Table 3-3 of SP 800-78-2.}	SP 800-78-2, Section 3.2.1 Para 2 pg.5	EP-TP.1
EP.79	{The SignedData content type shall} include the digital signature.	FIPS 201-1, Section 4.2.2 Para 2 pg.31	EP-TP.1
EP.80	{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 Para 3 pg.31	EP-TP.1
EP.81	{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 800-78-2.}	SP 800-78-2, Section 3.2.1 Para 2 pg.5	EP-TP.1
EP.82	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 Para 2 pg.35	EP-TP.1
EP.83	The {digital signature is implemented} as a SignedData Type.	FIPS 201-1, Section 4.4.2 Para 3 pg.35	EP-TP.1
EP.84	{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 Para 3 pg.35	EP-TP.1
EP.85	The digestAlgorithms field {of the SignedData content type} shall be {in accordance with Table 3-3 of} SP	FIPS 201-1, Section 4.4.2 Para 3 pg.35	EP-TP.1

	800-78{-2}.		
EP.86	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 Para 3 pg.35	EP-TP.1
EP.87	The encapContentInfo {of the SignedData content type} shall omit the eContent field.	FIPS 201-1, Section 4.4.2 Para 3 pg.35	EP-TP.1
EP.88	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 Para 3 pg.35	EP-TP.1
EP.89	The crls field {from the SignedData content type} shall be omitted.	FIPS 201-1, Section 4.4.2 Para 3 pg.35	EP-TP.1
EP.90	{The} signerInfos {in the SignedData content type} shall {contain} only a single SignerInfo type.	FIPS 201-1, Section 4.4.2 Para 3 pg.35	EP-TP.1
EP.91	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 Para 3 pg.35	EP-TP.1
EP.92	{The SignerInfo type shall specify a digestAlgorithm in accordance with Table 3-3 of SP 800-78-2.}	SP 800-78-2, Section 3.2.1 Para 2 pg.5	EP-TP.1
EP.93	{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 Para 3 pg.36	EP-TP.1
EP.94	{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 Para 3 pg.36	EP-TP.1

EP.95	{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 Para 3 pg.36	EP-TP.1
EP.96	{The signatureAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-4 of SP 800-78-2 and based on the signature generation date of the object, in accordance with Table 3-3 of SP 800-78-2.}	SP 800-78-2, Section 3.2.1 Para 2 pg.5	EP-TP.1
EP.97	{The SignedData content type shall} include the digital signature.	FIPS 201-1, Section 4.4.2 Para 3 pg.36	EP-TP.1
EP.98	{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 Para 4 pg.36	EP-TP.1
EP.99	{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 800-78-2.}	SP 800-78-2, Section 3.2.1 Para 2 pg.5	EP-TP.1
EP.100	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 Para 2 pg.35	EP-TP.1
EP.101	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 Para 3 pg.35	EP-TP.1
EP.102	{The value of the} version field {of the SignedData content type shall be v1 or} v3 {based on whether the	FIPS 201-1, Section 4.4.2	EP-TP.1

	certificates field is omitted or not}. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	Para 3 pg.35	
EP.103	The digestAlgorithms field {of the SignedData content type shall be in accordance with Table 3-3 of} SP 800-78{-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 Para 3 pg.35	EP-TP.1
EP.104	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 Para 3 pg.35	EP-TP.1
EP.105	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 Para 3 pg.35	EP-TP.1
EP.106	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 Para 3 pg.35	EP-TP.1
EP.107	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 Para 3 pg.35	EP-TP.1
EP.108	{The} signerInfos {in the SignedData content type} shall {contain} only a single SignerInfo type. *(This requirement will be evaluated only if the*	FIPS 201-1, Section 4.4.2 Para 3 pg.35	EP-TP.1

	facial image is populated in the card provided to the Lab)		
EP.109	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}. *(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 Para 3 pg.35	EP-TP.1
EP.110	{The SignerInfo type shall specify a digestAlgorithm in accordance with Table 3-3 of SP 800-78-2.} *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-78-2, Section 3.2.1 Para 2 pg.5	EP-TP.1
EP.111	{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 Para 3 pg.36	EP-TP.1
EP.112	{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 Para 3 pg.36	EP-TP.1
EP.113	{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 Para 3 pg.36	EP-TP.1

EP.114	{The signatureAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-4 of SP 800-78-2 and based on the signature generation date of the object, in accordance with Table 3-3 of SP 800-78-2.} *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-78-2, Section 3.2.1 Para 2 pg.5	EP-TP.1
EP.115	{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 Para 3 pg.36	EP-TP.1
EP.116	{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 Para 4 pg.36	EP-TP.1
EP.117	{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 800-78-2.} *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-78-2, Section 3.2.1 Para 2 pg.5	EP-TP.1
EP.118	{The message digests for the various data objects present in the security object shall be identical to the message digest of the data object itself.}	Derived	EP-TP.1
EP.119	{The security object buffer shall contain an asymmetric digital signature as specified in RFC (3852).}	SP 800-73-3, Section 3.1.4 Para 1 pg.6	EP-TP.1
EP.120	{The digital signature is implemented as a SignedData Type.}	SP 800-73-3, Section 3.1.4 Para 1 pg.6	EP-TP.1
EP.121	{The value of the version field of the	SP 800-73-3,	EP-TP.1

