FIPS 201 Evaluation Program -
Electronic Personalization (Service) Approval Procedure

Version 12.0.0
October 31, 2007

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	04/27/06	Document creation	Limited
Draft	0.0.2	05/11/06	Update to the document	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	1.1.1	06/30/06	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
Revision	2.3.0	08/04/06	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	Public
Revision	5.0.1	10/09/06	Updated based on feedback from the Evaluation Lab	Limited
Revision	5.1.0	10/16/06	Submitted to GSA for Approval	GSA
Approved	6.0.0	10/18/06	Approved by GSA	Public
Revision	6.1.0	11/15/06	Updated to include requirement for SHA256 with RSA 2048 bit keys	GSA
Approved	7.0.0	11/16/06	Approved by GSA	Public
Revision	7.1.0	01/29/07	Updated based on feedback from GSA	GSA
Revision	7.2.0	02/26/07	Updated based on feedback from GSA	GSA
Approved	8.0.0	03/13/07	Approved by GSA	Public
Approved	9.0.0	04/04/07	Approved by GSA	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
Revision	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

List of Tables

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 an Electronic Personalization Service (hereafter referred to as the Service) 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* Service involves generating and loading, at a minimum, the mandatory objects as well as any optional objects, as defined by SP 800-73-1, to a PIV Card. More specifically, the Service Provider 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. The Service Provider is responsible for formatting and loading all data containers on the PIV Card, which implies that the certificates populated on the PIV Card shall be issued from a Certification Authority (CA) that participates in the hierarchical Federal PKI Framework for the Common Policy, 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 Service Provider. 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 hierarchical PKI for the Common Policy 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 Service 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. Supplier documentation should also specify the Certificate Authority for which X.509 certificates that are loaded onto PIV Cards are obtained.

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

  - A sample INCITS 385 profile, if supported by the Service Provider, 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[1], that identifies the components used to generate data objects on the PIV Card.
  - A list of the Supplier site(s) that will be electronically personalizing PIV Cards
  - Electronic Personalization Service Standard Operating Procedures
  - Human Resources Standard Operating Procedures
  - The background investigations service contract
  - The Security Plan for the facility
  - Server penetration reports for all servers which are publicly available on the Facility's network
  - The Security Equipment Inventory List
  - A screenshot of the PIV Card Automated Inventory Control System
  - Server security vulnerability report
  - Privacy Impact Assessment, which is in accordance with OMB Memoranda 06-06, Appendix E

[1] 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 (Service)

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	Reqt. #	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	1.1-93	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	1.1-94	Vendor Documentation Review
EP.3	The PIV Card shall include the following objects as defined in SP 800-73-1: • Card Capabilities Container • CHUID • PIV Authentication Key Pair • Biometric Fingerprints • Security Object	Derived	N/A	Vendor Documentation Review
EP.4	The PIV Card may include the following objects as defined in SP 800-73-1. • Biometric Facial Image • Printed Information • Digital Signature Key Pair • Key Management Key Pair • Card Management Key • Card Authentication Key Pair	Derived	N/A	Vendor Documentation Review
EP.5	The device which generates cryptographic keys shall be validated to FIPS 140-2 with an overall	FIPS 201-1, Section B.4	1.1-221	Certification

	Security Level 2 (or higher).			
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	2-11	Vendor Documentation Review
EP.7	When facial imagery is stored on the PIV Card, only one image shall be stored. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-76-1, Section 5.2	2-36	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	4.1-57	Lab Test Data Report
EP.11	The CCC shall contain the mandatory BER-TLV fields as specified and identify the registered data model number 0x10.	SP 800-73-1, Section 1.8.1	4.1-2	Lab Test Data Report
EP.12	The CHUID on a PIV card shall meet the following quirements: • The length of the CHUID is indicated in BER-TLV format, identified by tag 0xEE. • The Federal Agency Smart Credential Number (FASC-N) shall be consistent with the Technical Implementation Guidance Smart Card Enabled	SP 800-73-1, Section 1.8.3	4.1-4	Lab Test Data Report

	Physical Access Control System (TIG SCEPACS) Option for "System Code || Credential Number" to establish a credential number space of 9,999,999,999 credentials. • The Global Unique Identifier (GUID) field must be present, and may include either an issuer assigned IPv6 address or be coded as all zeros. • The Expiration Date is tagged 0x35 and value is within the next five years. This field shall be 8 bytes in length and shall be encoded as YYYYMMDD.			
EP.13	The fingerprint buffer specifies the primary and secondary fingerprints within Tag value 0xBC.	SP 800-73-1, Appendix A	4.1-60	Lab Test Data Report
EP.14	The fingerprint template length shall not exceed 4,000 bytes.	SP 800-73-1, Appendix A	4.1-60	Lab Test Data Report
EP.15	The facial image is preceded with tag value 0xBC *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-73-1, Appendix A	4.1-60	Lab Test Data Report
EP.16	The facial image length shall not exceed 12,704 bytes *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-73-1, Appendix A	4.1-60	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 800-76-1 Table 7, "Simple CBEFF Structure". Lengths of the biometric data must be less than 4,000 and 12,704 bytes for the fingerprint	SP 800-76-1, Section 6	N/A	Lab Test Data Report

	and facial image, respectively.			
EP.19	The CBEFF header must comply with SP 800-76-1 Table 8, “Patron Format PIV Specification”. Multi-byte integers must be in big-endian byte ordering.	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 of the Signature Block Header (SBH) security options field to b00001101.	SP 800-76-1, Section 6	N/A	Lab Test Data Report
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. The value for other biometric modalities shall be that given in CBEFF, 5.2.1.5. For modalities not listed there the value shall be 0x00.	SP 800-76-1, Section 6	N/A	Lab Test Data Report
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	SP 800-76-1, Section 6	N/A	Lab Test Data Report

