

# **FIPS 201 Evaluation Program - Electronic Personalization (Product) Approval Procedure**

Version 12.0.0  
October 31, 2007



## Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	05/11/06	Document creation	Limited
Draft	0.1.0	05/11/06	Submitted to GSA for approval	GSA
Approved	1.0.0	05/11/06	Approved by GSA.	Public
Revision	1.0.1	06/29/06	Updated based on feedback from GSA	Limited
Revision	1.1.0	06/29/06	Submitted to GSA for approval	GSA
Revision	1.1.1	06/29/06	Updated based on feedback from GSA	Limited
Revision	1.2.0	06/30/06	Submitted to GSA for approval	GSA
Approved	2.0.0	06/30/06	Approved by GSA	Public
Revision	2.0.1	08/02/06	Updated based on feedback from GSA	Limited
Revision	2.1.0	08/02/06	Submitted to GSA for approval	GSA
Revision	2.1.1	08/03/06	Updated based on feedback from GSA	Limited
Revision	2.2.0	08/03/06	Submitted to GSA for approval	GSA
Approved	3.0.0	08/04/06	Approved by GSA	Public
Revision	3.1.0	08/21/06	Submitted to GSA for Approval	Limited
Approved	4.0.0	08/24/06	Approved by GSA	Public
Approved	5.0.0	09/08/06	Updated content for the Application Package Submission. Updated requirements approval mechanisms.	Public
Revision	5.1.0	09/27/06	Updated based on feedback from GSA and submitted to GSA for Approval	GSA
Approved	6.0.0	09/28/06	Approved by GSA	Public
Approved	7.0.0	11/16/06	Updated to include requirement for SHA256 with RSA 2048 bit keys	Public
Approved	8.0.0	02/09/07	Updated to include process for product updates, resubmissions and evaluation fees	Public
Approved	9.0.0	04/02/07	Updated with details for the evaluation fees.	Public
Approved	10.0.0	04/26/07	Updated with details for the upgrade process.	Public
Revision	10.1.0	07/17/07	Revised Reqt. EP 53 to be consistent with SP 800-76-1 and INCITS 385.	GSA
Approved	11.0.0	07/19/07	Approved by GSA	Public
Revision	11.1.0	10/09/07	Revised to update requirements for SP 800-78-1 requirements. Updated to split approval processes from document. Processes can now be found in Suppliers Handbook.	GSA
Approved	12.0.0	10/31/07	Approved by GSA	Public

## Table of Contents

<b>1</b>	<b>Introduction</b> .....	1
<b>1.1</b>	<b>Overview</b> .....	1
<b>1.2</b>	<b>Category Description</b> .....	1
<b>1.3</b>	<b>Purpose</b> .....	1
<b>2</b>	<b>Application Package Contents</b> .....	3
<b>3</b>	<b>Evaluation Procedure for Graphical Personalization</b> .....	5
<b>3.1</b>	<b>Requirements</b> .....	5
<b>3.2</b>	<b>Approval Mechanism Matrix</b> .....	36
<b>3.3</b>	<b>Evaluation Criteria</b> .....	36
3.3.1	Vendor Documentation Review.....	36
3.3.2	Vendor Test Data Report .....	38
3.3.2.1	EP.8.....	38
3.3.2.2	EP.51 .....	38
3.3.2.3	EP.53 .....	39
3.3.2.4	EP.55.....	39
3.3.2.5	EP.167, EP.168 .....	40
3.3.3	Lab Test Data Report .....	41
3.3.4	Certification .....	41
3.3.5	Attestation.....	42
	<b>Appendix A: Generation of PIV Data Objects by the Product</b> .....	43

## List of Tables

Table 1 - Applicable Requirements .....	35
Table 2 - Approval Mechanism Matrix .....	36

## 1 Introduction

### 1.1 Overview

The FIPS 201 Evaluation Program (EP) is a U.S. Government entity administered by the Office of Government-wide Policy (OGP), within the General Services Administration (GSA) agency. The goal of the FIPS 201 Evaluation Program (EP) is to evaluate products and services against the requirements outlined in FIPS 201 and its supporting documents. In addition to derived test requirements developed to test conformance to the National Institute of Standards and Technology (NIST) Standard, GSA has also established interoperability and performance metrics to further determine product suitability. A set of approval and test procedures have been developed which outline the evaluation criteria, approval mechanisms and test process employed by the Laboratory during their evaluation of a Supplier's product or service against the requirements for that category.

A Supplier desiring to submit a Electronic Personalization Product (hereafter referred to as the Product) for evaluation must follow the Suppliers Policies and Procedures Handbook. In addition to this handbook, Supplier also need to refer to this Approval Procedure which provides the necessary category-specific details in order to have a Supplier's Product evaluated by the EP and placed on the Approved Products List (APL).

### 1.2 Category Description

The *Electronic Personalization* product generates and loads the mandatory objects as well as any optional objects defined by SP 800-73, to a PIV Card. More specifically, the Product is responsible for generating and/or populating the mandatory data objects on personalized cards; the Card Capabilities Container, Cardholder Unique Identifier (CHUID), PIV Authentication Certificate, biometric fingerprints, and Security Object, as well as optional data elements such as the biometric facial image, printed information, and optional X.509 digital certificates for digital signature, card authentication and key management. Since, the product is responsible for formatting and loading all data containers on the PIV Card, this implies that the Product must contain the capability to maintain an interface to a Certification Authority(CA) which participates in the Federal Public Key Infrastructure Architecture, managed by the Federal PKI.

