

# FIPS 201 Evaluation Program

## Attestation Form for Authentication Key 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>	11.0.0
-----------------------------------	--------

### Requirements being attested to:

Identifier #	Requirement Description	Source
R-AUK.1	Contact card readers shall conform to the ISO7816 standard for the card-to-reader interface.	FIPS 201-1, Section 4.5.1  Para 1 pg.37
R-AUK.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-AUK.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-AUK.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-AUK.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 Authentication Key Reader**

Identifier #	Requirement Description	Source
		Para 1 pg.4
R-AUK.6	PIV Readers shall {not generate a Programming Voltage.}	Card /Card Reader Interoperability Requirements, Section 2.1.1.1
R-AUK.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-AUK.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-AUK.9	{The reader shall be able to read the PIV Authentication buffer on the PIV Card.}	Derived
R-AUK.10	{The reader shall be able to generate and send a cryptographic challenge to the PIV Card.}	FIPS 201-1 Section 6.2.4 Para 1 pg.50
R-AUK.11	{The reader shall be able to decrypt and match the cryptographic response from the PIV Card using algorithm and key sizes for the PIV Authentication Key as specified in Table 3-1 of SP 800-78-2.}	FIPS 201 Section 6.2.4 Para 1 pg.50
R-AUK.12	{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-AUK.13	{The reader shall be able to provide the personal identification number (PIN) to the card to access the PIV Authentication Key stored on the PIV Card.}	Derived
R-AUK.14	{The reader shall be able to conduct a standards-compliant PKI path validation on the PIV Authentication Certificate}. The related digital certificate is checked to ensure that it is from a trusted source.	FIPS 201-1 Section 6.2.4 Para 1 pg. 50
R-AUK.15	{The revocation status of the certificate is checked to ensure current validity}	FIPS 201-1 Section 6.2.4 Para 1 pg.50
R-AUK.16	{If the intended purpose for the reader is for physical access, then the reader shall contain an integrated PIN input device.}	FIPS 201-1, Section 4.5.3

# **FIPS 201 Evaluation Program**

## **Attestation Form for Authentication Key Reader**

Identifier #	Requirement Description	Source
		Para 1 pg.37
R-AUK.17	The Subject Distinguished Name (DN) and FASC-N from the authentication certificate are extracted and passed as input to the authorization function.	FIPS 201-1 Section 6.2.4 Para 1 pg.50
R-AUK.18	{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

### **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).
- 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			

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