Approved PACS Topology Mapping Document (PACS 13.02)

VERSION 1.3.3 Rev. G

FIPS 201 EVALUATION PROGRAM

February 1, 2018

FINAL

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

Document History

Status	Version	Date	Comment	Audience
First draft	0.0.1	2/6/2014	Mapping for PACS 13.02	Limited
Draft	0.0.2	2/14/2014	Initial edit	Limited
Draft	0.0.3	2/18/2014	Updated definitions, diagrams	Limited
Draft	0.0.4	2/19/2014	Team edits	Limited
Draft	0.0.5	2/20/2014	Team edits	Limited
Draft	0.0.6	2/22/2014	Cleaned up table inconsistencies	Limited
Draft	0.1.0	5/16/2014	Cleaned up grammatical errors.	Public
Draft	0.1.1	7/8/2014	Revised category descriptions and Topology illustration to make it clearer that the configurations are examples, and that other approaches are acceptable. Changed Program name back to FIPS 201 Evaluation Program.	Public
Final	1.3.0	3/2/2015	Revised to be in synch with FRTC v1.3.0	Public
Final	1.3.3	9/8/2017	• Revised to synch with PACS FRTC v1.3.3. • Updated links to online normative references. • Added security classifications, severity level definitions, APL listing requirements. • Reactivated 12 previously deprecated test cases, clarified 16, added 58, and deprecated 14 test cases. • Biometric verification of cardholder is required at time of registration. Security Object verification is mandatory at time of registration.	Public
Final	1.3.3 Rev A	9/18/2017	• Corrected typos. • Re-ordered and renumbered test certificate policy and interoperability test cases so that the same card can be used for multiple tests before switching to the next card. • Added one (1) missing certificate policy test case for PIV Authentication at time of access.	Public
Final	1.3.3 Rev B	11/3/2017	• Updated normative policy references for Federal Common Policy, FBCA, SSP, and PIV-I. • Updated Discovery Object tests to reflect that max retries of test cards are set to 10, not 5. • Added ICAM Test Card 54 (NFI PIV-I).	Public
Final	1.3.3 Rev C	1/7/2018	• Replaced all instances of the use of ICAM Test Card #01 with ICAM Test Card 46.	Public

			• Replaced all instances of the use of ICAM Test Card #02 with ICAM Test Card 54. • Corrected expected Global PIN retry counter, Test Cases 2.18.02 and 5.17.02. • Added ICAM Test Card 55 (Missing Security Object) and Test Case 2.14.03. • Clarified the expected result of Test Cases 2.16.02 and 5.15.02.	
Final	1.3.3 Rev. D	4/24/2018	• Deprecated Test Cases 2.06.03, 2.06.04, 5.06.03., 5.06.04, and 5.11.01. (and removed Section 5.11). • For time-of-access fault path testing, included instructions as to which golden card must be registered with the PACS. • Activated ICAM Test Card 48 (PPS with LEN value greater than zero). • Corrected bit ordering of last 5 digits of example FASC-N in Credential Identifier Processing in Section 5. • Corrected card type from Card Authentication Certificate to PIV Authentication Certificate in Test Cases 2.06.07 and 5.06.07. • Added "Valid/Invalid" column to card description table. • Verified and updated links to normative references. • Clarified card type (PIV/PIV-I) for test cases 7.05.01 and 7.05.02	Public
Final	1.3.3 Rev. E	6/21/2018	• Deprecated Test Case 5.12.02 • Clarified that Card 7 must be personalized with the tester's biometric. • Removed Fault Paths 37-40 • Deprecated Test Cases 8.01.01-8.10.04 (Handheld)	Public
Final	1.3.3 Rev. F	8/21/2018	• Deprecated Test Cases 2.17.14 and 5.16.14 because RSA 4096 was deprecated by FIPS 186-3 and subsequently SP 800-78-2. • Changed wording of Test Case 5.02.03 to "With ICAM Test Card 46 registered with the PACS, verify product's ability to reject a credential when notAfter date of any certificate in the path is sometime in the past." • Deprecated Test Case 5.02.05 because Test Case 5.02.03 was updated to include all certificates in the path. • Added Test Cases 2.10.8 and 2.10.9 because Paths 3 and 16 can be used to test them.	Public
Final	1.3.3 Rev. G	2/1//2019	• Changed 5.15.04 to "With ICAM Test Card 46" • Deprecated Test Cases 2.04.05 and 5.04.05 (requires SKID to consist of SHA-1 of public key). Going forward, PACS should not enforce this rule.	Public

			• Replaced "CHUID signature" with Card Authentication" in the description for Test Case 5.06.13. We are testing for a Card Authentication certificate policy OID. • The description for Test Case 5.15.04 was changed to, "With ICAM Test Card 46...". • Added Test Cards 57, 58, and 59 and Test Cases 2.09.11, 2.10.10, 5.09.11, and 5.10.1 • Changed Test Case 5.12.05 to " With ICAM Test Card 59 registered..." • Added Sections 4.5 Testing Criteria, 4.5.1 Severity Levels.	

