

# **FIPS 201 Evaluation Program**

## **Attestation Form for Biometric Authentication Reader**

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**

<b>Company Name</b>	
---------------------	--

### **Product/Service Information**

<b>Name</b>			
<b>Part Number</b>			
<b>Hardware Version</b>			
<b>Software Version</b>			
<b>Firmware Version</b>			

### **Lab Specific Information**

<b>Approval Procedure Version</b>	4.0.0
-----------------------------------	-------

### **Requirements being attested to:**

Identifier #	Requirement Description	Source
R-BIO-A.1	Contact card readers shall conform to the ISO 7816 standard for the card-to-reader interface.	FIPS 201-1, Section 4.5.1  Para 1 pg.37
R-BIO-A.2	{Logical contact card} readers shall conform to the Personal Computer/Smart Card (PC/SC) Specification for the reader-to-host system interface in general desktop computing environment.	FIPS 201-1, Section 4.5.1  Para 1 pg.37
R-BIO-A.3	PIV readers 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 2.2.2.1  Para 1 pg.3
R-BIO-A.4	The contact interface of the reader shall support both the T=0 and T=1 transmission protocols as defined in ISO/IEC 7816-3:1997.	Card /Card Reader Interoperability Requirements, Section 2.2.2.2  Para 1 pg.3
R-BIO-A.5	PIV readers shall support the Protocol and Parameters Selection (PPS) protocol as defined in ISO/IEC 7816-3:1997	Card /Card Reader Interoperability Requirements, Section 3.2.3.1

**FIPS 201 Evaluation Program**  
**Attestation Form for Biometric Authentication Reader**

Identifier #	Requirement Description	Source
		Para 1 pg.4
R-BIO-A.6	PIV Readers shall {not generate a Programming Voltage.}	Card /Card Reader Interoperability Requirements, Section 2.1.1.1
R-BIO-A.7	PIV Readers shall support implicit protocol and parameter selections as defined in ISO/IEC 7816-3:1997.	Card /Card Reader Interoperability Requirements, Section 2.2.2.3 Para 1 pg.1
R-BIO-A.8	The reader buffer size shall be no less than 256 bytes.	Card /Card Reader Interoperability Requirements, Section 3.2.1.1 Para 1 pg.4
R-BIO-A.9	{Fingerprint sensors used for PIV authentication shall conform to FBI specification ( <a href="#">FBI PIV Spec 071006</a> ).}	Derived
R-BIO-A.10	{Devices shall be capable of imaging an area of at least 12.8 millimeters horizontally x 16.5 millimeters vertically.} The native scanning resolution of the device shall be at least 197 pixels per centimeter (500 pixels per inch) {in each direction.}	SP 800-76-1, Section 3.3 Para 2 pg.5
R-BIO-A.11	{Devices shall contain embedded fingerprint template generators and matchers on the device that have been certified by NIST as conformant to FIPS 201 and related documents.}	Derived
R-BIO-A.12	{The reader shall be able to read data from the CHUID buffer on the PIV Card.}	FIPS 201-1, Section 6.2.2 Para 1 pg.48
R-BIO-A.13	{The reader shall be able to compare the CHUID expiration date to the current date and determine card expiry.}	FIPS 201-1, Section 6.2.2 Para 1 pg.48
R-BIO-A.14	{The reader shall be able to parse the FASC-N from the CHUID.}	FIPS 201-1, Section 6.2.3.1
R-BIO-A.15	{The reader shall be able to provide the personal identification number (PIN) to the card to access the biometric stored on the PIV Card.}	Derived
R-BIO-A.16	The digital signature on the biometric is checked {based on signature algorithms and key sizes specified in Table 3-3 of SP 800-78-2} to ensure the biometric was signed by a trusted source and is unaltered.	FIPS 201-1, Section 6.2.2 Para 1 pg.48

## **FIPS 201 Evaluation Program**

### **Attestation Form for Biometric Authentication Reader**

Identifier #	Requirement Description	Source
R-BIO-A.17	{If the Product interfaces with a Certificate Validator to perform certificate path discovery and validation, it uses a GSA FIPS 201 EP approved SCVP client.}	Derived
R-BIO-A.18	{If the intended purpose of the reader is for physical access,} then the reader shall contain an integrated PIN input device.	FIPS 201-1, Section 4.5.3 Para 1 pg.37
R-BIO-A.19	{The reader shall be able to extract the FASC-N in the Signed Attributes field of the biometric signature block and compare to the FASC-N found in the CHUID.}	FIPS 201-1, Section 6.2.3.1 Para 1 pg.48
R-BIO-A.20	One or more of the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) are used as input to the authorization check to determine whether the cardholder should be granted access.	FIPS 201-1, Section 6.2.3.1 Para 1 pg.48
R-BIO-A.21	{For externally-facing readers <sup>1</sup> , the reader's cryptographic module shall be FIPS 140-2 validated with an overall Security Level 2 (or higher). If not externally-facing, the reader's cryptographic module shall be FIPS 140-2 validated with an overall Security Level 1.}	Derived
R-BIO-A.22	The biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card (i.e. the reader performs a 1:1 biometric match).	FIPS 201-1, Section 6.2.3.1 Para 1 pg.48

#### **Signature**

I hereby claim that I am authorized to sign this form on behalf of the above specified company. By signing this form I acknowledge that,

- I 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.
- The organization will notify the GSA FIPS 201 EP of any manufacturing or product (form, fit or function) change that the product may undergo from the date it was placed on the Approved Products List until it is removed and placed on the Removed Products List.
- The organization will not use any product's approval status in a way that, in the opinion of GSA EP:
  - Is inconsistent with the scope of the product's approval status.
  - Brings the credibility of GSA FIPS 201 EP into question.
  - Is misleading or inaccurate.
- The organization agrees upon withdrawal, suspension or revocation of compliance status to immediately cease and desist any and all advertising or statements claiming the approval status of the affected product(s).

---

<sup>1</sup> Readers are considered to be externally-facing if they are designed for placement and use on doors that provide entry to a building or facility. Such readers are considered more susceptible to vandalism, tampering and electrical compromise.

**FIPS 201 Evaluation Program**  
**Attestation Form for Biometric Authentication Reader**

- The organization will use the approval status only in the manner for which it was issued and reference only the requirements of the specific category to which the product was found to be compliant
- The organization is aware that any false claims could result in a penalty as defined by the Federal Acquisition Regulation (FAR) including removal of the product from the Approved Products List.

Signature		Date	
Name			
Title			