**Note:** *The effective date for SP 800-78-1 conformance has been set by NIST for January 1, 2008. Products submitted to GSA EP Labs under this category may conform to the signature and key size requirements of SP 800-78 or SP 800-78-1. Suppliers submitting must to state which special publication their offering is conformant in the Attestation Form. The Product submitted will be held to the applicable requirements for the appropriate Special Publication to which conformance is being achieved.*

### 1.3 Purpose

The purpose of this document is to provide the following information:

- (i) Provide a list of the artifacts and/or documentation that needs to be submitted to the Evaluation Lab as part of the application package submission.

- (ii) Document the list of the requirements that apply to this category
- (iii) Specify the evaluation criteria along with their approval mechanisms that will be used by Evaluation Labs to verify compliance of the Product against the requirements that apply to this category.

## 2 Application Package Contents

The Application Package Contents include the artifacts, documentation and in some cases the product itself that needs to be submitted to the Evaluation Lab so that evaluation can be performed. The Application Package Contents for this category include the following:

- An electronically personalized PIV Card. The card should include all of the objects that can possibly be loaded by the Product. This should be delivered to the Lab (address can be found at <http://fips201ep.cio.gov/labs.php>) using a reliable method of delivery that requires acknowledgement of receipt (e.g., FedEx, UPS, hand delivery) At a minimum, Electronically Personalized PIV Cards should contain: (i) Card Capabilities Container; (ii) CHUID (iii) PIV Authentication Certificate; (iv) Biometric Fingerprints and (v) Security Object. Optionally, submitted cards may also contain: (i) Facial Image, (ii) Printed Information, (iii) Digital Signature Certificate; (iv) Key Management Certificate, and (v) Card Authentication Certificate.

Please note that if the Supplier chooses to have the content of the certificates populated on the card evaluated, the certificates must come from a Certification Authority (CA) that participates in the Federal Public Key Infrastructure Architecture, managed by the Federal PKI.

Additionally, the Supplier needs to provide the following information to the Lab:

- PIV Card Application Administration Key (i.e. key reference value: 9B) in ASCII hexadecimal format;
- PIN; and
- PIN Unblock Value.
- Completed Application Form, provided on the Evaluation Program website. (This form will be available through the web interface once users have been assigned a login credential);
- Completed and signed Lab Service Agreement (found in the application submission package ZIP file). The Lab Service Agreement should be completed and scanned into a document to be uploaded to Evaluation Program website;
- Completed and signed Attestation Form (found in the application submission package ZIP file). The Attestation Form should be completed and scanned into a document to be uploaded to Evaluation Program website;
- Completed Supplier VDR-VTDR justification worksheet (found in the application submission package ZIP file);
- A Vendor Test Data Report, which provides test results showing that the Product complies with the requirements for this category. In this regard, the Supplier is expected to develop and document the test procedures used to determine how the Product was tested to arrive at the conclusion that it met all necessary requirements. The VTDR must typically contain information as stated in Section 3.2. Wherever possible, information to be supplied as part of this Vendor Test Data Report has been described in Section 4.3;

- Official Certification documentation from the appropriate entity (e.g., NIST) showing conformance of the Product to the tested requirements of FIPS 201. Specific reference to the exact type of certification necessary can be found in Section 3.3; and
- All necessary Supplier documentation providing proof that the Product complies with the subset of requirements (as outlined in Section 4.1) for this category which has Supplier documentation review as its approval mechanism. Examples of specific documentation would include: user guides, technical specifications, white papers, line cards, etc.

Additionally, the Supplier needs to provide the following to the Lab:

- A sample INCITS 385 profile, if supported by the Product, provided by the Supplier, which has been formatted in a text file such that the individual fields in the profile are distinguishable by the human eye. Where appropriate, notes have been added by the Supplier to clarify the interpretation of a particular flag. For example, the flag 0x10 in the hair color field indicates that the subject is bald.
- The electronic version of the photograph that is included in the INCITS 385 profile.
- The completed table, presented in Appendix A<sup>1</sup>, that identifies the modules responsible for generating the data objects loaded by the Product on the PIV Card.

---

<sup>1</sup> Irrespective of Appendix A, the cards submitted for evaluation shall contain the mandatory data objects as stated in the list of application package contents.

**3 Evaluation Procedure for Electronic Personalization**

**3.1 Requirements**

In order to approve the Service as conformant to the requirements of PIV, it at a minimum, must comply with all the requirements listed below. The approval mechanism column describes the technique utilized by the Lab to evaluate compliance to that particular requirement.

Identifier #	Requirement Description	Source	Req. #	Approval Mechanism
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	2-51	Vendor Documentation Review  Lab Test Data Report
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	2-52	Vendor Documentation Review
EP.3	The PIV Card shall include the following objects as defined in SP 800-73-1: <ul style="list-style-type: none"> <li>• Card Capabilities Container</li> <li>• CHUID</li> <li>• PIV Authentication Key Pair</li> <li>• Biometric Fingerprints</li> <li>• Security Object</li> </ul>	FIPS 201-1, Section 4.2	2-54	Vendor Documentation Review
EP.4	The PIV Card may include the following objects as defined in SP 800-73-1. <ul style="list-style-type: none"> <li>• Biometric Facial Image</li> <li>• Printed Information</li> <li>• Digital Signature Key Pair</li> </ul>	Derived	N/A	Vendor Documentation Review