Table of Contents

1. Background *1*

2. Objectives *1*

3. Normative References *1*

4. FIPS 201 Evaluation Program Defined Categories *3*

4.1 PACS and Validation Infrastructure (PVI) Category **3**

4.1.1 PACS Functionality 3

4.1.2 Validation Functionality 4

4.2 PIV Reader Category **4**

4.3 Implementation & FISMA **5**

4.4 Topology Diagrams **5**

4.5 Testing Criteria **7**

4.5.1 Severity Levels 7

4.5.2 APL Listing Requirements 7

4.5.3 Classification Codes and Scoring Guidelines 8

5. Topology Mapping *9*

1. Background

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) 201 Evaluation Program and its associated Approved Products List (APL), as well as services for Federal ICAM (FICAM) conformance and compliance.

2. Objectives

The FIPS 201 Evaluation Program's PACS evaluation process is designed to be agnostic to architecture and focuses solely on functional testing using an end-to-end testing methodology. This document facilitates applicant mapping of the functional requirements identified in *Functional Requirements and Test Cases* [FRTC] to the categories identified in the FIPS 201 Evaluation Program's PACS 13.02 topology.

3. Normative References

[BAA] Buy American Act Certification FAR 52.225-2
https://www.law.cornell.edu/cfr/text/48/52.225-2

Common] FPKIPA X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 1.27, June 29, 2017, or as amended
https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-policy-common.pdf

[E-PACS] FICAM Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), Version 3.0 March 26, 2014
https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/piv-in-epacs.pdf

[FBCA] FBCA X.509 Certificate Policy for Federal Bridge Certification Authority (FBCA), Version 2.31 June 29, 2017, or as amended
http://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FBCA-Certificate-Policy-v2.31-06-29-17.pdf

[FIPS 201] Federal Information Processing Standard 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

[FRTC] FIPS 201 Evaluation Program Functional Requirements and Test Cases
https://www.idmanagement.gov/pacs-frtc-v1-3-3/

[HSPD-12] Homeland Security Presidential Directive 12, August 27, 2004
https://www.dhs.gov/homeland-security-presidential-directive-12

[M-05-24] Office of Management and Budget (OMB) Memorandum M-05-24, August 5, 2005
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf

[M-06-18] Office of Management and Budget (OMB) Memorandum M-06-18, June 30, 2006
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2006/m06-18.pdf

[M-11-11] OMB Memorandum M-11-11, February 3, 2011
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-11.pdf

[PIV-I] CIO Council Personal Identity Verification Interoperability for Issuers, Version 2.0.1 July 27, 2017, or as amended
https://www.idmanagement.gov/piv-i-for-issuers

[PROF] X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program, Version 1.8 June 17, 2017, or as amended
http://www.idmanagement.gov/fpki-cert-profile-ssp/

[Roadmap] FICAM Roadmap and Implementation Guidance, Version 2.0, December 2, 2011
http://www.idmanagement.gov/ficam_roadmap_and_implem_guid/

[Sect508] Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998
http://www.section508.gov/section508-laws

[SP800-73] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-73-4, Part 1-3, May 2015
http://dx.doi.org/10.6028/NIST.SP.800-73-4

[SP800-76] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-76-2, July 2013
http://dx.doi.org/10.6028/NIST.SP.800-76-2.pdf

[SP800-78] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-78-4, May 2015
http://dx.doi.org/10.6028/NIST.SP.800-78-4.pdf

[SP800-96] NIST SP 800-96, September 2006
http://csrc.nist.gov/publications/nistpubs/800-96/SP800-96-091106.pdf

[SP800-116] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116, November 2008
http://dx.doi.org/10.6028/NIST.SP.800-116

[SP800-153] NIST SP 800-153, February 2012
http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf

[TAA] Trade Agreement Act Certification FAR 52.225-6
http://acquisition.gov/far/current/html/52_223_226.html

