

FIPS 201 Evaluation Program

Attestation Form for Caching Status Proxy

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	1.0.0
----------------------------	-------

Requirements being attested to:

Identifier #	Requirement Description	Source
CSP.1	If a caching status proxy is employed, information about the cardholder {for performing all PIV authentication mechanisms}, including the cardholder's certificate, must be added to the database {used}.	SP 800-116, Section 7.4
CSP.2	Enrollment using a caching status proxy {shall} collect and store information required for all supported FIPS 201 authentication mechanisms needed. {i.e. PIV, BIO, CHUID and CAK},	SP 800-116, Section 7.4
CSP.3	The caching status proxy obtains the PIV Authentication or asymmetric Card Authentication Key certificate from the PIV Card, validates the certificate (including checking the certificate's revocation status), and sends a challenge to the card to verify that the card holds the private key corresponding to the certificate prior to adding it to its database along with other information regarding the individual.	SP 800-116, Section 7.4
CSP.4	The cached data shall be protected against tampering.	SP 800-116, Section 7.5
CSP.5	The caching status proxy shall periodically re-validate all of the certificates in its database. The cache status must be updated at least once every 24	SP 800-116, Section 7.4

FIPS 201 Evaluation Program

Attestation Form for Caching Status Proxy

Identifier #	Requirement Description	Source
	hours.	
CSP.6	The caching status proxy shall deactivate the access privileges of any {registered} individual {in the database} whose certificate has expired or has been revoked.	SP 800-116, Section 7.4
CSP.7	The CHUID may be collected at registration, but it should be treated as if it were a password for purposes of retention, i.e., hashed, the hash stored, and the CHUID deleted.	SP 801-116, Section 7.4
CSP.8	If the Product is capable of registering PIV information directly from a PIV Card, it uses GSA FIPS 201 EP approved PIV Middleware.	Derived
CSP.9	The Product must support all of the asymmetric algorithms permitted for the PIV Authentication Key and/or Card Authentication Key , as specified in Table 3-1 of SP 800-78-1, i.e., RSA 1024 (through 31 December 2013), RSA 2048, and ECDSA P-256.	SP 800-116, Section 6.1
CSP.10	The Product uses a cryptographic module validated to FIPS 140-2.	Derived
CSP.11	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

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).

FIPS 201 Evaluation Program
Attestation Form for Caching Status Proxy

- 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			