FRTC Express Process Companion Paper

FRTC VERSION 1.4.2 Rev A

FIPS 201 EVALUATION PROGRAM

March 31, 2021

Version 1.0

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

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	2/12/2021	Initial draft for comment	Public
Initial Release	1.0	3/31/2021	Initial publication	Public

Table of Contents

Table of Contents **3**

1. Background **4**

2. Objectives **4**

3. Methodology **5**

4. Outcome **5**

5. Test Cases and Changes **6**

5.1 Consolidated Test Cases 6

5.2 Deprecated Test Cases 9

5.3 New Test Cases 10

References **12**

1. Background

The Federal Information Processing System (FIPS) 201 Evaluation Program lab tests Physical Access Control Systems (PACS) submitted by industry vendors for conformance and compliance to appropriate standards (e.g., NIST [SP 800-73], NIST [SP 800-78]). The purpose of this testing is to list conformant and compliant products on the FIPS 201 Approved Products List (APL).

PACS solutions are tested against controls identified in the Functional Requirements Test Cases [FRTC] and documented in a consolidated lab test. The [FRTC] controls have been revised and updated as security and usability requirements are identified, and is currently composed of 267 individual test cases. The consolidation effort labels each test case as Required, Consolidated, and New. Technical tests and checks of a PACS solution support the following functionality and interoperability categories with FIPS 201 compliant smart cards:

- Cryptographic function;
- Certificate and identifier data;
- Path discovery and validation;
- Biometric validation; and
- PACS-specific security and usability considerations.
- Test case categories are also separated into the following subsections that align to the PACS lifecycle:
- Subsection 2 – Requirements at Time of In-Person Registration
- Subsection 4 – Requirements for Automated Provisioning in Accordance with [PIV in ePACS] PIA-8
- Subsection 5 – Authentication at Time of Access Test Cases
- Subsection 7 – PACS Design Use Cases

2. Objectives

GSA seeks to streamline testing to encourage solution providers to ensure listings on the APL are current and relevant to purchasing officials. GSA tasked the FIPS 201 Evaluation Program to review current FRTC controls for updates or revisions to the current testing procedures to potentially drive efficiencies and subsequently reduce PACS solution testing times and bring testing requirements in line with real world scenarios. The FIPS 201 Evaluation Program determine the following would meet GSA's goals:

1. Update Applications received within one year of prior approval can be tested under FRTC Express
2. Fewer test cases in the FRTC express over full FRTC, with an estimated 30% reduction in testing time.
3. Encourage most recent versions of solutions to be approved and listed, allowing the government to install latest solutions.

3. Methodology

The lab used the following methodology and approach for improving efficiencies is as follows:

- Review existing Functional Requirements Test Cases Matrix [FRTC] v1.3.3
- Review failure analysis to inform gaps, areas of improvement, and consistency with proposed consolidations
- Evaluate real world operational use of Federal PKI implementations
- Perform consolidation of commonly test criteria and create new comprehensive test cases
- Perform risk-based decision on test cases if alternative test case performs similar functionality
- Perform risk analysis on every test case that was labeled as Consolidated to validate reduction approach
- Perform team review and revisions

4. Outcome

For updated products being tested by the GSA Test Lab, a 27% overall reduction in test cases, improving testing process efficiency and reducing level of effort, is achievable through updates in FRTC test methodology and process. When considering Time of Registration and Time of Access only (not Design Analysis), the reduction is 36%.

These efficiencies were achieved by consolidating several test cases into a single new test case. Greater efficiency was achieved by labeling some test cases, beyond those that were consolidated, as deprecated. The consolidation combines several tests, or removes tests, that will still indicate compliance of an updated solution.

5. Test Cases and Changes

5.1 Consolidated Test Cases

Old Test Case Goals	Top Level Test Case #	Test Case #s consolidated into top-level
Positive PIV card registration and validation	2.16.15	2.01.01 2.06.01 2.06.07 2.06.08 2.06.09 2.08.01 2.15.01 2.16.01 2.16.04 2.16.08 2.17.10 2.17.12
Positive CAC card registration and validation	2.16.16	2.16.01
Positive PIV-I card registration and validation	2.16.17	2.01.02 2.06.12 2.06.13 2.06.14 2.16.01 2.16.06 2.16.10 2.17.10 2.17.12
Test to determine invalid signature in certificate	2.01.03	2.01.04 2.10.08 2.10.09
Test to reject Not-After date of the intermediate certificate is sometime in past	2.02.04	2.02.02