	<ul style="list-style-type: none"> <li>• Key Management Key Pair</li> <li>• Card Management Key</li> <li>• Card Authentication Key Pair</li> </ul>			
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	N/A	Certification
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	N/A	Vendor Documentation Review
EP.7	When facial imagery is stored on the PIV Card, only one image shall be stored.  <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	SP 800-76-1, Section 5.2	N/A	Vendor Documentation Review
EP.8	The personalized card shall be tested by the SP 800-85B test tool for data format compliance.	Derived	N/A	Vendor Test Data Report Lab Test Data Report
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	N/A	Vendor Documentation Review
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	N/A	Lab Test Data Report
EP.11	The CCC shall contain the mandatory BER-TLV fields	SP 800-73-1,	N/A	Lab Test Data

	as specified and identify the registered data model number 0x10.	Appendix A		Report
EP.12	<p>The CHUID on a PIV card shall meet the following requirements:</p> <ul style="list-style-type: none"> <li>• The length of the CHUID is indicated in BER-TLV format, identified by tag 0xEE.</li> <li>• 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.</li> <li>• The Global Unique Identifier (GUID) field must be present, and may include either an issuer assigned IPv6 address or be coded as all zeros.</li> <li>• 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.</li> </ul>	SP 800-73-1, Section 1.8.3	N/A	Lab Test Data Report
EP.13	The fingerprint buffer specifies the primary and secondary fingerprints within Tag value 0xBC.	SP 800-73-1, Appendix A	N/A	Lab Test Data Report

EP.14	The fingerprint template length shall not exceed 4,000 bytes.	SP 800-73-1, Appendix A	N/A	Lab Test Data Report
EP.15	The facial image is preceded with tag value 0xBC <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	SP 800-73-1, Appendix A	N/A	Lab Test Data Report
EP.16	The facial image length shall not exceed 12,704 bytes <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	SP 800-73-1, Appendix A	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.20	The Patron Header Version of the CBEFF Patron Format shall be 0x03.	SP 800-76-1, Section 6	N/A	Lab Test Data Report
EP.21	The biometric data block is digitally signed but not encrypted, and this shall be reflected by setting the value	SP 800-76-1, Section 6	N/A	Lab Test Data Report

	of the Signature Block Header (SBH) security options field to b00001101.			
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.26	Biometric Type field within the PIV Patron Format shall be 0x000008 for fingerprint template and shall be 0x000002 for facial images.	SP 800-76-1, Section 6	N/A	Lab Test Data Report

	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.			
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	N/A	Lab Test Data Report
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 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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report

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	N/A	Lab Test Data Report
EP.31	The "Reserved for future use" field in the PIV Patron Format shall contain 0x00000000.	SP 800-76-1, Section 6	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.34	The Format Identifier of the General Header Record shall be 0x464D5200.	SP 800-76-1, Section 3.3.2	N/A	Lab Test Data Report
EP.35	The Version Number of the General Header Record shall be 0x20323000.	SP 800-76-1, Section 3.3.2	N/A	Lab Test Data Report
EP.36	The length of the entire CBEFF wrapped record shall fit within the container size limits specified in SP 800-73-1.	Derived	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.39	The Capture Equipment	SP 800-76-1,	N/A	Lab Test Data

	Compliance of the General Record Header shall be 1000b.	Section 3.3.2		Report
EP.40	The Capture Equipment ID of the General Record Header is greater than zero.	SP 800-76-1, Section 3.3.2	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.42	The Number of Views of the General Header Record shall be 2.	SP 800-76-1, Section 3.3.2	N/A	Lab Test Data Report
EP.43	The Reserved Byte of the General Header Record shall be 0.	SP 800-76-1, Section 3.3.2	N/A	Lab Test Data Report
EP.44	The View Number of the Single Finger View Record shall be 0.	SP 800-76-1, Section 3.3.2	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.47	The Number of Minutiae of Single Finger View Record is between 0 and 128.	SP 800-76-1, Section 3.3.2	N/A	Lab Test Data Report
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	SP 800-76-1, Section 3.3.2	N/A	Lab Test Data Report

	encoded as 00b.			
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	N/A	Certification
EP.50	The mandatory value for Extended Data Block Length for MINUSTD template shall be zero.	SP 800-76-1, Section 3.3.2	N/A	Lab Test Data Report
EP.51	All facial images must conform to the requirements in SP 800-76-1 Table 6, “INCITS 385 Profile for PIV Facial Images.”  <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	SP 800-76-1, Section 5.2	N/A	Vendor Test Data Report Lab Test Data Report
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.  <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	Derived	N/A	Lab Test Data Report
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 ratio of 7:4 defined in Section 8.3.4 of INCITS 385.  <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	SP 800-76-1, Section 5.2 INCITS 385, Section 8.3.4	N/A	Vendor Test Data Report Lab Test Data Report

EP.54	<p>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.</p> <p><i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i></p>	SP 800-76-1, Section 5.2	N/A	Vendor Documentation Review
EP.55	<p>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.</p> <p><i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i></p>	SP 800-76-1, Section 5.2	N/A	Vendor Test Data Report
EP.56	<p>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.</p>	FIPS 201-1, Section 4.2.2	N/A	Lab Test Data Report
EP.57	<p>The digital signature is implemented as a SignedData Type.</p>	FIPS 201-1, Section 4.2.2	N/A	Lab Test Data Report
EP.58	<p>The value of the version field of the SignedData content type shall be v3.</p>	FIPS 201-1, Section 4.2.2	N/A	Lab Test Data Report
EP.59	<p>The digestAlgorithms field of the SignedData content type shall be in accordance with Table 3-3 of SP 800-78-1.</p>	FIPS 201-1, Section 4.2.2	N/A	Lab Test Data Report

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	N/A	Lab Test Data Report
EP.61	The encapContentInfo of the SignedData content type shall omit the eContent field.	FIPS 201-1, Section 4.2.2	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.63	The crls field from the SignedData content type shall be omitted.	FIPS 201-1, Section 4.2.2	N/A	Lab Test Data Report
EP.64	The SignerInfos in the SignedData content type shall contain only a single SignerInfo type.	FIPS 201-1, Section 4.2.2	N/A	Lab Test Data Report
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		Lab Test Data Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.68	The signedAttrs of the SignerInfo shall include the pivSigner-DN (OID = 2.16.840.1.101.3.6.5) attribute	FIPS 201-1, Section 4.2.2	N/A	Lab Test Data Report

	containing the subject name that appears in the X.509 certificate for the entity that signed the CHUID.			
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	N/A	Lab Test Data Report
EP.70	The SignedData content type shall include the digital signature.	FIPS 201-1, Section 4.2.2	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.74	The digital signature is implemented as a SignedData Type.	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report

