FIPS 201 Evaluation Program
Attestation Form for CHUID Authentication Reader (Contact)

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	2.0.0

Requirements being attested to:

Identifier #	Requirement Description	Source
R-CHU-CA.1	Contact card readers shall conform to the ISO 7816 standard for the card-to-reader interface.	FIPS 201, Section 4.5.1
R-CHU-CA.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 4.5.2
R-CHU-CA.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-CHU-CA.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-CHU-CA.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 2.2.2.4
R-CHU-CA.6	PIV Readers shall not generate a Programming Voltage.	Card /Card Reader Interoperability Requirements, Section 2.2.2.1

FIPS 201 Evaluation Program
Attestation Form for CHUID Authentication Reader (Contact)

Identifier #	Requirement Description	Source
R-CHU-CA.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-CHU-CA.8	The reader buffer size shall be no less than 256 bytes.	Card /Card Reader Interoperability Requirements, Section 3.2.1.1
R-CHU-CA.9	The reader shall be able to read the CHUID buffer on the PIV Card.	FIPS 201-1, Section 6.2.2
R-CHU-CA.10	The authentication attempt shall compare the CHUID expiration date to the current date and determine card expiry.	FIPS 201-1, Section 6.2.2
R-CHU-CA.11	The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered.	FIPS 201-1, Section 6.2.2
R-CHU-CA.12	One or more of the CHUID data elements are used as input to the authorization check	FIPS 201-1, Section 6.2.2
R-CHU-CA.13	For performing cryptographic operations (during verification of CHUID signature), the cryptographic module shall be FIPS 140-2 validated with an overall Security Level 1 (or higher).	Derived

Signature

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