Basic Constraint extension is present and critical in intermediate CA but CA component is false	2.04.03	2.04.02
intermediate certificate includes Key Usage extension keyCertSign and crlSign false, and Key Usage not critical	2.05.04	2.05.01 2.05.02 2.05.03
Policy checking for PIV PIV-I on PIV/PIV-I hardware, PIV/PIV-I CardAuth, PIV/PIV-I Content Signing verification at registration	2.06.18 2.06.19	2.06.02 2.06.05 2.06.10 2.06.11 2.06.15 2.06.16 2.06.17
Certificate revocation check	2.09.02	2.09.01 2.09.03
OCSP to CRL rollover	2.09.12	2.09.11
OID inspection on Card Auth certificate	2.16.09	2.16.11
Positive PIV card time of access test	5.15.15	5.01.01 5.06.01 5.06.07 5.06.08 5.06.09 5.08.01 5.14.01 5.15.01 5.15.04 5.15.08 5.16.02 5.16.10 5.16.12 7.06.03
Positive CAC card time of access test	5.15.16	5.15.01 5.16.02 5.16.10 5.16.12

Positive PIV-I card time of access test	5.15.17	5.01.02 5.06.12 5.06.13 5.06.14 5.15.01 5.15.06 5.15.10 5.16.02 5.16.10 5.16.12 7.06.03
EKU Extension verification	5.05.04	5.05.01 5.05.02 5.05.02
EKU KeyPurpose OID verification	5.15.05	5.15.07
Constraints extension is present and critical in the intermediate CA certificate but the cA component is false	5.04.03	5.04.02
Policy checking for PIV PIV-I on PIV/PIV-I hardware, PIV/PIV-I CardAuth, PIV/PIV-I Content Signing verification at time of access	5.06.18	5.06.02 5.06.05 5.06.10 5.06.15 5.06.16 5.06.17
CHUID Signature policy verification	5.06.19	5.06.11
Unknown End Entity certificates at time of access	5.09.02	5.09.01
Revoked End Entity certificates at time of access	5.09.12	5.09.03 5.09.11
EKU KeyPurpose OID verification	5.15.11	5.15.09
Use cards with SHA-384 Signature	5.16.08	5.16.11

.

5.2 Deprecated Test Cases

Test Case Goal	Test Case # being Deprecated
notBefore Date on Intermediate CA Registration	2.02.01
notBefore on End Entity at Registration	2.02.03
NotAfter on EndEntity at registration	2.02.05
notBEfore date on crl on cert path on registration	2.09.06
Invalid End Entity signature at time of access	5.01.04
notBefore Date on Intermediate CA Time of access	5.02.01
notBefore on End Entity at Time of access	5.02.02
NotAfter on End Entity sometime in past at time of access	5.02.04
CRL with notBefore in the future at time of access	5.09.07
PKIX_OCSP_NOCHECK Flag on Revoked OCSP signature	2.15.3 2.15.04 5.14.03 5.14.04

5.3 New Test Cases

Test Case Goal	Test Case # being added
Verify product's ability to recognize when intermediate certificate includes Key Usage extension keyCertSign and crlSign false, and Key Usage not critical	2.05.04
Policy OID checking at registration	2.06.18
Policy OID checking at registration	2.06.19
OCSP to CRL rollover	2.09.12
CBEFF for Facial	2.11.02
CBEFF for fingerprint	2.13.07
CRL to OCSP rollover	2.15.06
Valid PIV registration positive Test Case	2.16.15
Valid CAC registration positive Test Case	2.16.16
Valid PIV-I registration positive Test Case	2.16.17
Verify product's ability to recognize when intermediate certificate includes Key Usage extension keyCertSign and crlSign false, and Key Usage not critical	5.05.04
Policy OID verification at time of access	5.06.18

Policy OID verification at time of access	5.06.19
Name constraint checking at time of access	5.08.03
OCSP to CRL failover and End Entity certificate validation	5.09.12
CRL to OCSP failover	5.14.05
Valid PIV positive Test Case at time of access	5.15.15
Valid CAC positive Test Case at time of access	5.15.16
Valid PIV-I positive Test Case at time of access	5.15.17

References

[FIPS 201]	Personal Identity Verification (PIV) of Federal Employees and Contractors, Federal Information Processing Standard 201-2, August 2013, or as amended http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
[FRTC]	FIPS 201 Evaluation Program Functional Requirements and Test Cases, August 2018 https://www.idmanagement.gov/docs/pacsapp-frtcworkbook.xlsx
[PIV in ePACS]	Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), March 2014, or as amended https://www.idmanagement.gov/docs/pacs-piv-epacs.pdf
[SP800-73]	Interfaces for Personal Identity Verification, NIST Special Publication 800-73-4, May 2015, or as amended https://csrc.nist.gov/publications/detail/sp/800-73/4/final
[SP800-78]	Cryptographic Algorithms and Key Sizes for Personal Identity Verification, NIST Special Publication 800-78-4, May 2015, as amended https://csrc.nist.gov/publications/detail/sp/800-78/4/final