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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.78	The encapContentInfo of the SignedData content type shall omit the eContent field.	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.80	The crls field from the SignedData content type shall be omitted.	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
EP.81	The signerInfos in the SignedData content type shall contain only a single SignerInfo type.	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.84	The signedAttrs of the SignerInfo shall include the	FIPS 201-1,	N/A	Lab Test Data

	MessageDigest (OID = 1.2.840.113549.1.9.4) attribute containing the hash of the concatenated CBEFF_HEADER and the STD_BIOMETRIC_RECORD.	Section 4.4.2		Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.88	The SignedData content type shall include the digital signature.	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
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	SP 800-78-1, Section 3.2.1	N/A	Lab Test Data Report

	the object, in accordance with Table 3-3 of SP 800-78-1.			
EP.91	The CBEFF_SIGNATURE_BLOCK shall be encoded as a Cryptographic Message Syntax external digital signature as defined in RFC 3852.  <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
EP.92	The digital signature is implemented as a SignedData Type.  <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
EP.93	The value of the version field of the SignedData content type shall be v3.  <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
EP.94	The digestAlgorithms field of the SignedData content type shall be in accordance with Table 3-3 of SP 800-78-1.  <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	SP 800-78-1, Section 3.2.1	N/A	Lab Test Data Report
EP.95	The eContentType of the encapContentInfo shall be id-PIV-biometricObject (OID = 2.16.840.1.101.3.6.2).  <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
EP.96	The encapContentInfo of the SignedData content type shall omit the eContent field.  <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report

<p>EP.97</p>	<p>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.</p> <p><i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i></p>	<p>FIPS 201-1, Section 4.4.2</p>	<p>N/A</p>	<p>Lab Test Data Report</p>
<p>EP.98</p>	<p>The crls field from the SignedData content type shall be omitted.</p> <p><i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i></p>	<p>FIPS 201-1, Section 4.4.2</p>	<p>N/A</p>	<p>Lab Test Data Report</p>
<p>EP.99</p>	<p>The signerInfos in the SignedData content type shall contain only a single SignerInfo type.</p> <p><i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i></p>	<p>FIPS 201-1, Section 4.4.2</p>	<p>N/A</p>	<p>Lab Test Data Report</p>
<p>EP.100</p>	<p>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.</p> <p><i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i></p>	<p>FIPS 201-1, Section 4.4.2</p>	<p>N/A</p>	<p>Lab Test Data Report</p>
<p>EP.101</p>	<p>The SignerInfo type shall specify a digestAlgorithm in accordance with Table 3-3 of SP 800-78-1.</p> <p><i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i></p>	<p>SP 800-78-1, Section 3.2.1</p>	<p>N/A</p>	<p>Lab Test Data Report</p>

	<i>in the card provided to the Lab)</i>			
EP.102	<p>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.</p> <p><i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i></p>	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
EP.103	<p>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.</p> <p><i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i></p>	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
EP.104	<p>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.</p> <p><i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i></p>	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
EP.105	<p>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.</p> <p><i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i></p>	SP 800-78-1, Section 3.2.1	N/A	Lab Test Data Report

EP.106	The SignedData content type shall include the digital signature.  <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
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).  <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
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.  <i>(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)</i>	SP 800-78-1, Section 3.2.1	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.110	The security object buffer shall contain an asymmetric digital signature as specified in RFC (3852).	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
EP.111	The digital signature is implemented as a SignedData Type.	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report
EP.112	The value of the version field of the SignedData content type shall be v3.	FIPS 201-1, Section 4.4.2	N/A	Lab Test Data Report

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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.116	The certificates field shall be omitted since it is included in the CHUID.	SP 800-73-1-1, Section 1.8.5	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.119	The SignedData content type shall include the digital signature.	Derived	N/A	Lab Test Data Report
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	N/A	Lab Test Data Report
EP.121	The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in	SP 800-78, Section 3.2.1	N/A	Lab Test Data Report

	<p>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.</p> <p><i>(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)</i></p>			
EP.122	<p>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.</p> <p><i>(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)</i></p>	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9	N/A	Lab Test Data Report
EP.123	<p>The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78.</p> <p><i>(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)</i></p>	SP 800-78, Section 3.2.2	N/A	Lab Test Data Report
EP.124	<p>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.</p>	SP 800-78, Section 3.2.2	N/A	Lab Test Data Report

	<i>(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)</i>			
EP.125	The keyUsage extension shall assert only the digitalSignature bit. No other bits shall be asserted.  <i>(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)</i>	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9	N/A	Lab Test Data Report
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).  <i>(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)</i>	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9	N/A	Lab Test Data Report
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.  <i>(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)</i>	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9	N/A	Lab Test Data Report
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).	FIPS 201-1, Section 4.3	N/A	Lab Test Data Report

	<i>(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)</i>			
EP.129	<p>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.</p> <p><i>(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)</i></p>	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9	N/A	Lab Test Data Report
EP.130	<p>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.</p> <p><i>(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)</i></p>	SP 800-78, Section 3.1	N/A	Lab Test Data Report
EP.131	<p>The public key present in the PIV authentication certificate correspond to the PIV authentication private key.</p> <p><i>(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)</i></p>	FIPS 201-1, Section 4.3	N/A	Lab Test Data Report
EP.132	<p>The FASC-N in the subjectAltName field in the PIV authentication certificate is the same as the FASC-N present in the CHUID.</p> <p><i>(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)</i></p>	Derived	N/A	Lab Test Data Report
EP.133	<p>The expiration of the PIV authentication certificate is not beyond the expiration of</p>	FIPS 201-1, Section 4.3	N/A	Lab Test Data Report