	SignedData content type shall be v1.}	Section 3.1.4 Para 1 pg.6	
EP.122	{The digestAlgorithms field of the SignedData content type shall be in accordance with Table 3-7 of SP 800-78-2.}	SP 800-78-2, Section 3.2.3 Para 1 pg.7	EP-TP.1
EP.123	The eContentType of the encapContentInfo shall be id-icao-ldsSecurityObject (OID = 1.3.27.1.1.1).	PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version - 1.1, Annex C	EP-TP.1
EP.124	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-TP.1
EP.125	The certificates field shall {be} omitted since it is included in the CHUID.	SP 800-73-3, Section 3.1.5 Para 4 pg.6	EP-TP.1
EP.126	{The digestAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-7 of SP 800-78-2.}	SP 800-78-2, Section 3.2.3 Para 1 pg.7	EP-TP.1
EP.127	{The signatureAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-4 of SP 800-78-2 and based on the PIV card expiration date in accordance with Table 3-3 of SP 800-78-2.}	SP 800-78-2, Section 3.2.1 Para 2 pg.5	EP-TP.1
EP.128	{The SignedData content type shall include the digital signature.}	SP 800-73-3, Section 3.1.5 Para 4 pg.6	EP-TP.1
EP.129	The card issuer's digital signature key used to sign the CHUID shall also be used to sign the security object.	SP 800-73-3, Section 3.1.5 Para 4 pg.6	EP-TP.1

EP.130	{The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78-2 and based on the certificate expiration date in accordance with Table 3-3 of SP 800-78-2.} *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.2.1 Para 2 pg.5	EP-TP.1
EP.131	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. *(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-TP.1
EP.132	{The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78-2.} *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.2.2 Para 1 pg.6	EP-TP.1
EP.133	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 800-78-2 or the implicitlyCA choice. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.2.2 Para 2 pg.6	EP-TP.1
EP.134	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*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006,	EP-TP.1

	authorized Certification Authority)	Worksheet 9	
EP.135	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
EP.136	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-TP.1
EP.137	{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-TP.1
EP.138	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-TP.1
EP.139	{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 800-78-2.} *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.1 Para 2 pg.3	EP-TP.1

EP.140	{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 Para 1 pg.31	EP-TP.1
EP.141	{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-TP.1
EP.142	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 Para 7 pg.32	EP-TP.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 PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.1 Para 5 pg.4	EP-TP.1
EP.144	{The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78-2 and based on the certificate expiration date in accordance with Table 3-3 of SP 800-78-2.} *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.1 Para 2 pg.5	EP-TP.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.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	EP-TP.1

	(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)		
EP.146	{The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78-2.} *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.2.2 Para 1 pg.6	EP-TP.1
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 800-78-2 or the implicitlyCA choice.} *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.2.2 Para 1 pg.6 X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	EP-TP.1
EP.148	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-TP.1
EP.149	{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 800-78-2.} *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.1 Para 2 pg.3	EP-TP.1
EP.150	{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 Para 7 pg.32	EP-TP.1
EP.151	The expiration of the digital signature certificate is not beyond the expiration of the CHUID. *(This requirement will be evaluated only if the*	FIPS 201-1, Section 4.3 Para 7 pg.32	EP-TP.1

	digital signature certificate is issued by an authorized Certification Authority)		
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 digital signature certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.1 Para 5 pg.4	EP-TP.1
EP.153	{The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78-2 and based on the certificate expiration date in accordance with Table 3-3 of SP 800-78-2.} *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.2.1 Para 2 pg.5	EP-TP.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 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-TP.1
EP.155	{The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78-2.} *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.2.2 Para 1 pg.6	EP-TP.1
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 800-78-2 or the implicitlyCA choice.} *(This requirement will be evaluated only if the key management certificate is issued by an*	SP 800-78-2, Section 3.2.2 Para 1 pg.6	EP-TP.1

	authorized Certification Authority)		
EP.157	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-TP.1
EP.158	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-TP.1
EP.159	{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 800-78-2.} *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.1 Para 2 pg.3	EP-TP.1
EP.160	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 Para 7 pg.33	EP-TP.1
EP.161	{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 800-78-2, Section 3.1 Para 5 pg.4	EP-TP.1
EP.162	{The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78-2 and based on the certificate expiration date in accordance with Table 3-3 of SP 800-78-2.} *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.2.1 Para 2 pg.5	EP-TP.1