[UL 294] The Standard of Safety for Access Control System Units, UL Edition Number – 6, Date 05/10/2013, Type ULSTD
https://standardscatalog.ul.com/standards/en/standard_294_6

[UL 1076] The Standard of Safety for Proprietary Alarm Units, UL Edition Number – 5, Date 09/29/1995, Type ULSTD
https://standardscatalog.ul.com/standards/en/standard_1076_5

[UL 1981] The Standard for Central-Station Automation Systems UL Edition Number - 3, Date 10/29/2014, Type ULSTD
https://standardscatalog.ul.com/standards/en/standard_1981_3

4. FIPS 201 Evaluation Program Defined Categories

The PACS 13.02 Topology defines one new category and re-uses a category from the PACS 13.01 Topology (4.1 – 4.2 below). Each of these categories is defined as part of a whole PACS solution that can be tested end-to-end using the [FRTC]. Note that a category is not defined as a single object that is procured as a single SKU. The following definitions define the objects that make up a functional element called a category:

1. ***Compatible*** components are proved to work with each other.
2. ***Interoperable*** components are tested to determine the set of like and related components with which it can reliably be operated in combinations. Interoperable components must use an industry standard (e.g., ISO, ANSI, IETF RFC) to enable standardized interfaces between components.
3. A ***subsystem*** is assembled of compatible components. Hence a subsystem would be tested and acquired as a unit or "configuration item". A subsystem may leverage an interoperable component external to the subsystem.
4. A ***category*** is made up of subsystems, compatible and/or interoperable components that meet functional requirements defined in [FRTC].

The two categories defined by this topology are ***PACS and Validation Infrastructure,*** and ***PIV Reader.*** They are further described in the following sections.

4.1 PACS and Validation Infrastructure (PVI) Category

The PACS and Validation Infrastructure is made up of a single product that has unified the PACS Infrastructure and Validation System functionality from topology 13.01 into a single infrastructure product. The resulting application becomes a unified infrastructure providing both capabilities with a single part number with many compatible components. This section will provide a definition for the compatible components that constitute a PACS and Validation Infrastructure. They are as follows:

1. PACS and Validation Application (PVA) and its server (also called the head-end);
2. Database and its server (often an integral part of the PVA, and on the same server);
3. Controllers (also called bridges, field panels, controllers, or secure controllers);
4. SCVP servers;
5. OCSP responders;
6. Full path discovery and validation software; and
7. Workstations (e.g., for administration, registration of individuals, help desk).

Other approaches that meet the functional requirements are also valid.

4.1.1 PACS Functionality

The PVI's functionality is made up of both PVA functions associated with physical access control and controllers. The PVA software runs on a server (be it physical, virtual image or cloud) and performs traditional PACS functionality as well as full support for FICAM Approved authentication methods leveraging PKI. The PVA communicates with controllers that are connected to PIV Readers. The controller is commonly installed locally to ensure performance and local security. Historically, this has included storing a local database within the controller for increased performance, for making access decisions and event logging should communications be lost with the host. The PVI controller's functionality may include:

1. Communications between the PIV Reader and the PVA;
2. Access control status and logging;
3. I/O controllers;
4. Alarm controllers; and
5. Door controllers for the lockset, door position switch and request to exit.

Some vendors might want to consolidate these controller functions into a single component to increase performance or reduce the overall deployed footprint, thereby lowering costs.

A PACS and Validation Infrastructure is a diverse environment that interoperates with many different subsystems outside the scope of the current FIPS 201 Evaluation Program. These often include:

1. Intrusion Detection Systems (IDS);
2. Video Management Systems (VMS);
3. Visitor Management Systems (also called VMS);
4. Enterprise Identity Management Systems (E-IdM); and
5. Physical Security Information Management systems (PSIM).

These additional subsystems comprising a total physical security program may become categories in a future FIPS 201 Evaluation Program spiral.

4.1.2 Validation Functionality

Validation functions of the PVI provide the necessary capabilities to perform identification and authentication of the credential and the bearer of a credential according to various approved FICAM Authentication Methods. These methods and the controls necessary to implement them, are defined fully in [E-PACS] and tested as an end-to-end system according to [FRTC]. Validation functions, as defined by the FIPS 201 Evaluation Program, have a direct impact on PACS behaviors as well as the PIV Reader. The interoperable components that may constitute or support the PVA's validation functionality include:

1. SCVP Servers/Clients;
2. OCSP responders; and
3. Full path discovery and validation software.

PKI validation functions are in integral part of the PVA. For convenience, an SCVP Client (and potentially server) may be part of the solution that generally resides in the same footprint as the PVA.