	0x00000000.			
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 Compliance of the General Record Header shall be 1000b.	SP 800-76-1, Section 3.3.2	N/A	Lab Test Data 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 encoded as 00b.	SP 800-76-1, Section 3.3.2	N/A	Lab Test Data Report
EP.49	If used by the Service provider, the template generator used 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". *(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	N/A	Vendor Test Data Report Lab Test Data Report
EP.52	If facial imager is stored on the PIV card, the length of the entire record shall fit within the container size	Derived	N/A	Lab Test Data Report

	limits specified in SP 800-73-1. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*			
EP.53	The spatial resolution of the facial image shall be such that the width of the head shall be at least 240 pixels in width and the total width of the image at least 420 pixels in width as defined in the Normative Note #7 of Section 5.2 in SP 800-76-1. Widths exceeding the minimum requirements for spatial resolution should conform to the Image Width: Head Width ration of 7:4 defined in Section 8.3.4 of INCITS 385. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-76-1, Section 5.2 INCITS 385, Section 8.3.4	N/A	Vendor Test Data Report Lab Test Data Report
EP.54	Facial image data shall be formatted in one of the two compression formats enumerated in Section 6.2 of FACESTD. Both whole-image and single-region-of-interest (ROI) compression are permitted. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-76-1, Section 5.2	N/A	Vendor Documentation Review
EP.55	Facial images shall be compressed using a compression ratio no higher than 15:1. However, when facial images are stored on PIV cards, JPEG 2000 shall be used with ROI compression in which the innermost region shall be centered on the face and compressed at no more than 24:1. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-76-1, Section 5.2	N/A	Vendor Test Data Report
EP.56	The CHUID buffer shall contain an Asymmetric digital signature of the CHUID object, which has been encoded as a Cryptographic Message Syntax external digital signature as	FIPS 201-1, Section 4.2.2	1.1-100	Lab Test Data Report

	defined in RFC 3852.			
EP.57	The digital signature is implemented as a SignedData Type.	FIPS 201-1, Section 4.2.2	1.1-102	Lab Test Data Report
EP.58	The value of the version field of the SignedData content type shall be v3.	FIPS 201-1, Section 4.2.2	1.1-102	Lab Test Data Report
EP.59	The digestAlgorithms field of the SignedData content type shall be in accordance with Table 3-3 of SP 800-78-1.	FIPS 201-1, Section 4.2.2	1.1-102	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	1.1-102	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	1.1-102	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	1.1-102	Lab Test Data Report
EP.63	The crls field from the SignedData content type shall be omitted.	FIPS 201-1, Section 4.2.2	1.1-102	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	1.1-102	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	1.1-102	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	5.1-13	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	1.1-102	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 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	1.1-102	Lab Test Data Report
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	5.1-13	Lab Test Data Report
EP.70	The SignedData content type shall include the digital signature.	FIPS 201-1, Section 4.2.2	1.1-102	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	1.1-102	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	5.1-13	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	1.1-143	Lab Test Data Report
EP.74	The digital signature is implemented as a SignedData Type.	FIPS 201-1, Section 4.4.2	1.1-141	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	1.1-141	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	1.1-141	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	1.1-141	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	1.1-141	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	1.1-141	Lab Test Data Report
EP.80	The crls field from the SignedData content type shall be omitted.	FIPS 201-1, Section 4.4.2	1.1-141	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	1.1-141	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	1.1-141	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	5.1-13	Lab Test Data Report
EP.84	The signedAttrs of the SignerInfo shall include the MessageDigest (OID = 1.2.840.113549.1.9.4) attribute containing the hash of the concatenated CBEFF_HEADER and the STD_BIOMETRIC_RECORD.	FIPS 201-1, Section 4.4.2	1.1-141	Lab Test Data 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	1.1-141	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	FIPS 201-1, Section 4.4.2	1.1-141	Lab Test Data Report

	card.			
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	5.1-13	Lab Test Data Report
EP.88	The SignedData content type shall include the digital signature.	FIPS 201-1, Section 4.4.2	1.1-141	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	1.1-141	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 the object, in accordance with Table 3-3 of SP 800-78-1.	SP 800-78-1, Section 3.2.1	5.1-13	Lab Test Data Report
EP.91	The CBEFF_SIGNATURE_BLOCK shall be encoded as a Cryptographic Message Syntax external digital signature as defined in RFC 3852. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2	1.1-143	Lab Test Data Report
EP.92	The digital signature is implemented as a SignedData Type. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2	1.1-141	Lab Test Data Report
EP.93	The value of the version field of the SignedData content type shall be v3. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2	1.1-141	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. *(This requirement will be evaluated only if*	SP 800-78-1, Section 3.2.1	5.1-13	Lab Test Data Report

