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

Company Name	

Product/Service Information

Name	
Part Number	
Hardware Version	
Software Version	
Firmware Version	

Lab Specific Information

Approval Procedure Version	8.0.0

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, Section 4.5.1
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, Section 4.5.1
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 2.2.2.2
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 2.2.2.3
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
R-AUK.6	PIV Readers shall not generate a Programming Voltage.	Card /Card Reader Interoperability Requirements,

FIPS 201 Evaluation Program
Attestation Form for Authentication Key Reader

Identifier #	Requirement Description	Source
		Section 2.2.2.1
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 2.2.2.4
R-AUK.8	The reader buffer size shall be no less than 256 bytes.	Card /Card Reader Interoperability Requirements, Section 3.2.1.1
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 Section 6.2.4
R-AUK.11	The reader shall be able to decrypt and match the cryptographic response from the PIV Card.	FIPS 201 Section 6.2.4
R-AUK.12	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.13	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 Section 6.2.4
R-AUK.14	The revocation status of the certificate is checked to ensure current validity	FIPS 201 Section 6.2.4
R-AUK.15	If the intended purpose for the reader is for physical access, then the reader shall contain an integrated PIN input device.	FIPS 201, Section 4.5.3
R-AUK.16	The reader shall be able to parse the PIV Authentication Certificate to extract relevant fields (signer DN, FASC-N) for the purpose of access control.	FIPS 201 Section 6.2.4
R-AUK.17	If the reader contains a cryptographic module, it shall be validated to FIPS 140-2 with an overall Security Level 1 (or higher).	Derived

Signature

FIPS 201 Evaluation Program
Attestation Form for Authentication Key Reader

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			