Other approaches that meet the functional requirements are also valid.

4.2 PIV Reader Category

A PIV Reader is a shared category with the 13.01 topology. It is an accepting device as defined in [E-PACS] that provides the human interface, the card interface, and the communications[1] to and from the PACS and Validation Infrastructure. It is installed at a door, portal, or gateway. As an accepting device, a PIV Reader may be a wholly-integrated unit, or it may be an assembly of components including:

1. Contact smart card reader;
2. Contactless smart card reader;
3. LCD display;
4. LED lights;
5. Audio announcers;
6. PIN pad;
7. Fingerprint sensor;
8. Other biometric modalities (e.g., iris); and
9. Communications to a PACS and Validation Infrastructure (e.g., Wiegand, RS-485, secure wireless, Ethernet).

The PIV Reader is a device that is installed at the door and performs functions to interact with the bearer of the credential, the credential itself. This configuration can vary. The

[1] Vendors have the flexibility on how the communication works (i.e., whether communication is direct at run time or other mechanisms are used).

PIV Reader must support a minimum of one FICAM authentication mode as defined in [E-PACS], but may support multi-factor authentication.

Other approaches that meet the functional requirements are also valid.

4.3 Implementation & FISMA

The Government recognized the importance of information security to the economic and national security interests of the United States, and to address these concerns the President in December 2002 signed into law the E-Government ACT (Public Law 107347). Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), which requires each federal agency to develop, document and implement an agency-wide program to provide information security for the information and information systems that support operations and assets of an agency.

Since all PACS and Validation Infrastructure requires access to private or public network domains at a minimum for PKI validation services, FISMA requirements for securing access to the systems hosting these applications and communications to their infrastructures come into play.

The specific requirements needed to comply with FISMA vary upon the security policies and procedures based on the individual agency's risk assessment.

Also impacting requirements is the manner by which the 13.02 topology is deployed. The deployment options for 13.02 and definitions may include the following:

1. **Standalone Server** - A built-for-purpose server that may or may not belong to a domain or workgroup but hosts the PVA, typically hosted locally in a secure LAN room or NOC and accessible through the locally configured network or enterprise.
2. **Server Cluster** - A built for purpose cluster used to host the PVA and provide high performance computing, with high availability characteristics, typically hosted locally in a secure LAN room or NOC and accessible through the locally configured network or enterprise.
3. **Virtual Server** - Uses a method of hosting virtual machines within a physical server environment, and is typically hosted locally in a secure LAN room or NOC and accessible through the locally configured network or enterprise.
4. **Cloud Software as a Service (SaaS)** - When implementing cloud based services, communications between endpoints (i.e., controllers and the PVA SaaS) is generally protected by secure VPN connections or other FICAM-approved cryptographic protocol.
    a. *Private* - A private cloud solution is typically a vendor-hosted, dedicated computing resource allocated within the scope of the privately-controlled network infrastructure. This model provides a level of isolation from Public network access, while enabling SaaS capability. This allows enterprise security applications to be shared among organizations or facilities within the private network domain.
    b. *Public* - A public cloud solution could provide PVA functionality in the SaaS model hosted by the vendor. This type of implementation generally travels outside the locally configured network to outside hosted networks.

Depending on the deployment options, additional functional requirements may vary to reflect FISMA guidelines, as it relates to protection of information and assets

4.4 Topology Diagrams

The Applicant must submit a topology diagram to the FIPS 201 Evaluation Program. The diagram must show the architectural linkage between the PVI and the interoperable components that make up an end-to-end system. It must show which components belong to a given category. The diagram facilitates an understanding of how a system is linked together and how it performs the functions required by [FRTC]. In other words, the diagram is a communications tool to enable the FIPS 201 Evaluation Program to understand how a given solution is put together to support end-to-end operational testing.

Figure portrays possible locally-hosted approach. Figure 2 portrays a possible cloud-hosted approach. Other approaches that meet the functional requirements are also valid.