	the facial image is populated in the card provided to the Lab)			
EP.95	The eContentType of the encapContentInfo shall be id-PIV-biometricObject (OID = 2.16.840.1.101.3.6.2). *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2	1.1-141	Lab Test Data Report
EP.96	The encapContentInfo of the SignedData content type shall omit the eContent field. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2	1.1-141	Lab Test Data Report
EP.97	If the signature on the facial image biometric was generated with a different key as the signature on the CHUID, the certificates field shall include only a single certificate in the SignerInfo field which can be used to verify the signature; else the certificates field shall be omitted. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2	1.1-141	Lab Test Data Report
EP.98	The crls field from the SignedData content type shall be omitted. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2	1.1-141	Lab Test Data Report
EP.99	The signerInfos in the SignedData content type shall contain only a single SignerInfo type. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2	1.1-141	Lab Test Data Report
EP.100	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*	FIPS 201-1, Section 4.4.2	1.1-141	Lab Test Data Report

	the facial image is populated in the card provided to the Lab)			
EP.101	The SignerInfo type shall specify a digestAlgorithm in accordance with Table 3-3 of SP 800-78-1. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-78-1, Section 3.2.1	5.1-13	Lab Test Data Report
EP.102	The signedAttrs of the SignerInfo shall include the MessageDigest (OID = 1.2.840.113549.1.9.4) attribute containing the hash of the concatenated CBEFF_HEADER and the STD_BIOMETRIC_RECORD. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2	1.1-141	Lab Test Data Report
EP.103	The signedAttrs of the SignerInfo shall include the pivSigner-DN (OID = 2.16.840.1.101.3.6.5) attribute containing the subject name that appears in the X.509 certificate for the entity that signed the biometric data. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2	1.1-141	Lab Test Data Report
EP.104	The signedAttrs of the SignerInfo shall include the pivFASC-N (OID = 2.16.840.1.101.3.6.6) attribute containing the FASC-N of the PIV card. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2	1.1-141	Lab Test Data Report
EP.105	The signatureAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-4 of SP 800-78-1 and based on the signature generation date of the object, in accordance with Table 3-3 of SP 800-78-1. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-78-1, Section 3.2.1	5.1-13	Lab Test Data Report

EP.106	The SignedData content type shall include the digital signature. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	FIPS 201-1, Section 4.4.2	1.1-141	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). *(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	1.1-141	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. *(This requirement will be evaluated only if the facial image is populated in the card provided to the Lab)*	SP 800-78-1, Section 3.2.1	5.1-13	Lab Test Data Report
EP.109	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.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	1.1-141	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	1.1-141	Lab Test Data Report
EP.113	The digestAlgorithms field of the SignedData content type shall be in accordance with Table 3-7 of SP 800-78-1.	SP 800-78-1, Section 3.2.3	5.1-23	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	1.1-141	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, Section 1.8.5	4.1-10	Lab Test Data Report
EP.117	The digestAlgorithm field specified in the SignerInfo field is in accordance with Table 3-7 of SP 800-78-1.	SP 800-78-1, Section 3.2.3	5.1-23	Lab Test Data Report
EP.118	The signatureAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-4 of SP 800-78-1 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	5.1-13	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, Section 1.8.5	4.1-9	Lab Test Data Report
EP.121	The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78-1 and based on the certificate expiration date in accordance with Table 3-3 of SP 800-78-1. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.2.1		Lab Test Data Report
EP.122	If Rivest Shamir & Adleman (RSA) with Probabilistic Signature Scheme (PSS) padding is used, the parameters field of the AlgorithmIdentifier type shall assert Secure Hash Algorithm (SHA) 256 (OID =	X.509 Certificate and CRL Profile for the Common Policy,	N/A	Lab Test Data Report

	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)*	February 6, 2006, Worksheet 9		
EP.123	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78-1. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.2.2	N/A	Lab Test Data Report
EP.124	If the public key algorithm is Elliptic Curve, then the EcpkParameters field uses either the namedCurve field populated with the appropriate OID from Table 3-6 of SP 800-78-1 or the implicitlyCA choice. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.2.2	N/A	Lab Test Data Report
EP.125	The keyUsage extension shall assert only the digitalSignature bit. No other bits shall be asserted. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9	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). *(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	N/A	Lab Test Data Report
EP.127	The authorityInfoAccess field shall	X.509	N/A	Lab Test Data