EP.163	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-TP.1
EP.164	{The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78-2.} *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.2.2 Para 1 pg.6	EP-TP.1
EP.165	{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 800-78-2 or the implicitlyCA choice.} *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.2.2 Para 1 pg.6 X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	EP-TP.1
EP.166	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-TP.1
EP.167	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-TP.1
EP.168	The extKeyUsage extension shall assert id-PIV-cardAuth (OID = 2.16.840.1.101.3.6.8). This extension	X.509 Certificate and CRL Profile for the Common	EP-TP.1

	is critical. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	Policy, February 6, 2006, Worksheet 6	
EP.169	The authorityInfoAccess field shall contain an id-ad-ocsp accessMethod. The access location uses the URI name form to 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)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	EP-TP.1
EP.170	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-TP.1
EP.171	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-TP.1
EP.172	{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 800-78-2.} *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-2, Section 3.1 Para 2 pg.3	EP-TP.1
EP.173	{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*	FIPS 201-1, Section 4.3 Para 7 pg.33	EP-TP.1

	authorized Certification Authority)		
EP.174	{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-TP.1
EP.175	{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 800-78-2, Section 3.1 Para 5 pg.4	EP-TP.1
EP.178	{The Key History Object in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 18.} *(This requirement will be evaluated only if the Key History Object is implemented in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 20 pg.23	EP-TP.1
EP.179	{The Retired Certificate 1 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 19.} *(This requirement will be evaluated only if the Retired Certificate 1 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 21 pg.23	EP-TP.1
EP.180	{The Retired Certificate 2 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 20.} *(This requirement will be evaluated only if the Retired Certificate 2 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 22 pg.24	EP-TP.1
EP.181	{The Retired Certificate 3 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 21.} *(This requirement will be evaluated only if the Retired Certificate 3 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 23 pg.23	EP-TP.1
EP.182	{The Retired Certificate 4 for Key Management in a PIV Card shall	SP 800-73-3,	EP-TP.1

	contain the BER-TLV fields as specified in SP 800-73-3 Table 22.} *(This requirement will be evaluated only if the Retired Certificate 4 is present in the card provided to the Lab)*	Appendix A Para 24 pg.23	
EP.183	{The Retired Certificate 5 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 23.} *(This requirement will be evaluated only if the Retired Certificate 5 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 25 pg.23	EP-TP.1
EP.184	{The Retired Certificate 6 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 24.} *(This requirement will be evaluated only if the Retired Certificate 6 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 26 pg.23	EP-TP.1
EP.185	{The Retired Certificate 7 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 25.} *(This requirement will be evaluated only if the Retired Certificate 7 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 27 pg.25	EP-TP.1
EP.186	{The Retired Certificate 8 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 26.} *(This requirement will be evaluated only if the Retired Certificate 8 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 28 pg.25	EP-TP.1
EP.187	{The Retired Certificate 9 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 27.} *(This requirement will be evaluated only if the Retired Certificate 9 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 29 pg.25	EP-TP.1
EP.188	{The Retired Certificate 10 for Key Management in a PIV Card shall contain the BER-TLV fields as	SP 800-73-3, Appendix A Para 30 pg.25	EP-TP.1

	specified in SP 800-73-3 Table 28.} *(This requirement will be evaluated only if the Retired Certificate 10 is present in the card provided to the Lab)*		
EP.189	{The Retired Certificate 11 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 29.} *(This requirement will be evaluated only if the Retired Certificate 11 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 31 pg.26	EP-TP.1
EP.190	{The Retired Certificate 12 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 30.} *(This requirement will be evaluated only if the Retired Certificate 12 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 32 pg.26	EP-TP.1
EP.191	{The Retired Certificate 13 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 31.} *(This requirement will be evaluated only if the Retired Certificate 13 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 33 pg.26	EP-TP.1
EP.192	{The Retired Certificate 14 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 32.} *(This requirement will be evaluated only if the Retired Certificate 14 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 34 pg.26	EP-TP.1
EP.193	{The Retired Certificate 15 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 33.} *(This requirement will be evaluated only if the Retired Certificate 15 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 35 pg.26	EP-TP.1
EP.194	{The Retired Certificate 16 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 34.} *(This requirement will be evaluated only if the*	SP 800-73-3, Appendix A Para 36 pg.27	EP-TP.1

