FIPS 201 Evaluation Program
Attestation Form for PIV Card

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

Applicant Information

Company Name	

Product/Service Information

Name	
Part Number	
Hardware Version	
Software Version	
Firmware Version	

Lab Specific Information

Approval Procedure Version	9.0.0

Requirements being attested to:

Identifier #	Requirement Description	Source
PIV-C.1	The PIV Card shall comply with characteristics as described in ISO/IEC 7810.	FIPS 201-1, Section 4.1
PIV-C.2	The PIV Card shall comply with characteristics as described in ISO/IEC 10373.	FIPS 201-1, Section 4.1
PIV-C.3	The PIV Card shall comply with characteristics as described in ISO/IEC 7816 for contact cards.	FIPS 201-1, Section 4.1
PIV-C.4	The PIV Card shall comply with characteristics as described in ISO/IEC 14443 for contactless cards.	FIPS 201-1, Section 4.1
PIV-C.5	The PIV Card shall contain a contact and a contactless ICC interface.	FIPS 201-1, Section 4.1.3
PIV-C.6	The card body structure shall consist of card material(s) that satisfy the card characteristics in ISO 7810.	FIPS 201-1, Section 4.1.3
PIV-C.7	The card body structure shall consist of card material(s) that satisfy the test methods in American National Standards Institute (ANSI) 322.	FIPS 201-1, Section 4.1.3
PIV-C.8	The ANSI 322 test methods tests shall be used to evaluate card material durability and performance.	FIPS 201-1, Section 4.1.3
PIV-C.9	The ANSI 322 tests shall include card flexure.	FIPS 201-1, Section 4.1.3
PIV-C.10	The ANSI 322 tests shall include card static stress.	FIPS 201-1, Section 4.1.3
PIV-C.11	The ANSI322 tests shall include plasticizer exposure.	FIPS 201-1, Section 4.1.3
PIV-C.12	The ANSI 322 tests shall include impact resistance.	FIPS 201-1, Section 4.1.3
PIV-C.13	The ANSI 322 tests shall include card structural integrity.	FIPS 201-1, Section 4.1.3
PIV-C.14	The ANSI 322 tests shall include Delamination – 90°.	Derived
PIV-C.15	If the PIV Card contains a magnetic stripe, the ANSI 322 tests shall include Magnetic Stripe Abrasion.	Derived

PIV-C.16	Cards shall not malfunction after hand cleaning with a mild soap and water mixture.	FIPS 201-1, Section 4.1.3
PIV-C.17	The reagents called out in Section 5.4.1.1 of ISO 10373 shall be modified to include a two percent soap solution.	FIPS 201-1, Section 4.1.3
PIV-C.18	The card shall be subjected to actual, concentrated, or artificial sunlight to appropriately reflect 2000 hours of southwestern United States' sunlight exposure. The tests shall be in accordance with ANSI 322, Section 5.15.	FIPS 201-1, Section 4.1.3
PIV-C.19	The card shall be subjected to the ISO 10373 dynamic bending test and shall have no visible cracks or failures.	FIPS 201-1, Section 4.1.3
PIV-C.20	The card shall be 27- to 33-mil thick (before lamination) in accordance with ISO 7810.	FIPS 201-1, Section 4.1.3
PIV-C.21	The card material shall allow production of a flat card in accordance with ISO 7810 after lamination of one or both sides of the card.	FIPS 201-1, Section 4.1.3
PIV-C.22	The PIV Card must be activated to perform privileged operations such as reading biometric information and using asymmetric keys.	FIPS 201-1, Section 4.1.6
PIV-C.23	The PIV Card shall be activated for privileged operations only after authenticating the cardholder or the appropriate card management system.	FIPS 201-1, Section 4.1.6
PIV-C.24	PIV Cards shall implement PIN-based cardholder activation to allow privileged operations using PIV credentials held by the card.	FIPS 201-1, Section 4.1.6.1
PIV-C.25	For PIN-based cardholder activation, the cardholder shall supply a numeric PIN.	FIPS 201-1, Section 4.1.6.1
PIV-C.26	The PIN shall be transmitted to the PIV Card and checked by the card. If the presented PIN is correct, the PIV Card is activated.	FIPS 201-1, Section 4.1.6.1
PIV-C.27	The PIV Card shall include mechanisms to limit the number of guesses an adversary can attempt if a card is lost or stolen.	FIPS 201-1, Section 4.1.6.1
PIV-C.28	The PIN authentication mechanism shall meet the identity-based authentication requirements of FIPS PUB 140-2 Level 2. [FIPS140-2]	FIPS 201-1, Section 4.1.6.1
PIV-C.29	The PIV CHUID shall be accessible from the contact interface of the PIV Card without card activation.	FIPS 201-1, Section 4.2
PIV-C.30	The PIV CHUID shall be accessible from the contactless interface of the PIV Card without card activation.	FIPS 201-1, Section 4.2
PIV-C.31	Cryptographic operations with this key [PIV Authentication] are performed only through the contact interface.	FIPS 201-1, Section 4.3
PIV-C.32	The PIV Card shall implement RSA or elliptic curve key pair generation.	FIPS 201-1, Section 4.3
PIV-C.33	The PIV Card shall implement RSA or elliptic curve private key cryptographic operations.	FIPS 201-1, Section 4.3
PIV-C.34	The PIV Card shall implement importation and storage of X.509 certificates.	FIPS 201-1, Section 4.3
PIV-C.35	All cryptographic operations using the PIV keys shall be performed on-card.	FIPS 201-1, Section 4.3
PIV-C.36	All PIV cryptographic keys shall be generated within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above.	FIPS 201-1, Section 4.3
PIV-C.37	The PIV Card shall provide [FIPS 140-2] Level 3 physical security to protect the PIV private keys in storage.	FIPS 201-1, Section 4.3
PIV-C.38	The PIV Authentication Key shall be generated on the PIV Card.	FIPS 201-1, Section 4.3
PIV-C.39	The PIV Card shall not permit exportation of the PIV authentication key.	FIPS 201-1, Section 4.3
PIV-C.40	The PIV authentication key shall only be available through the contact interface of the PIV Card.	FIPS 201-1, Section 4.3
PIV-C.41	The PIV Card shall not permit exportation of the card authentication	FIPS 201-1,