	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)*	Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9		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). *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	FIPS 201-1, Section 4.3		Lab Test Data Report
EP.129	The piv-interim extension (OID = 2.16.840.1.101.3.6.9.1) shall be present and contain an interim_indicator field which is populated with a Boolean value. This extension is not critical. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9	N/A	Lab Test Data Report
EP.130	The size of the public key for PIV authentication shall be determined by the expiration of the certificate in accordance with Table 3-1 of SP 800-78-1. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.1	5.1-4	Lab Test Data Report
EP.131	The public key present in the PIV authentication certificate correspond to the PIV authentication private key. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	FIPS 201-1, Section 4.3	1.1-105	Lab Test Data Report
EP.132	The FASC-N in the subjectAltName field in the PIV authentication certificate is the same as the FASC-N	Derived	N/A	Lab Test Data Report

	present in the CHUID. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*			
EP.133	The expiration of the PIV authentication certificate is not beyond the expiration of the CHUID. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	FIPS 201-1, Section 4.3		Lab Test Data Report
EP.134	If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537. *(This requirement will be evaluated only if the PIV authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.1	5.1-11	Lab Test Data Report
EP.135	The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78-1 and based on the certificate issue date in accordance with Table 3-3 of SP 800-78-1. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.1	N/A	Lab Test Data Report
EP.136	If RSA with PSS padding is used, the parameters field of the AlgorithmIdentifier type shall assert SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For the other RSA algorithms, the parameters field is populated with NULL. For ECDSA, the parameters field is absent. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	N/A	Lab Test Data Report
EP.137	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78-1. *(This requirement will be evaluated only if the digital signature certificate is issued by*	SP 800-78-1, Section 3.2.2	N/A	Lab Test Data Report

	an authorized Certification Authority)			
EP.138	If the public key algorithm is Elliptic Curve, then the EcpkParameters field uses either the namedCurve field populated with the appropriate OID from Table 3-6 of SP 800-78-1 or the implicitlyCA choice. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.2.2 X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	N/A	Lab Test Data Report
EP.139	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	N/A	Lab Test Data Report
EP.140	The size of the public key for digital signature shall be determined by the expiration of the certificate in accordance with Table 3-1 of SP 800-78-1. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.1	5.1-4	Lab Test Data Report
EP.141	The public key present in the digital signature certificate corresponds to the digital signature private key. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	FIPS 201-1, Section 4.3	N/A	Lab Test Data Report
EP.142	The expiration of the digital signature certificate is not beyond the expiration of the CHUID. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.1	N/A	Lab Test Data Report
EP.143	If the public key algorithm is RSA, the exponent shall be greater than or	SP 800-78-1,	5.1-11	Lab Test Data

	equal to 65,537. *(This requirement will be evaluated only if the digital signature certificate is issued by an authorized Certification Authority)*	Section 3.1		Report
EP.144	The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78-1 and based on the certificate issue date, in accordance with Table 3-3 of SP 800-78-1. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.2.1	N/A	Lab Test Data Report
EP.145	If RSA with PSS padding is used, the parameters field of the AlgorithmIdentifier type shall assert SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For the other RSA algorithms, the parameters field is populated with NULL. For ECDSA, the parameters field is absent. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	N/A	Lab Test Data Report
EP.146	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78-1. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.2.2	N/A	Lab Test Data Report
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 800-78-1 or the implicitlyCA choice. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.2.2	N/A	Lab Test Data Report
EP.148	If the public key algorithm is RSA, then the keyUsage extension shall	X.509 Certificate	N/A	Lab Test Data Report

	only assert the keyEncipherment bit. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5		
EP.149	If the public key algorithm is Elliptic Curve, then the keyUsage extension shall only assert the keyAgreement bit. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	N/A	Lab Test Data Report
EP.150	The size of the public key for key management shall be determined by the expiration of the certificate in accordance with Table 3-1 of SP 800-78-1. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.1	N/A	Lab Test Data Report
EP.151	The public key present in the key management certificate corresponds to the key management private key. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	FIPS 201-1, Section 4.3	N/A	Lab Test Data Report
EP.152	If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537. *(This requirement will be evaluated only if the key management certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.1	N/A	Lab Test Data Report
EP.153	The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78-1 and based on the certificate issue date in accordance with Table 3-3 of SP 800-78-1. *(This requirement will be evaluated only if*	SP 800-78-1, Section 3.2.1	N/A	Lab Test Data Report

	the card authentication certificate is issued by an authorized Certification Authority)			
EP.154	If RSA with PSS padding is used, the parameters field of the AlgorithmIdentifier type shall assert SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For the other RSA algorithms, the parameters field is populated with NULL. For ECDSA, the parameters field is absent. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	N/A	Lab Test Data Report
EP.155	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78-1. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	SP 800-76-1, Section 3.2.2	N/A	Lab Test Data Report
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 800-78-1 or the implicitlyCA choice *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority).*	SP 800-78-1, Section 3.2.2 X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	N/A	Lab Test Data Report
EP.157	The keyUsage extension shall assert only the digitalSignature bit. No other bits shall be asserted. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	N/A	Lab Test Data Report
EP.158	The policyIdentifier field in the certificatePolicies must assert id-fpki-common-cardAuth (OID =	X.509 Certificate and CRL	N/A	Lab Test Data Report