	<p>the CHUID.</p> <p><i>(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)</i></p>			
EP.134	<p>If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537.</p> <p><i>(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)</i></p>	SP 800-78, Section 3.1	N/A	Lab Test Data Report
EP.135	<p>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.</p> <p><i>(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)</i></p>	SP 800-78, Section 3.1	N/A	Lab Test Data Report
EP.136	<p>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.</p> <p><i>(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)</i></p>	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	N/A	Lab Test Data Report
EP.137	<p>The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78.</p> <p><i>(This requirement will be evaluated</i></p>	SP 800-78, Section 3.2.2	N/A	Lab Test Data Report

	<i>only if the digital signature certificate is issued by an authorized Certification Authority)</i>			
EP.138	<p>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.</p> <p><i>(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)</i></p>	<p>SP 800-78, Section 3.2.2</p> <p>X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5</p>	N/A	Lab Test Data Report
EP.139	<p>The keyUsage extension shall assert both the digitalSignature and nonRepudiation bits. No other bits shall be asserted.</p> <p><i>(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)</i></p>	<p>X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5</p>	N/A	Lab Test Data Report
EP.140	<p>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.</p> <p><i>(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)</i></p>	<p>SP 800-78, Section 3.1</p>	N/A	Lab Test Data Report
EP.141	<p>The public key present in the digital signature certificate corresponds to the digital signature private key.</p> <p><i>(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)</i></p>	<p>FIPS 201-1, Section 4.3</p>	N/A	Lab Test Data Report
EP.142	<p>The expiration of the digital signature certificate is not beyond the expiration of the</p>	<p>SP 800-78, Section 3.1</p>	N/A	Lab Test Data Report

	<p>CHUID.</p> <p><i>(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)</i></p>			
EP.143	<p>If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537.</p> <p><i>(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)</i></p>	SP 800-78, Section 3.1	N/A	Lab Test Data Report
EP.144	<p>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.</p> <p><i>(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)</i></p>	SP 800-78, Section 3.2.1	N/A	Lab Test Data Report
EP.145	<p>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.</p> <p><i>(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)</i></p>	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	N/A	Lab Test Data Report
EP.146	<p>The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78.</p> <p><i>(This requirement will be evaluated</i></p>	SP 800-78, Section 3.2.2	N/A	Lab Test Data Report

	<i>only if the key management certificate is issued by an authorized Certification Authority)</i>			
EP.147	<p>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.</p> <p><i>(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)</i></p>	SP 800-78, Section 3.2.2	N/A	Lab Test Data Report
EP.148	<p>If the public key algorithm is RSA, then the keyUsage extension shall only assert the keyEncipherment bit.</p> <p><i>(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)</i></p>	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	N/A	Lab Test Data Report
EP.149	<p>If the public key algorithm is Elliptic Curve, then the keyUsage extension shall only assert the keyAgreement bit.</p> <p><i>(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)</i></p>	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	N/A	Lab Test Data Report
EP.150	<p>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.</p> <p><i>(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)</i></p>	SP 800-78, Section 3.1	N/A	Lab Test Data Report
EP.151	<p>The public key present in the key management certificate</p>	FIPS 201-1, Section 4.3	N/A	Lab Test Data Report

	<p>corresponds to the key management private key.</p> <p><i>(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)</i></p>			
EP.152	<p>If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537.</p> <p><i>(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)</i></p>	SP 800-78, Section 3.1	N/A	Lab Test Data Report
EP.153	<p>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.</p> <p><i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i></p>	SP 800-78, Section 3.2.1	N/A	Lab Test Data Report
EP.154	<p>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.</p> <p><i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i></p>	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	N/A	Lab Test Data Report
EP.155	<p>The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78.</p>	SP 800-76, Section 3.2.2	N/A	Lab Test Data Report

	<i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i>			
EP.156	<p>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.</p> <p><i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i></p>	<p>SP 800-78, Section 3.2.2</p> <p>X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6</p>	N/A	Lab Test Data Report
EP.157	<p>The keyUsage extension shall assert only the digitalSignature bit. No other bits shall be asserted.</p> <p><i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i></p>	<p>X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6</p>	N/A	Lab Test Data Report
EP.158	<p>The policyIdentifier field in the certificatePolicies must assert id-fpki-common-cardAuth (OID = 2.16.840.1.101.3.2.1.3.17).</p> <p><i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i></p>	<p>X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6</p>	N/A	Lab Test Data Report
EP.159	<p>The extKeyUsage extension shall assert id-PIV-cardAuth (OID = 2.16.840.1.101.3.6.8). This extension is critical.</p> <p><i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i></p>	<p>X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6</p>	N/A	Lab Test Data Report
EP.160	<p>The authorityInfoAccess field shall contain an id-ad-ocsp</p>	<p>X.509 Certificate</p>	N/A	Lab Test Data

	<p>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.</p> <p><i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i></p>	<p>and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6</p>		<p>Report</p>
EP.161	<p>The FASC-N shall be populated in the subjectAltName extension using the pivFASC-N attribute OID = 2.16.840.1.101.3.6.6).</p> <p><i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i></p>	<p>X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6</p>	N/A	<p>Lab Test Data Report</p>
EP.162	<p>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.</p> <p><i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i></p>	<p>X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6</p>	N/A	<p>Lab Test Data Report</p>
EP.163	<p>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.</p> <p><i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i></p>	<p>SP 800-76, Section 3.1</p>	N/A	<p>Lab Test Data Report</p>
EP.164	<p>The public key present in the card authentication certificate</p>	<p>FIPS 201-1, Section 4.3</p>	N/A	<p>Lab Test Data Report</p>