	Retired Certificate 16 is present in the card provided to the Lab)		
EP.195	{The Retired Certificate 17 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 35.} *(This requirement will be evaluated only if the Retired Certificate 17 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 37 pg.27	EP-TP.1
EP.196	{The Retired Certificate 18 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 36.} *(This requirement will be evaluated only if the Retired Certificate 18 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 38 pg.27	EP-TP.1
EP.197	{The Retired Certificate 19 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 37.} *(This requirement will be evaluated only if the Retired Certificate 19 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 39 pg.27	EP-TP.1
EP.198	{The Retired Certificate 20 for Key Management in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 38.} *(This requirement will be evaluated only if the Retired Certificate 20 is present in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 40 pg.28	EP-TP.1
EP.199	{The Cardholder Iris Images Object in a PIV Card shall contain the BER-TLV fields as specified in SP 800-73-3 Table 39.} *(This requirement will be evaluated only if the Cardholder Iris Images Object is implemented in the card provided to the Lab)*	SP 800-73-3, Appendix A Para 43 pg.28	EP-TP.1

Table 1 - Applicable Requirements

3.2 Test Components

Table 2 provides the details of all the components required by the Lab to execute this test procedure. Based on the different test cases, different components may be required to execute different cases.

#	Component	Component Details	Identifier
1	Host System	Includes a Workstation with the SP 800-85B data conformance tool installed and operational	HOST
2	PIV Card Reader (contact)	Gemalto GemPC Twin USB HW111459A[3]	CREADER
3	The electronically personalized PIV Card under test	-	PROD

Table 2 - Test Procedure: Components

3.3 Test Cases

This section discusses the various test cases that are needed to test the populated PIV Card against the requirements mentioned above.

3.3.1 Test Case EP-TP.1

3.3.1.1 Purpose

The purpose of this test is to verify whether the PIV Card submitted successfully completes the SP 800-85B conformance testing.

3.3.1.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ HOST ▪ CREADER ▪ PROD

[3] Any reader from the GSA FIPS 201 Approved Products List (APL) may be used as a substitute in the event that the specified reader is not available.

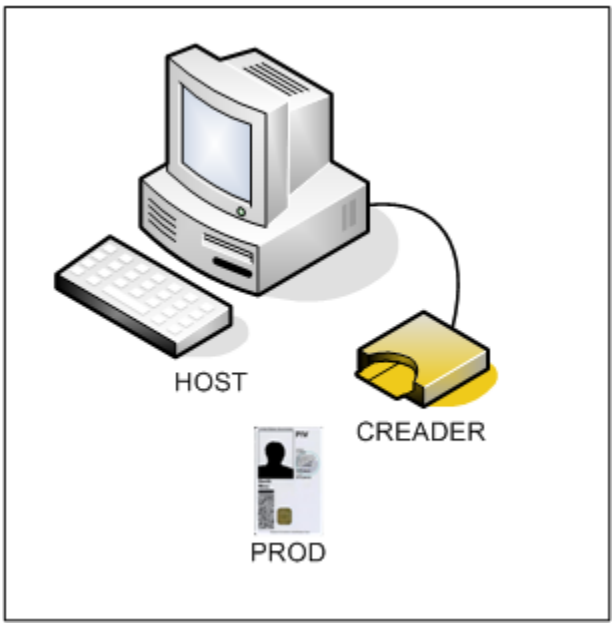
<table>
<tr><td>Configuration Diagram:</td><td> 

Figure 1 - Configuration Diagram for Test Case EP-TP.2</td></tr>
<tr><td>Preparation:</td><td>

Connect the CREADER into the appropriate port on the HOST.
Verify that the CREADER is correctly installed by reviewing its presence in list of hardware using the device manager of the host system.
Start up the SP 800-85B data conformance tool

1. Click the Configuration Tab
a. Click Report Settings.
i. In Implementation Under Test, the value should reflect the Case # and Product Name
ii. In IUI Date, the value should reflect the current date
b. Click Test Settings
i. If the data under evaluation resides on a PIV Card, the <code>GET_CONTAINERS_FROM_CARD</code> value must be 1, otherwise enter 0.
ii. The Optional Test Filter value should reflect all known optional containers on the PIV Card.
iii. The <code>PIN_VALID</code> value should reflect the PIV Application PIN.
c. Expand the Test Settings hive. Click Output Locations.
i. For the sake of orderliness, modify the Configuration Main Path value to append the Case number of the product under evaluation to the <code>.\apdu_tests_data_model\</code> directory.
d. Click Connectivity
i. The Reader Name value should reflect the exact name of the attached CREADER.
</td></tr>
</table>

	ii. The Smart Card Protocol should reflect `SCARD_PROTOCOL_T0` for T=0 smart cards and `SCARD_PROTOCOL_T1` for T=1 smart cards.

3.3.1.3 Test Process

Test Steps:	1. Insert the PROD into the CREADER 2. Click the Test Manager tab. 3. Execute the required tests by first clicking on the group of tests to perform, and then clicking the Run Selected button. 4. Verify that the test has completed by viewing the result on the screen. 5. Retain a PDF copy of the report for PROD.
Expected Result(s):	The test completes successfully with all results showing a "PASS" indicating that the objects on the PIV Card are conformant to the PIV data model.