	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)*	Profile for the Common Policy, February 6, 2006, Worksheet 6		
EP.159	The extKeyUsage extension shall assert id-PIV-cardAuth (OID = 2.16.840.1.101.3.6.8). This extension is critical. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	N/A	Lab Test Data Report
EP.160	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	N/A	Lab Test Data Report
EP.161	The FASC-N shall be populated in the subjectAltName extension using the pivFASC-N attribute OID = 2.16.840.1.101.3.6.6). *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	N/A	Lab Test Data Report
EP.162	The piv-interim extension (OID = 2.16.840.1.101.3.6.9.1) shall be present contain an interim_indicator field which is populated with a Boolean value. This extension is not critical. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	N/A	Lab Test Data Report
EP.163	The size of the public key for card	SP 800-76-1,	N/A	Lab Test Data

	authentication shall be determined by the expiration of the certificate in accordance with Table 3-1 of SP 800-78-1. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	Section 3.1		Report
EP.164	The public key present in the card authentication certificate correspond to the card authentication private key. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	FIPS 201-1, Section 4.3	N/A	Lab Test Data Report
EP.165	The FASC-N in the subjectAltName field in the card authentication certificate is the same as the FASC-N present in the CHUID. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	Derived	N/A	Lab Test Data Report
EP.166	If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537. *(This requirement will be evaluated only if the card authentication certificate is issued by an authorized Certification Authority)*	SP 800-78-1, Section 3.1	N/A	Lab Test Data Report
EP.167	If present, the card management key shall be imported onto the card by the issuer.	FIPS 201-1, Section 4.3	2-84	Vendor Documentation Review
EP.168	If the public key size of the certificate that signs the CHUID, Biometrics and Security Object is 2048 bits or greater, then the hash 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]).	Derived	N/A	Vendor Test Data Report Lab Test Data Report
EP.169	If the public key size of the PIV Authentication, Digital Signature, Key Management or Card Management certificate is 2048 bits or greater, then the hash algorithm	Derived	N/A	Vendor Test Data Report Lab Test Data Report

	asserted in the AlgorithmIdentifier of the signature shall be SHA256 (1.2.840.113549.1.1.11 [PKCS v1.5 padding scheme] or 1.2.840.113549.1.1.10. [PSS padding scheme]). *(This requirement will be evaluated only if the above listed certificates are issued by an authorized Certification Authority)*			
EP.170	Personalization facilities shall use a common set of standard operating procedures for production of PIV Cards.	Derived Test Requirement	N/A	Vendor Documentation Review
EP.171	Delivery facilities shall employ personnel who are knowledgeable of the organization's operating procedures.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
EP.172	Delivery facilities shall employ personnel who are not on the list of known terrorists.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
EP.173	Delivery facilities shall perform background checks on personnel handling PIV Cards. Background checks must reflect Federal, State and Local databases to ensure felonies have not been committed by PIV Card handlers.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
EP.174	Delivery facilities shall maintain adequate security on the premise of the building.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
EP.175	Delivery facilities shall utilize a PIV Card storage container which contains a multi-factor form of authentication to access the contents of the container.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
EP.176	Delivery facilities shall maintain a log of visitors who enter the area which has been designated to personalize PIV Cards.	Derived Test Requirement	N/A	Site Visit
EP.177	Delivery facilities shall utilize	Derived Test	N/A	Vendor

	automated card inventory control, which utilizes the either the Agency Serial Number (printed on the back of the card) or CHUID to track and manage the following transactions: a) Inventory to be delivered from the personalization facility (if applicable) b) Inventory of provisioned PIV Cards on hand c) Inventory which has been delivered.	Requirement		Documentation Review Site Visit
EP.178	Delivery facilities shall utilize a mechanism to notify Agencies, on a regular basis, which personalized cards have been received (if applicable) and delivered.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
EP.179	Delivery facilities shall utilize only FIPS 201 approved equipment according to the GSA FIPS 201 Approved Product List.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
EP.180	Delivery facilities must send personalized cards to their respective locations using a secure and reliable courier which provides delivery tracking and notification.	Derived Test Requirement	N/A	Vendor Documentation Review
EP.181	Facility personnel shall encode a card which is conformant to the requirements of Electronic Personalization Approval Procedure	Derived Test Requirement	N/A	Site Visit Lab Test Data Report
EP.182	Information Technology systems used to store personally identifiable system shall have a Privacy Impact Assessment conducted.	Derived		Vendor Documentation Review Site Visit
EP.183	The Supplier shall utilize a secure mechanism to transfer data related to the card printing request.	Derived		Vendor Documentation Review Site Visit
EP.184	Electronic Personalization Facilities shall be reviewed every two (2) years, from the date of GSA approval, to	Derived Test Requirement	N/A	Vendor Documentation Review

	ensure Standard Operating Procedures are followed by Electronic Personalization Personnel.			Site Visit

Table 1 - Applicable Requirements

3.2 Approval Mechanism Matrix

The table below provides an indication of the total number of requirements applicable for the Service 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
184	13	6	157	22	2	1
Legend: 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 Service against the requirements enumerated above.