	<p>correspond to the card authentication private key.</p> <p><i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i></p>			
EP.165	<p>The FASC-N in the subjectAltName field in the card authentication certificate is the same as the FASC-N present in the CHUID.</p> <p><i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i></p>	Derived	N/A	Lab Test Data Report
EP.166	<p>If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537.</p> <p><i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i></p>	SP 800-78, Section 3.1	N/A	Lab Test Data Report
EP.167	<p>If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537.</p> <p><i>(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)</i></p>	SP 800-78, Section 3.1	2-84	Vendor Documentation Review
EP.168	<p>If the public key size of the certificate that signs the CHUID, Biometrics and Security Object is 2048 bits or greater, then the hash 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])</p>	Derived	N/A	Vendor Test Data Report Lab Test Data Report
EP.169	<p>If the public key size of the PIV Authentication, Digital</p>	Derived	N/A	Vendor Test Data Report

	<p>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])</p> <p><i>(This requirement will be evaluated only if the above listed certificates are issued by an authorized Certification Authority)</i></p>			<p>Lab Test Data Report</p>
--	--	--	--	-----------------------------

**Table 1 - Applicable Requirements**

### 3.2 Approval Mechanism Matrix

The table below provides an indication of the total number of requirements applicable for the Product and provides a breakup of how the evaluation will be conducted based on the different approval mechanisms available to the Lab.

Total Requirements	Approval Mechanisms					
	SV	VTDR	LTDR	VDR	C	A
169	N/A	6	158	9	2	1
<b>Legend:</b> SV – Site Visit; VTDR – Vendor Test Data Report; LTDR – Lab Test Data Report; VDR – Vendor Doc. Review; C – Certification; A - Attestation						

Table 2 - Approval Mechanism Matrix

### 3.3 Evaluation Criteria

This section provides details on the process employed by the Lab for evaluating the Product against the requirements enumerated above.

#### 3.3.1 Vendor Documentation Review

<b>Reference(s):</b>	EP.1 to EP.4, EP.6, EP.7, EP.9, EP.54, EP.167
<b>Evaluation Procedure:</b>	<ol style="list-style-type: none"> <li>1. The Lab will update the status in the Web-Enabled Tool to “VDR Begun” as instructed in the Web-enabled Tool Laboratory User Guide.</li> <li>2. The Lab will review the Product’s documentation to determine the following. At a minimum the documents submitted by the Supplier must include:                         <ul style="list-style-type: none"> <li>▪ <i>Data Loading (EP.1, EP.167)</i> <ul style="list-style-type: none"> <li>• A statement indicating that authentication to the card using the Card Management Key through a challenge-response protocol is required to load or update any data which resides on the PIV Application.</li> <li>• A procedure which documents the exact steps, including APDUs, to update a produced card using the Card Management Key or similar cryptographic mechanism.</li> <li>• A statement which discusses how the card management key is loaded by the Issuer using the product.</li> </ul> </li> <li>▪ <i>Cryptographic Keys (EP.2)</i> <ul style="list-style-type: none"> <li>• A statement indicating that unique card management keys are issued to each PIV Card personalized.</li> <li>• A procedure which details how the uniqueness of card management keys are ensured by the product.</li> </ul> </li> <li>▪ <i>Population of Data Objects (EP.3, EP.4)</i></li> </ul> </li> </ol>

	<ul style="list-style-type: none"> <li>• A statement indicating that the following data objects are loaded onto personalized PIV Cards, as defined in FIPS 201 and SP 800-73-1:             <ul style="list-style-type: none"> <li>○ Card Capabilities Container</li> <li>○ CHUID</li> <li>○ PIV Authentication Key Pair</li> <li>○ Biometric Fingerprints</li> <li>○ Security Object</li> <li>○ Biometric Facial Image</li> <li>○ Printed Information</li> <li>○ Digital Signature Key Pair</li> <li>○ Key Management Key Pair</li> <li>○ Card Management Key</li> <li>○ Card Authentication Key Pair</li> </ul> </li> <li>▪ <i>Biometric Data Conformance (EP.6, EP.7)</i> <ul style="list-style-type: none"> <li>• A statement indicating that the primary and secondary biometric fingerprint templates are stored in one minutiae template on the PIV Card.</li> <li>• A statement indicating that, when used, only one facial image is stored on the PIV Card.</li> </ul> </li> <li>▪ <i>Data Object Tags (EP.9)</i> <ul style="list-style-type: none"> <li>• Data objects populated in containers shall contain all appropriate tags and lengths for each element in the object.</li> </ul> </li> <li>▪ <i>Encoding and Compression Format of Facial Images (EP.54)</i> <ul style="list-style-type: none"> <li>• Indication of the encoding format used by the Product                 <ul style="list-style-type: none"> <li>a. JPEG</li> <li>b. JPEG-2000</li> </ul> </li> <li>• Indication the compression format is utilized by the Product.                 <ul style="list-style-type: none"> <li>a. whole-image</li> <li>b. single-region-of-interest (ROI)</li> </ul> </li> </ul> </li> <li>▪ <i>Card Management Key Importation (EP.167)</i> <ul style="list-style-type: none"> <li>• A statement indicating that the Service Provider imports the card management key onto the PIV Card.</li> <li>• The technical process (diagrams and/or APDUs) for importing the Card Management Key to the PIV Card.</li> </ul> </li> </ul> <p>3. The Lab will update the status to “VDR Complete” as instructed in the Web-enabled Tool Laboratory User Guide.</p>
<p><b>Expected Result:</b></p>	<p>1. Electronically Personalized PIV Cards require authentication through a cryptographic key-based challenge-response protocol, using the Card Management Key, before data can be written to the card.</p> <p>2. Unique Card Management Keys are loaded onto the card by the</p>

	<p>issuer of the personalized PIV Card.</p> <p>3. Electronically Personalized PIV Cards contain at a minimum the mandatory elements as defined SP 800-73-1.</p> <p>4. Primary and secondary biometrics are stored on the card and when facial imagery is used, only one image is stored on the card.</p> <p>5. The Product uses the appropriate encoding/compression formats for facial images.</p>
--	---

3.3.2 Vendor Test Data Report

The Lab will update the status in the Web-Enabled Tool to “VTDR Begun” as instructed in the Web-enabled Tool Laboratory User Guide.

