FIPS 201 Evaluation Program
PACS Test Card Loaner Set
User Guide

VERSION 1.0.1

FIPS 201 Evaluation Program

May 21, 2014

Office of Government-wide Policy
Office of Technology Strategy
Identity Management Division
Washington, DC 20405

1. Overview

The General Services Administration (GSA) is responsible for supporting the adoption of interoperable and standards-based Identity, Credential, and Access Management (ICAM) technologies throughout the Federal Government. As part of that responsibility, GSA operates and maintains the Federal Information Processing Standard (FIPS) Publication 201 Approved Products List (APL) , as well as services for Federal ICAM (FICAM) conformance and compliance.

The Federal Government's emphasis on strong authentication for physical access to federal agencies contributes to the growing need to support agency implementers. Accordingly, the FIPS 201Evaluation Program has produced a set of test cards available for loan to agencies and vendors for the purpose of testing Physical Access Control Systems (PACS) in advance of submitting their products to the Program for testing. The cards may also be used by security professionals and integrators to ensure their system was installed correctly and is able to handle security threats and interoperability issues.

This User Guide document provides direction/information on how to use the ICAM Test Cards in an optimal manner.

2. ICAM Test Cards

Table 1 shows the ICAM Test Cards and their configuration. They are used in conjunction with the ICAM PKI as prescribed in the FIPS 201 Evaluation Program Functional Requirements and Test Cases document.

Table 1 - ICAM Test Card Configurations

ICAM Test Card	Description	Threat Type
1	Golden PIV	None
2	Golden PIV-I	None
3	Substituted keypair in PKI-AUTH certificate	Manipulated Data
4	Tampered CHUID	Manipulated Data
5	Tampered PIV and Card Authentication Certificates	Manipulated Data
6	Tampered PHOTO	Manipulated Data
7	Tampered FINGERPRINT	Manipulated Data
8	Tampered SECURITY OBJECT	Manipulated Data
9	Expired CHUID signer	Invalid Date
10	Expired certificate signer	Invalid Date
11	PIV Authentication Certificate expiring after CHUID	Invalid Date
12	Authentication certificates valid in future	Invalid Date
13	Expired authentication certificates	Invalid Date
14	Expired CHUID	Invalid Date
15	Valid CHUID copied from one card to another **(PIV)**	Copied Credential
16	Valid Card Authentication Certificate copied from one card to another **(PIV)**	Copied Credential
17	Valid PHOTO copied from one card to another **(PIV)**	Copied Credential
18	Valid FINGERPRINT copied from one card to another **(PIV)**	Copied Credential

ICAM Test Card	Description	Threat Type
19	Valid CHUID copied from one card to another **(PIV-I)**	Copied Credential
20	Valid Card Authentication Certificate copied from one card to another **(PIV-I)**	Copied Credential
21	Valid PHOTO copied from one card to another **(PIV-I)**	Copied Credential
22	Valid FINGERPRINT copied from one card to another **(PIV-I)**	Copied Credential
23	Private and Public Key mismatch	No Trusted Path
24	Revoked authentication certificates	Revoked Credential

3. ICAM PKI Setup

Table 2 shows the ICAM PKI Root/Path Table, which helps explain the Fault Bridge setup.

Table 2 - ICAM PKI Path Descriptions

Path Number	Fault description	Operational group
1	Invalid CA Signature	Manipulated Data
2	Invalid CA notBefore Date	Revoked/Date Invalid
3	Invalid CA notAfter Date	Revoked/Date Invalid
4	Invalid Name Chaining	Standards Conformant Processing
5	Missing Basic Constraints	Standards Conformant Processing
6	Invalid CA False Critical	Manipulated Data
7	Invalid CA False not Critical	Standards Conformant Processing
8	Invalid pathLenConstraint	Standards Conformant Processing
9	keyUsage keyCertSign not set	Standards Conformant Processing
10	keyUsage Not Critical	Standards Conformant Processing
11	keyUsage Critical cRLSign False	Standards Conformant Processing
12	Invalid inhibitPolicyMapping	Standards Conformant Processing
13	Invalid DN nameConstraints	Standards Conformant Processing
14	Invalid SAN nameConstraints	Standards Conformant Processing
15	Invalid Missing CRL	Standards Conformant Processing
16	Invalid Revoked CA	Revoked/Date Invalid
17	Invalid CRL Signature	Manipulated Data
18	Invalid CRL Issuer Name	Standards Conformant Processing
19	Invalid Old CRL nextUpdate	Revoked/Date Invalid
20	Invalid CRL notBefore	Manipulated Data
21	Invalid distributionPoint	Standards Conformant Processing
22	Valid requiredExplicitPolicy	Standards Conformant Processing
23	Invalid requiredExplicitPolicy	Standards Conformant Processing
24	Valid GeneralizedTime	PKI/Crypto Compatibility
25	Invalid GeneralizedTime	Standards Conformant Processing
26	ECC prime256v1	PKI/Crypto Compatibility
27	ECC secp384r1	PKI/Crypto Compatibility
28	Invalid ECC Signature p256	Manipulated Data

Path Number	Fault description	Operational group
29	Invalid Policy Mapping p256	Standards Conformant Processing
30	Invalid ECC Signature secp384r1	Manipulated Data
31	Invalid Policy Mapping secp384r1	Standards Conformant Processing
32	Invalid SKID	Standards Conformant Processing
33	Invalid AKID	Standards Conformant Processing
34	Invalid CRL format	Standards Conformant Processing
35	4096 RSA key	PKI/Crypto Compatibility
36	Invalid CRL Signer	Manipulated Data
37	OCSP Invalid Response Signer	Manipulated Data
38	OCSP Expired Response Signer	Revoked/Date Invalid
39	OCSP Revoked Response Signer nocheck not present	Revoked/Date Invalid
40	OCSP Revoked Response Signer nocheck is present	Standards Conformant Processing