1.1.1 Vendor Documentation Review

Reference(s):	EP.1 to EP.4, EP.6, EP.7, EP.9, EP.54, EP.167, EP.170 to EP.175, EP.177 to EP.180, EP.182 to EP.184
Evaluation Procedure:	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. 2. The Lab will review the Product's documentation to determine the following. At a minimum the documents submitted by the Supplier must include: ▪ *Data Loading (EP.1, EP.167)* • 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. • A procedure which documents the exact steps, including APDUs, to update a produced card using the Card Management Key or similar cryptographic mechanism. • A statement which discusses how the card management key is loaded by the Service provider. ▪ *Cryptographic Keys (EP.2)* • A statement indicating that unique card management keys are issued to each PIV Card personalized. • A procedure which details how the uniqueness of card management keys are ensured by the product. ▪ *Population of Data Objects (EP.3, EP.4)* • A statement indicating which of the following data objects are loaded

	onto personalized PIV Cards, as defined in FIPS 201 and SP 800-73-1: o Card Capabilities Container o CHUID o PIV Authentication Key Pair o Biometric Fingerprints o Security Object o Biometric Facial Image o Printed Information o Digital Signature Key Pair o Key Management Key Pair o Card Management Key o Card Authentication Key Pair ▪ *Biometric Data Conformance (EP.6, EP.7)* • A statement indicating that the primary and secondary biometric fingerprint templates are stored in one minutiae template on the PIV Card. • A statement indicating that, when used, only one facial image is stored on the PIV Card. ▪ *Data Object Tags (EP.9)* • Data objects populated in containers shall contain all appropriate tags and lengths for each element in the object. ▪ *Encoding and Compression Format of Facial Images (EP.54)* • Indication of the encoding format used by the Product *a.* JPEG *b.* JPEG-2000 • Indication the compression format is utilized by the Product. *a.* whole-image *b.* single-region-of-interest (ROI) ▪ *Card Management Key Importation (EP.167)* • A statement indicating that the Service Provider imports the card management key onto the PIV Card. • The technical process (diagrams and/or APDUs) for importing the Card Management Key to the PIV Card. ▪ *Standard Operating Procedures (EP.170)* • The Supplier has submitted detailed documentation for the complete process of printing PIV Cards at the Facility. The SOP should include, at a minimum, the hours of operation for the Facility as well as the PIV Card personalization area, procedures for handling blank cardstock and/or printed cardstock, partitioning cardstock quantities for customers, handling procedures, a list of authorized PIV Card handlers and their supervisors, contact information for local law enforcement, storage procedures for printed PIV Cards, procedures for running batch orders, and methods for cryptographically locking

	personalized cardstock. ▪ *Personnel Training & Knowledge (EP.171)* • Training materials of the Facility's Operating Procedures have been developed for each role in the printing facility. • A list of trusted roles in the Facility system has been defined as part of the Standard Operating Procedures. • A list of authorized personnel is maintained by the Facility and is referenced by the Standard Operating Procedures. The list of authorized has been furnished to the Lab for review. • A statement by the Service Provider that when the list of authorized personnel changes for any reason, the Lab who has performed the original evaluation will be provided with an updated list. • The Facility Standard Operating Procedures states that training occurs on at least an annual basis for all personnel serving a role within the Facility. • The Facility Standard Operating Procedures state that employees are retrained within one week of a procedure-based changed to the SOP. ▪ *Personnel History Checks (EP.172, EP.173)* • A statement from the background investigation service provider has been submitted which states the source of the Federal agency responsible for maintaining the list(s) of known terrorists for which Facility personnel are checked against. Examples of Agencies maintaining lists of known terrorists include the Department of Homeland Security, the Federal Bureau of Investigations, and INTERPOL. Human Resources personnel records should indicate that this check has been performed on all personnel of the PIV Card Facility. • The contract with the service provider for Federal, State, and Local criminal history has been provided and personnel records indicate that this check has been performed on all PIV Card handlers. • Human Resources Standard Operating Procedures indicate that employees whose job function is to handle PIV Cards (trusted roles), are to undergo a background check before performing functions a particular role in the Electronic Personalization Facility. ▪ *Premise Security (EP.174)* • The security plan for the premise has been provided and all security protections on the building are documented, and listed within the security inventory list. ▪ *PIV Card Storage Container (EP.175)* • The security equipment inventory list includes the make and model of the container used to store PIV Cards. • The Electronic Personalization Facility Standard Operating Procedures describes the type of factors for authentication to the container.

