GSA U.S. General Services Administration

Validation System Approval Procedure

VERSION 0.1.0

DRAFT

FIPS 201 EVALUATION PROGRAM

January 23, 2013

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	1/3/2013	Document creation	Limited
Draft	0.0.2	1/4/2012	First team edit	Limited
Draft	0.0.3	1/4/2012	Second team edit	Limited
Draft	0.0.4	1/11/13	Edit based on full team review	Limited
Draft	0.0.5	1/13/13	Initial basic QA	Limited
Draft	0.0.6	1/17/13	QA fixes	Limited
Draft	0.0.7	1/20/13	QA	Limited
Draft	0.0.8	1/21/13	Added cryptographic requirements	Limited
Draft	0.1.0	1/23/13	Team review	EPTWG

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Overview

The Federal Information Processing Standard (FIPS) 201 Evaluation Program (EP) is a U.S. Government entity administered by the Office of Government-wide Policy (OGP), within the General Services Administration (GSA) agency. The goal of the FIPS 201 EP is to evaluate products and services against the requirements outlined in FIPS 201 and its supporting documents. The FIPS 201 EP is also charged with evaluation of products and services according to requirements from the Federal Identity, Credentialing and Access Management (FICAM) Program. The FICAM Testing Program encompasses both sets of requirements. The goal of the FICAM Testing Program is to provide the best known information on the conformance to standards, interoperability, and security of products and services for implementation of FICAM-conformant systems and services throughout the federal government. A set of approval and test procedures have been developed that outline the evaluation criteria (requirements), approval mechanisms, and test processes employed by Industry and ICAM Labs during their evaluation of a Supplier's product or service against the requirements for that category.

A Supplier submitting a Validation System (hereafter referred to as "Product") for evaluation must follow the *Suppliers Policies and Procedures Handbook*. In addition to that handbook, Suppliers also must refer to this Approval Procedure document, which provides the necessary category-specific details in order to have a Supplier's Product evaluated by the FIPS 201 EP and placed on the FICAM Testing Program Approved Products List (APL).

1.2 Category Description

A Validation System is comprised of software and hardware that validates a credential, its certificates, and the bearer of the credential. A Validation System is used in two strategic areas:

1. Before allowing the credential to be registered into the Physical Access Control System (PACS); and
2. Before sending the credential number to a PACS Head-End (through a field panel) for an access decision.

In both cases, the core functionality of the Validation System is to ensure that a given authentication mode's requirements are met when verifying the credential and the bearer of that credential. *FICAM PIV in Enterprise PACS Guidance Draft version 2.0.2* (*PIV in E-PACS*) controls PIA-3 and PIA-3.x provide additional detail for the requirements of authenticating the credential and the bearer.

A validation system interfaces with the following components:

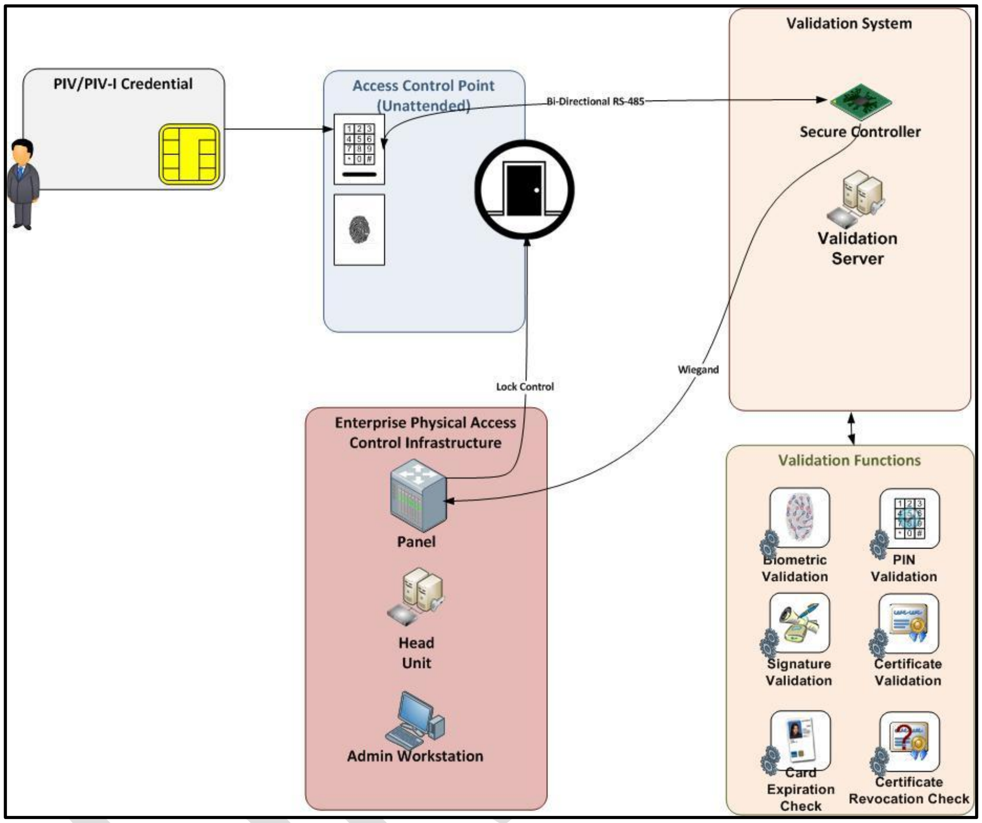
1. A Registration Station (sometimes integrated with the Head-End). The basic requirements are defined in *PIV in E-PACS* controls PIA-3, PIA-3.x, PIA-8, PIA-9. Registration Stations often leverage an Accepting Device as listed on the APL under the following component categories:
    - Transparent USB Card Reader