3.3.2.1 EP.8

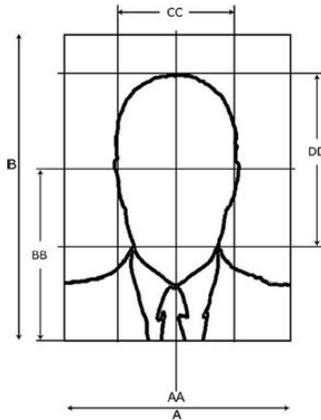
<b>Evaluation Procedure:</b>	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> <li>• <i>Data Model Conformance:</i> The Product is capable of being electronically personalized to meet the requirements of FIPS 201 and supporting documentation.</li> </ul> <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> <li>a. A report generated as a result of running the NIST SP 800-85B test tool by the Supplier against a PIV Card personalized by the Product.</li> </ol> <p>* Note: The SP 800-85B test tool can be found at the following location: <a href="http://fips201ep.cio.gov/tools.php">http://fips201ep.cio.gov/tools.php</a></p>
<b>Expected Result:</b>	<p>The PIV Card tested has successfully completed the NIST SP 800-85B validation for PIV data conformance by the Supplier.</p>

3.3.2.2 EP.51

<b>Evaluation Procedure:</b>	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> <li>• <i>INCITS 385 Profile Conformance:</i> The facial image shall be formatted as part of an INCITS 385 profile. The mandatory fields and values found in SP 800-76-1, Table 6 are present.</li> </ul> <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> <li>a. Convert the binary representation of the INCITS 385 to textual form.</li> <li>b. In the textual form, ensure that the fields that are</li> </ol>
------------------------------	---

	present in the submitted profile correspond to the values found in Table 6. All mandatory data values, such as the Format Identifier (“FAC\0” in ASCII), must be present and cross references to data values such as hair color and eye color must be made explicit.
<b>Expected Result:</b>	The submitted INCITS 385 profile is conformant to SP 800-76-1 Table 6.

3.3.2.3 EP.53

<b>Evaluation Procedure:</b>	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> <li>• <i>Full Frontal Image Type:</i> The electronic image submitted conforms to the diagram listed below.</li> </ul>  <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> <li>Measure the image width. This value is A. The width of A should exceed 420 pixels. Measure the width of the head. This value is CC. The width of CC should exceed 240 pixels. Find the ratio of the two widths: (Image Width : Head Width). This ratio must be 7:4 (A:CC). The electronic version of this measurement may be submitted to expedite the Lab’s evaluation of this requirement.</li> </ol>
<b>Expected Result:</b>	The full frontal image type meets the minimum spatial resolution and specified ratio of image width to head width of 7:4.

3.3.2.4 EP.55

<b>Evaluation Procedure:</b>	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> <li>• <i>Image Compression:</i> Facial images are compressed no more</li> </ul>
------------------------------	---

	<p>than 15: 1. If ROI compression is used then the innermost region is centered around the face and compressed at no more than 24:1.</p> <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <p><u>For regular compression</u></p> <ol style="list-style-type: none"> <li>a. Note down the size of the raw image obtained.</li> <li>b. Compress the image using appropriate compression format and encoding</li> <li>c. Note down the size of the compressed image.</li> </ol> <p><u>For ROI compression</u></p> <ol style="list-style-type: none"> <li>a. Using the raw image, extract the ROI.</li> <li>b. Note down the size of the ROI to be compressed</li> <li>c. Compress the image using appropriate compression format and encoding</li> <li>d. Note down the size of the final ROI</li> </ol>
<b>Expected Result:</b>	The test report indicates that an appropriate level of compression has been applied to the image for regular or ROI compression.

3.3.2.5 EP.168, EP.169

<b>Evaluation Procedure:</b>	<p>The Lab will review the documentation submitted by the Supplier to ascertain the following:</p> <ul style="list-style-type: none"> <li>• <i>Signature Generation:</i> Data that is digitally signed (Certificates, CHUID, Biometrics or Security Object) is hashed using the SHA256 algorithm when signed with a 2048 bit RSA key.</li> </ul> <p>At a minimum, the following test scenario must be performed to confirm compliance:</p> <ol style="list-style-type: none"> <li>a. Generate the data that is to be loaded on the card (Certificate, CHUID, etc)</li> <li>b. Using an ASN.1 utility, perform a dump of the data object such that it retains the ASN.1 syntax formatting</li> <li>c. Explicitly state which object the ASN.1 dump represents</li> </ol>
<b>Expected Result:</b>	The ASN.1 dump clearly denotes the SHA256 OID used for performing the hash function when digitally signing the data with a 2048 bit key.

The Lab will update the status in the Web-Enabled Tool to “VTDR Complete” as instructed in the Web-enabled Tool Laboratory User Guide.