- *Visitor Logging (EP.176)*
  - A template for the visitors log has been provided which matches the actual visitors log used at the Facility on a day-to-day basis.
- *Card Inventory Control (EP.177)*
  - An automated inventory control system has been developed to log all outgoing and the number of on-hand PIV Cards which utilizes, at a minimum, the Agency Serial number, which is printed on the back of the card, or other uniquely identifying number.
  - The automated inventory control system should provide both a count and itemization of every card printed for each contracting Agency. For cards that have been shipped from the facility, a list of each card must be maintained for a period of three (3) years for auditing purposes.
  - The Facility Standard Operating Procedures assigns duties to a particular role for auditing the number of cards stored at the Facility on a bi-weekly basis, using the automated inventory control system.
  - An automated inventory control system has been developed to track incoming, outgoing, and the number of on-hand PIV Cards which utilizes, at a minimum, the FASC-N value in the CHUID or the entire agency serial number, which is printed on the back of the card. If the FASC-N is used, the following values will be extracted from the data object to identify cards:
    a. Credential Number – The CN shall be used as the primary key to identify a cardholder.
    b. Agency Code – The AC shall be used as the secondary key, in the event that multiple CNs exist in the inventory control system.
    c. The facility may optionally choose to populate records using the card holder name which is printed on the front of the card; however, the PIN value of the card is never to be used to access privileged data objects (e.g. Printed Information Buffer) on the card for the purposes of card inventory.
- *Agency Notification (EP.178)*
  - The Facility Standard Operating Procedures describe the processes in place to notify an Agency that a card or batch of cards have been received and delivered to either the contracting Agency or another service provider.
- *GSA Approved Equipment (EP.179)*
  - The security equipment inventory list states the equipment make and model number of each Product used by the facility to ensure use of FIPS 201 approved products by GSA. The Approved Products List reference number must be provided to the Lab as well.
- *Card Transporting (EP.180)*
  - A contract with the secure and reliable courier (e.g. Brinks, Dunbar,

	UPS, FedEx) for transportation of personalized PIV Cards has been provided. • The Facility Standard Operating Procedures state how the delivery confirmation is to be checked after cards have been sent from the Facility to their respective locations. • The Facility Standard Operating Procedures states the steps that occur if and when a delivery has not been made by the courier. ▪ *Facility Review (EP.182)* • The Facility maintains a written record of the 2 year reevaluation of the Facility. • The Electronic Personalization Standard Operating Procedures state that the Facility is prepared for the Lab to visit every 2 years to ensure that the Facility is operating as per the Standard Operating Procedures. 3. The Lab will update the status to "VDR Complete" as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Result:	a. 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. b. Unique Card Management Keys are loaded onto the card by the issuer of the personalized PIV Card. c. Electronically Personalized PIV Cards contain, at a minimum, the mandatory data objects as defined SP 800-73-1. d. Primary and secondary biometrics are stored on the card and when facial imagery is used, only one image is stored on the card. e. The appropriate encoding/compression formats have been used for facial images. f. All documentation such as Standard Operating Procedures and contracts have been provided to the Lab for review.

1.1.2 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.

1.1.2.1 **EP.8**

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • *Data Model Conformance*: The Product is capable of being electronically personalized to meet the requirements of FIPS 201 and supporting documentation. At a minimum, the following test scenario must be performed to confirm compliance:

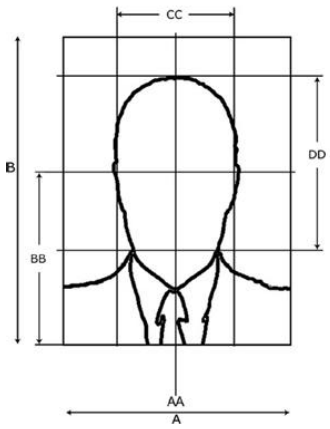
	a. A report generated as a result of running the NIST SP 800-85B test tool by the Supplier against a PIV Card personalized by the Product. * Note: The SP 800-85B test tool can be found at the following location: http://fips201ep.cio.gov/tools.php
Expected Result:	The PIV Card tested has successfully completed the NIST SP 800-85B validation for PIV data conformance by the Supplier.

1.1.2.2 **EP.51**

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • *INCITS 385 Profile Conformance*: 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. At a minimum, the following test scenario must be performed to confirm compliance: a. Convert the binary representation of the INCITS 385 to textual form. *b.* In the textual form, ensure that the fields that are 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.
Expected Result:	The submitted INCITS 385 profile is conformant to SP 800-76-1, Table 6.

1.1.2.3 **EP.53**

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • *Full Frontal Image Type:* The electronic image submitted conforms to the diagram listed below.

	 At a minimum, the following test scenario must be performed to confirm compliance: *a.* 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.
Expected Result:	The full frontal image type meets the minimum spatial resolution and specified ratio of image width to head width of 7:4.

1.1.2.4 **EP.55**

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • *Image Compression*: Facial images are compressed no more 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. At a minimum, the following test scenario must be performed to confirm compliance: <u>For regular compression</u> a. Note down the size of the raw image obtained. b. Compress the image using appropriate compression format and encoding c. Note down the size of the compressed image. <u>For ROI compression</u> a. Using the raw image, extract the ROI. b. Note down the size of the ROI to be compressed c. Compress the image using appropriate compression format and encoding

	d. Note down the size of the final ROI
Expected Result:	The test report indicates that an appropriate level of compression has been applied to the image for regular or ROI compression.

1.1.2.5 **EP.168, EP.169**

Evaluation Procedure:	The Lab will review the documentation submitted by the Supplier to ascertain the following: • *Signature Generation*: 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. At a minimum, the following test scenario must be performed to confirm compliance: a. Generate the data that is to be loaded on the card (Certificate, CHUID, etc) b. Using an ASN.1 utility, perform a dump of the data object such that it retains the ASN.1 syntax formatting *c.* Explicitly state which object the ASN.1 dump represents
Expected Result:	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.