Figure 1 – Sample Topology diagram of a locally-hosted PVA

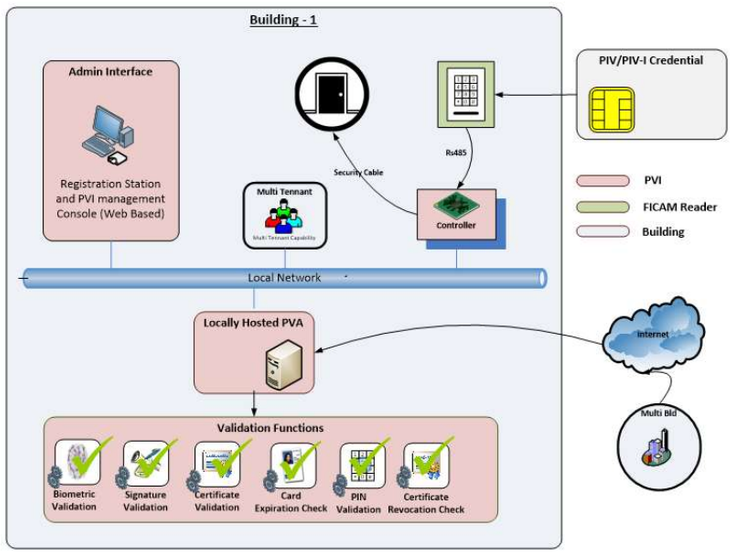
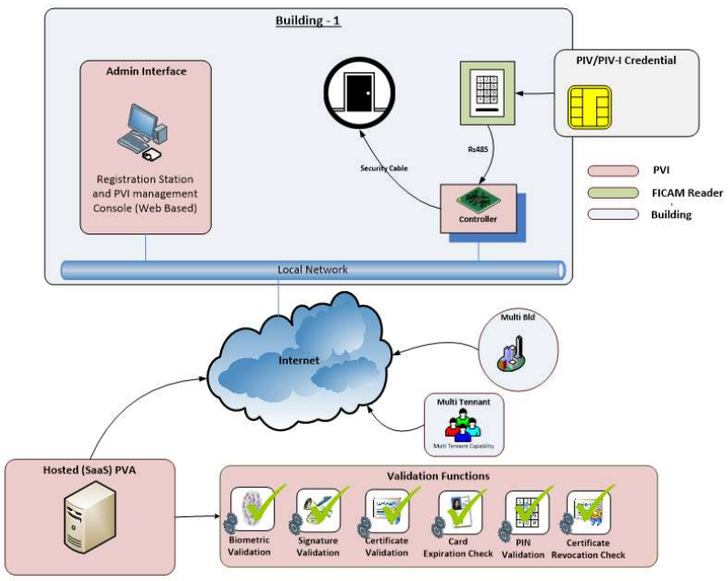


Figure 2 – Sample Topology diagram of a cloud-hosted (SaaS) PVA



A complete topology diagram identifies every component that makes up an applicant's solution for the FIPS 201 Evaluation Program categories and provides the specific linkages (communications, internal messaging) that makes up the solution. As new topologies are adopted per the FIPS 201 Evaluation Program's *Topology Adoption Process* [TAP], applicants must map their solution and its components into these new topologies.

4.5 Testing Criteria

4.5.1 Severity Levels

If [FRTC] functional requirements are revised due to time-sensitive security threats, noted technology vulnerabilities, or other critical issues, or alternatively, specific problems are discovered in a vendor's product (or class of products) after it has been listed on the APL, the affected vendor(s) will be notified that the identified product(s) must be improved as necessary in order to remain on the APL. A remediation grace period will be granted commensurate with the severity level of the problem.

4.5.2 APL Listing Requirements

Table 1 defines the APL listing requirements based on classification of the test case and its severity level. The program will not list a product that has a Severity 1 test case that failed (shown RED). ***Table 2*** specifies the remediation timeframes for each severity level. Products not corrected within the given timeframe will be moved to the Removed Products List (RPL).

Table 1 - APL listing based on Test Level and Classification

Test Level / Classification	*Severity 1*	*Listed on APL*	*Severity 2*	*Listed on APL*[2]	*Severity 3*	*Listed on APL*
Security Required	Pass	✓	Pass	✓	Pass	✓
	Uses APL approved product	✓	Uses APL approved product	✓	Uses APL approved product	✓
	Fail	✗	Fail	✗	Fail	✓
Security Optional: Supported by Product	Pass	✓	Pass	✓	Pass	✓
	Uses APL approved product	✓	Uses APL approved product	✓	Uses APL approved product	✓
	Fail	✗	Fail	✓	Fail	✓
Security Optional: Not Supported	Not Supported	✓	Not Supported	✓	Not Supported	✓
Usability Required	Pass	✓	Pass	✓	Pass	✓
	Uses APL approved product	✓	Uses APL approved product	✓	Uses APL approved product	✓
	Fail	✗	Fail	✓	Fail	✓
Usability Optional: Supported by Product	Pass	✓	Pass	✓	Pass	✓
	Uses APL approved product	✓	Uses APL approved product	✓	Uses APL approved product	✓
	Fail	✗	Fail	✓	Fail	✓
Usability Optional: Not Supported	Not Supported	✓	Not Supported	✓	Not Supported	✓