3.3.3 Lab Test Data Report

<b>Reference(s):</b>	EP.1, EP.8, EP.10 to EP.53, EP.56 to EP.169
<b>Test Procedure:</b>	<ol style="list-style-type: none"> <li>1. The Lab will update the status in the Web-Enabled Tool to “LTDR Begun” as instructed in the Web-enabled Tool Laboratory User Guide.</li> <li>2. The Lab will execute test procedures for this category in accordance with the “Electronic Personalization Test Procedure.”</li> <li>3. The Lab will update the status to “LTDR Complete” as instructed in the Web-enabled Tool Laboratory User Guide.</li> </ol>
<b>Expected Result:</b>	The Product successfully passes all the test cases documented within the test procedure.

3.3.4 Certification

<b>Reference(s):</b>	EP.5, EP.49
<b>Evaluation Procedure:</b>	<ol style="list-style-type: none"> <li>1. The Lab will update the status in the Web-Enabled Tool to “C Begun” as instructed in the Web-enabled Tool Laboratory User Guide.</li> <li>2. The Lab will perform the following activities for the device that generates Card Management Keys in order to determine certification status with FIPS 140-2 Level 2 requirements: <ul style="list-style-type: none"> <li>▪ Examine the certification statement to see if it is provided by NIST/CSE and that it is still current i.e. valid;</li> <li>▪ Verify the authenticity of this certification provided by NIST/CSE; and</li> <li>▪ Review the FIPS 140-2 Cryptographic Modules Validation List to determine inclusion of the Product and the level at which it has been certified. The list is available on the website located at: <a href="http://csrc.nist.gov/cryptval/140-1/1401val.htm">http://csrc.nist.gov/cryptval/140-1/1401val.htm</a>.</li> </ul> </li> <li>3. The Lab will perform the following activities for the Template Generator in order to determine certification status of the Product with SP 800-76-1 requirements: <ul style="list-style-type: none"> <li>▪ Examine the certification statement to see if it provided by NIST and that it is still current i.e. valid;</li> <li>▪ Verify the authenticity of this NIST certification as compliant to FIPS 201 and supporting documentation; and</li> <li>▪ Review the list of Template Generators to determine inclusion of the Product. The list is available on the website located at: <a href="http://fingerprint.nist.gov/MINEX/QPL.html">http://fingerprint.nist.gov/MINEX/QPL.html</a>.</li> </ul> </li> </ol>

	4. The Lab will update the status to “C Complete” as instructed in the Web-enabled Tool Laboratory User Guide.
<b>Expected Result:</b>	<ol style="list-style-type: none"> <li>1. The Cryptographic Module has been found to be certified by NIST/CSE at FIPS 140-2 Level 2.</li> <li>2. Template Generator used within the Product are approved under the NIST Template Generator certification process.</li> </ol>

3.3.5 Attestation

<b>Reference(s):</b>	N/A
<b>Evaluation Procedure:</b>	<ol style="list-style-type: none"> <li>1. The Lab will update the status in the Web-Enabled Tool to “A Begun” as instructed in the Web-enabled Tool Laboratory User Guide.</li> <li>2. Review the Attestation Form provided by the Supplier, confirming that the Product to the best of their knowledge, conforms to all the necessary requirements of the category under which the Product applies. Verify that person signing this Attestation Form has the authority to do so (a minimum “C” level [e.g. CSO, CEO, CIO, CFO, Vice-President, President, Business Partner or Owner]).</li> <li>3. The Lab will update the status in the Web-Enabled Tool to “A Complete” as instructed in the Web-enabled Tool Laboratory User Guide.</li> </ol>
<b>Expected Results:</b>	1. The Attestation Form has been signed by an authorized individual (e.g. CSO, CEO, CIO, CFO, Vice-President, President, Business Partner or Owner).

## Appendix A: Generation of PIV Data Objects by the Product

The table presented below states all objects that can potentially be generated and/or loaded onto the PIV Card by an Electronic Personalization Product. Please inform the Lab the containers that the Product is capable of generating by filling out the table below.

If the Product internally contains the functionality to generate a particular data object, mark the “Does the product generate?” column with a **Y** and state the vendor and software version of the module that has been integrated with the Product. If the Product does not contain the functionality to generate an object, mark the “Does the product generate?” column with an **N**. If the PIV Card submitted to the Lab doesn’t populate a particular container, please mark **N/A** in the “Does the product generate?” column.

Example 1: Supplier A’s Product incorporates an INCITS 378 minutiae template generator to extract the fingerprint image data from an INCITS 381 profile before putting the Biometric Fingerprint data object onto a PIV Card. Supplier A would mark the “Does the product generate?” column with a **Y** and state the vendor, product name, and software version of the template generator that has been integrated into their Electronic Personalization Product.

Example 2: Supplier B’s Product does not generate INCITS 378 templates at all. The Product either loads an already signed CBEFF wrapped INCITS 378 profile OR wraps and signs an existing INCITS 378 profile in a CBEFF structure. Both instances may be using INCITS 378 profiles which have been generated at the time of enrollment. The Supplier would mark the “Does the product generate?” column with an **N**, because the Product itself does not generate the INCITS 378 template.

Example 3: Supplier C’s Product does not have the capability to populate an optional container on the PIV Card (e.g. Digital Signature Certificate, Biometric Facial Image, etc.) The Supplier would mark the “Does the product generate?” column with **N/A**, because the product does not support populating optional containers to PIV Cards.

Object	Does the product generate? (Y/N/NA)	Vendor	Product	S/W Version
Card Capabilities Container	M			
CHUID	M			
PIV Authentication Certificate	M			
Biometric Fingerprint	M			
Security Object	M			
Printed Information	O			
Biometric Facial Image	O			
Digital Signature Certificate	O			
Key Management Certificate	O			
Card Authentication Certificate	O			

"M" stands for mandatory data; "O" stands for optional data