1.1.3 Site Visit

A Lab Technician will perform a site visit[2] at the Facility to determine whether the documented procedures and other necessary requirements are adhered to and followed by the Service Provider.

Reference(s):	EP.171 to EP.179, EP.181 to EP.184
Evaluation Procedure:	1. The Lab will update the status in the Web-Enabled Tool to "SV Begun" as instructed in the Web-enabled Tool Laboratory User Guide. 2. The Lab will conduct an on site review of the Facility to determine the following. In this respect the Lab Technician shall review processes employed at the facility: ▪ *Knowledge of Personnel (EP.170)* • Testing knowledge of PIV Card handlers. This will be conducted by interviewing a sample of key personnel to determine whether they are knowledgeable of the facility's standard operating procedures. ▪ *Personnel Background Checks (EP.171, EP.172)*

[2] Site visits not only include documentation review but may also include observing the actual process being carried out. Service Providers need to have equipment and processes in place for identity authentication and verification to demonstrate execution of the Electronic Personalization Service.

	• Reviewing records of the hiring process employed by the Facility to determine whether the potential employee is on a list of known terrorists, prior to hiring. • Reviewing records of the hiring process employed by the Facility to determine whether the potential employee has had a background check completed, prior to hiring. ▪ *Security Provisions (EP.173, EP.174, EP.175)* • Demonstration of security mechanisms that are in place on the premise of the facility. • Demonstration of the logging procedures for visitors who enter the designated PIV Card printing area. • Demonstration the security mechanisms that are in place on the storage container of PIV Cards waiting to be delivered. Mechanisms must employ a multi-factor form of authentication to gain access to the container. ▪ *Inventory Control (EP.176, EP.177)* • Demonstration of the procedures in place to log outgoing (delivered) PIV Cards. • Demonstration of the facility's ability to communicate the logs with the contracting Agency. ▪ *GSA Approved Equipment (EP.178)* • Review of GSA approved equipment that is listed in the Standard Operating Procedures, to ensure that the facility is using only approved products for card personalization. ▪ *Encoded Card (EP.181)* • Observation of the card being encoded at the time of site visit from blank cardstock. Lab Engineer will take possession of the card for evaluation at the Laboratory. ▪ *Facility Review (EP.182)* • The Facility maintains a written record of the 2 year reevaluation of the Facility. • The Facility is prepared for the Lab to visit every 2 years to ensure that the Facility is operating as per the Standard Operating Procedures. 3. The Lab will update the status to “SV Complete” as instructed in the Web-enabled Tool Laboratory User Guide.

1.1.4 Lab Test Data Report

Reference(s):	EP.1, EP.8 to EP.48, EP.50, EP.52, EP.56 to EP.169, EP.181
Test Procedure:	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. 2. The Lab will execute test procedures for this category in accordance with

	the "*Electronic Personalization Test Procedure*." 3. The Lab will update the status to "LTDR Complete" as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Result:	1. The Product successfully passes all the test cases documented within the test procedure.

1.1.5 Certification

Reference(s):	EP.5, EP.49
Evaluation Procedure:	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. 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: ▪ Examine the certification statement to see if it is provided by NIST/CSE and that it is still current i.e. valid; ▪ Verify the authenticity of this certification provided by NIST/CSE; and ▪ 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: http://csrc.nist.gov/cryptval/140-1/1401val.htm. 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: ▪ Examine the certification statement to see if it provided by NIST and that it is still current i.e. valid; ▪ Verify the authenticity of this NIST certification as compliant to FIPS 201 and supporting documentation; and ▪ Review the list of Template Generators to determine inclusion of the Product. The list is available on the website located at: http://fingerprint.nist.gov/MINEX/QPL.html. 4. The Lab will update the status to "C Complete" as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Result:	1. The Cryptographic Module has been found to be certified by NIST/CSE at FIPS 140-2 Level 2. 2. Template Generator used within the Product are approved under the NIST Template Generator certification process.

1.1.6 Attestation

Reference(s):	N/A
Evaluation Procedure:	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. 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]). 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.
Expected Results:	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 loaded onto the PIV Card by an Electronic Personalization Service. Please inform the Lab which containers that the Service is capable of generating and populating by filling out the table below.

If the Service has the capability of generating certain data containers (e.g. fingerprint templates) before populating the PIV Card, fill in the "`Vendor`", "`Product`" and "`S/W Version`" columns below for the Product that is used to populate that data container.

If the Service does not have the capability of generating data containers, but is able to populate the container, and relies on input data from the Agency mark the "`Agency submitted`" column with "`Yes`" and leave the remaining columns blank.

If the service does not have the capability of populating any data containers, mark "`No`" in all fields for that container

Rows which do not contain any information will be assumed to be not able to be populated or generated by the Service provider for that data container.

Object	Agency submitted	Vendor	Product	S/W Version
Mandatory Objects				
Card Capabilities Container				
CHUID				
PIV Authentication Certificate				
Biometric Fingerprint				
Security Object				
Optional Objects				
Printed Information				
Biometric Facial Image				
Digital Signature Certificate				
Key Management Certificate				
Card Authentication Certificate				