Table 2 - Severity Remediation Timeframes

Severity Level	*Severity Description*	*Remediation Timeframe*
1	The identified problem results in a High impact to any of security, PACS operations, PACS availability, or other area examined.	30 days
2	The identified problem results in a Moderate impact to any of security, PACS	90 days

[2] No new solution that fails a test case labeled Security/Required Severity Level 2 (SR-2) will be listed on the APL. Existing solutions that initially passed a SR-2 test case, but in subsequent revisions fail a SR-2 test case, are subject to remediation within 90 days as specified in ***Table 2*** below.

Severity Level	*Severity Description*	*Remediation Timeframe*
	operations, PACS availability, or other area examined.	
3	The identified problem results in a Low impact to any of security, PACS operations, PACS availability, or other area examined.	1 year

4.5.3 Classification Codes and Scoring Guidelines

The Topology Mapping form includes a classification code for each test case. The classification code is shorthand that indicates the test type for the requirement is *Security* or *Usability* and whether the requirement is mandatory (*Required*) or *Optional*.

Table 3 - Classification Codes

Classification Code	*Security/Usability*
S[RO]-[123]	**Security** - A control directly impacting security of the system.
U[RO]-[123]	**Usability** - A control impacting end user system usability. Does not directly impact security.
[SU]R-[123]	**Required** - Must be present. Must work correctly: Red/Green.
[SU]O-[123]	**Optional** - May be present. If present, it must work correctly: Red/Green. Not Supported: Yellow.
Example: SR-2	**Security, Required, Severity Level 2**
Example: UO-3	**Usability, Optional, Severity Level 3**

5. Topology Mapping

Mapping is the process of taking the functional requirements defined in [FRTC] and allocating them into the FIPS 201 Evaluation Program categories, and then indicating the specific named components within your solution that perform the operations for that requirement. For example, if the requirement is for a product to validate signatures as defined in [FRTC] §2.1-Test 2.1.1, the Applicant should follow the example given in below.

Table 4 - Example Mapping Table for Time of Individual Registration Signature Verification

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Category(ies)	Components	Process
		2.0			**Requirements at Time of In-Person Registration in Accordance With [E-PACS] PIA-9**	All tests use PKI-AUTH unless specifically noted.	Note all requirements sourced from [E-PACS] unless otherwise noted.			`
		2.01			Signature Verification					
1.2.0	SR-1	2.01.01	01	00	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV credential	Registration succeeds.	PIA-2 thru PIA-7	Validation System (13.01), PACS Infrastructure (13.01)	Registration Workstation, PACS application, Path Discovery and Validation engine	EE certificate signature is validated immediately by the Validation System. The CA certificate signatures are evaluated, but may be cached by the path discovery and validation engine if they have

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Category(ies)	Components	Process
										been previously seen.

In the example provided in , the signature verification involves several elements. It is allocated to the PACS Infrastructure and Validation System, as both solutions require information from the credential. The PACS Infrastructure provides the registration workstation. The Validation System is doing the PKI signature verification for the end entity, and the Validation System's PDVAL engine is evaluating signatures and caching status for the CA certificate path. Clearly there are many potential combinations of components within categories that could perform this function and it is up to the applicant to describe the process of how, when, and where [FRTC] requirements are met.

5.1 Topology Mapping Workbook

The PACS FRTC 1.3.3 Topology Mapping Workbook contains a listing of requirements used with the 13.02 topology. Beginning with FRTC 1.3.3, we provide this artifact in the form of a Microsoft Excel workbook which allows you to hide columns as needed and maneuver more easily. You will find the Topology Mapping Workbook included in the evaluation application. Use it to provide the Lab with the PACS 13.02 topology mapping of functional requirements identified in the [FRTC] to the FIPS 201 Evaluation Program categories as defined in this document. The columns for Category(ies), Components and Process are intentionally left blank in this table. These three columns must be completed by the Applicant when submitting a component/solution to the FIPS 201 Evaluation Program for evaluation, testing, and approval.