	key, if present.	Section 4.3
PIV-C.42	The PIV digital signature key, if present, shall be generated on the PIV Card.	FIPS 201-1, Section 4.3
PIV-C.43	The PIV Card shall not permit exportation of the digital signature key.	FIPS 201-1, Section 4.3
PIV-C.44	Cryptographic operations using the digital signature key, if present, shall only be performed using the contact interface of the PIV Card.	FIPS 201-1, Section 4.3
PIV-C.45	Private key operations using the digital signature key shall only be performed after explicit user action.	FIPS 201-1, Section 4.3
PIV-C.46	The Key Management Key shall be either generated on the PIV Card or imported to the card.	FIPS 201-1, Section 4.3
PIV-C.47	If present, the key management key must only be accessible using the contact interface of the PIV Card.	FIPS 201-1, Section 4.3
PIV-C.48	If the key management key is present, the PIV Card shall import and store a corresponding X.509 certificate to support validation of the key.	FIPS 201-1, Section 4.3
PIV-C.49	If present, the card management key shall be imported onto the card by the issuer.	FIPS 201-1, Section 4.3
PIV-C.50	If present, the card management key shall only be accessible using the contact interface of the PIV Card.	FIPS 201-1, Section 4.3
PIV-C.51	If supported, initialization and update of trust anchor certificates shall require explicit cardholder action, in addition to activation of the card.	FIPS 201-1, Section 4.3
PIV-C.52	Biometric data specified to be stored on the PIV Card under FIPS 201 shall NOT be accessed over the contactless interface.	FIPS 201-1, Section 4.4
PIV-C.53	PIV biometric data shall be protected through an authentication mechanism such as a PIN.	FIPS 201-1, Section 4.4.2
PIV-C.54	At a minimum, PIV Cards shall support either the T=0 or T=1 transmission protocol as defined in ISO/IEC 7816-3:1997. The card may support both protocols.	Card /Card Reader Interoperability Requirements Section 2.1.1.3
PIV-C.55	PIV Cards shall not require the use of any RFU bits in the Global or Specific Interface Bytes to operate correctly.	Card /Card Reader Interoperability Requirements Section 2.1.1.4
PIV-C.56	Retrieval time of CHUID components through the contactless interface of the card shall not exceed 1.0 seconds.	Derived
PIV-C.57	Retrieval time of the fingerprint biometrics through the contact interface of the card shall not exceed 1.0 seconds.	Derived
PIV-C.58	PIV Cards shall not require a Programming Voltage to operate correctly.	Card /Card Reader Interoperability Requirements Section 2.1.1.1
PIV-C.59	PIV cards shall support the Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.	Card /Card Reader Interoperability Requirements Section 2.1.1.2
PIV-C.60	PIV Cards submitted for testing shall have the biometric fingerprint buffer populated, which has been retrieved from the EP Website.	Derived
PIV-C.61	PIV Cards submitted for testing shall have the CHUID available, on	Derived

	the contactless ICC, which has been retrieved from the EP Website.	
PIV-C.62	Zone 3—Magnetic Stripe. If used, the magnetic stripe shall be high coercively.	FIPS 201-1, Section 4.1.4.4
PIV-C.63	Zone 3—Magnetic Stripe. If used, the magnetic stripe shall be placed in accordance with ISO-7811, as illustrated in Figure 4-7.	FIPS 201-1, Section 4.1.4.4
PIV-C.64	To activate the card for personalization or update, the card shall perform a challenge response with a card management system using cryptographic keys stored on the card in accordance with [SP800-73].	Derived
PIV-C.65	Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800-78-1, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78]	FIPS 201-1, Section 4.1.6.2
PIV-C.66	The PIV Card shall store a corresponding X.509 certificate to support validation of the PIV Authentication private key.	Derived
PIV-C.67	The PIV Card shall store a corresponding X.509 certificate to support validation of the Digital Signature private key.	Derived
PIV-C.68	The PIV Card shall store a corresponding X.509 certificate to support validation of the Key Management private key.	Derived
PIV-C.69	The PIV Card shall store a corresponding X.509 certificate to support validation of the Card Authentication private key, if applicable.	Derived

Signature

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

Signature		Date	
Name			
Title			