4. Building a Valid Trust Path (Direct Trust)

A valid trust path is the simplest way to use the ICAM Test card set. In order to build a valid trust path, the following certificates are needed:

- ICAM_Test_Card_Root_CA.cer (Trusted Root Certification Authorities)
- ICAM Test Card Signing CA[1] (Intermediate Certification Authorities)

To install the valid direct trust path, open the appropriate certificate store using the Microsoft Management Console Certificates snap-in. In most cases, the local computer certificate store will be used, but this may change for different applications. Expand the certificates tree to view the certificate store folders subtrees. Import the Test Card Root CA certificate to the Trusted Root Certification Authorities folder. Import the CertsIssuedToICAMTestCardSigningCA.p7c certificate package into the Intermediate Certification Authorities folder. The valid direct trust path is now configured, and the card may be validated.

Note: Only one valid trust path should be installed at a time. Remove any ICAM Trust Root from the Trusted Root Certification Authorities cert store folder except the one that is currently being used.

Note: Some applications may require additional configuration.

5. Building a Valid Trust Path (Bridged Trust)

If you wish to implement a **valid trust path through a bridge** (useful for policy mapping use cases), you will need to install the following certificates:

[1] This file is a .p7c certificate package containing the signing certificate. By default, this file cannot be opened directly in windows. If you wish to explore the package and view the cert, you must rename the file to .p7b.

- A "Valid" certificate from http://http.apl-test.cite.fpki-lab.gov/roots/ (e.g. ICAM_Valid_Generalized_Time.cer) (Trusted Root Certification Authorities)
- ICAM_Test_Card_Bridge_CA[2] (Intermediate Certification Authorities)
- ICAM_Test_Card_Root_Crosscert[2] (Intermediate Certification Authorities)
- ICAM_Test_Card_Signing_CA[2] (Intermediate Certification Authorities)

Implementing a trust path through a Fault Bridge is performed in a similar fashion to direct trust. Download the files listed above. Remove any previously installed trust roots from the Trusted Root Certification Authorities certificate store folder and import one of the valid trust roots. Next, import the certsIssuedToICAMTestCardBridgeCA.p7c, certsIssuedToICAMTestCardRootCA.p7c, and certsIssuedToICAMTestCardSigningCA.p7c the Intermediate Certification Authorities folder. Note that the certsIssuedToICAMTestCardBridgeCA.p7c will contain each of the cross certificates needed to build paths for each of the Fault Bridge trusted roots. Leave these cross certificates installed for additional tests and manipulate which path is valid by removing and adding one trusted root at a time. With each of the above certificates installed, the test card can now use bridged trust.

6. Building an Invalid Trust Path (Bridged Trust)

Implementing an invalid trust path through a bridge is an identical process to building the valid trust path through a bridge, described above. If the cross certificates and signing ca has already been installed, simply remove the previous root certificate from the Trusted Root Certification Authorities certificate store folder and import the desired Fault Bride root. It is recommended that testing of invalid trust paths be performed with valid Test Cards 1 and 2, the Golden PIV and PIV-I.

7. Creating your own Test Certificates

GSA has added two subordinate CAs, which can be used by vendors to issue test certificates to create their own test cards that can leverage the ICAM PKI. To enable full use of the various fault conditions, these subordinate CAs are constrained to the following name space:

C=US
O=U.S. Government
OU=Independent Testing

To create vendor-specific cards in the ICAM Test Environment, download one of the CA's p12[3] from http://http.apl-test.cite.fpki-lab.gov/roots/ICAMIndTestSubCA1.p12 or http://http.apl-test.cite.fpki-lab.gov/roots/ICAMIndTestSubCA2.p12

ICAMIndTestSubCA1 has a 2048 bit RSA key, ICAMIndTestSubCA2 has a 3072 bit RSA key. The vendor can then load the appropriate certificate and private key into their own CA implementation, and issue either another subordinate CA to issue end-entity certificates or issue end-entity certificates directly from this CA.

[2] This file is a.p7c certificate package containing the appropriate certificates. By default, these files are unable to be opened directly in Windows. If you wish to explore the package and view the certificates therein, you must rename the file to .p7b.
[3] For the requested password, use: icamindtest

When issuing end-entity certificates, the Certificate Revocation List Distribution Point(CDP) must point to a location under control of the vendor. If Online Certificate Status Protocol (OCSP) is desired, the OCSP URI in the Authority Information access (AIA) must also point to an OCSP responder managed by the vendor.

If the vendor decides to issue a subordinate CA certificate from the GSA-provided ICAM Independent SubCA, please provide a copy of that subordinate CA certificate to the FIPS 201 Evaluation Program so it can be added to the appropriate ICAM Independent SubCA's SIA p7c file.

ICAM Independent Test SubCA1
SIA: http://http.apl-test.cite.fpki-lab.gov/sia/certsIssuedByICAMIndTestSubCA1.p7c[4]
nameConstraints: permitted: c=us,o=U.S. Government,OU=Independent Testng

ICAM Independent Test SubCA2
SIA: http://http.apl-test.cite.fpki-lab.gov/sia/certsIssuedByICAMIndTestSubCA2.p7c[4]
nameConstraints: permitted: c=us,o=U.S. Government,OU=Independent Testng

[4] This is a.p7c file. By default, these files are unable to be opened directly in Windows. If you wish to explore this file, you must rename the file to .p7b.