- Integrated Card Reader/Writer and Single Fingerprint Capture Device

2. An Accepting Device that is installed at a door/gate/portal for use in time-of-access decisions. The Accepting Device is listed on the APL under the following categories:
    - Transparent Reader;
    - Transitional Transparent Reader; and
    - FICAM Transparent Reader.
3. A Secure Controller (may be a hardware device or part of the validation service software) that is listed as a component of the Validation Service. The Secure Controller component provides the linkage between the Accepting Device, the Validation Service, and the PACS Field Panel. This functionality may be fully integrated within the PACS Field Panel.
4. A Validation Service (may be a proprietary validation service; it may depend on a PKI Validation Engine component such as an SCVP server). The Validation Service often provides multiple capabilities, including credential/bearer validation at time of registration and at time of access, as well as periodic certificate validation in a back-end process for the PACS Head-End.
5. A PACS Head-End system is the actual PACS software used in conjunction with a backend database that stores the access control infrastructure information, card holder information, schedules, shifts, access alarm management, and communicates with the access control field hardware.

Figure 1 shows the basic architecture for the “at time of access” scenario. The diagram shows the linkage between the Accepting Device, Secure Controller, Validation Service, and PACS Head-End. There are many ways to implement these capabilities. This is one way that a system developer may deliver the capabilities required.

Figure 1 - Representative architecture for a Validation System



1.3 Purpose

The purpose of this document is to provide the following information:

- Provide a list of the artifacts and/or documentation that needs to be submitted to the ICAM Test Lab as part of the application package submission.
- Document the list of the requirements that apply to this category.
- Specify the evaluation criteria along with their approval mechanisms that will be used by the ICAM Test Lab to verify compliance of the Product against the requirements that apply to this category.

2 Application Package Content

Application Package Content include the artifacts, documentation, and the Product itself that needs to be submitted to the Evaluation Lab so that evaluation can be performed. The Application Package Contents for this category include the following:

1. The Product itself. Will be delivered to the ICAM Test Lab (address can be found at http://fips201ep.cio.gov/labs.php) using a secure delivery method that requires acknowledgement of receipt (e.g., FedEx, UPS, hand delivery). The Supplier shall provide installation and configuration support as appropriate.
2. Completed Application Form, provided on the FIPS 201 EP website. (This form will be available through the web interface once users have been assigned a login credential.)
3. Completed and signed Lab Service Agreement (found in the application submission package ZIP file). The Lab Service Agreement should be completed and scanned into a document to be uploaded to the FIPS 201 EP website.
4. Completed and signed Attestation Form (found in the application submission package ZIP file). The Attestation Form should be completed and scanned into a document to be uploaded to the FIPS 201 EP website.
5. All necessary Supplier documentation providing proof that the Product complies with the requirements (as outlined in Section 3.1). Examples of specific documentation includes user guides, technical specifications, and white papers.

3 Evaluation Procedure for a Validation System (VS)

3.1 Requirements

The Validation System must be tested as a component within a full system using an end-to-end testing methodology. Table 1 - Validation System Requirements is derived from the *FICAM PACS Master Test Procedures* document. It provides the requirements that must be met for the Validation System. Under the "Required Components" column are labels that detail which requirements are specific to the Head-End ("H"), the Validation System ("V"), or the Reader ("R"). These clarify the linkages between the components under test.

Tables 3-7 present a summarized form of the requirements for cryptographic algorithms and key sizes. These are the source of the requirements for support required within the Validation System

Table 1 - Validation System Requirements

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
Time of Registration					
R-VS-1	H,V	Verify Product's ability to validate signatures in the certificates found in the certification path for a PIV credential.	*PIV in E-PACS*	PIA-2 – PIA-7 and PIA-9	ICAM Test Lab
R-VS-2	H,V	Verify Product's ability to validate signatures in the certificates found in the certification path for a PIV-I credential.	*PIV in E-PACS*	PIA-2 – PIA-7 and PIA-9	ICAM Test Lab
R-VS-3	V	Verify Product's ability to recognize invalid signature on an intermediate CA in the certification path.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-4, PIA-5, PIA-9	ICAM Test Lab
R-VS-4	V	Verify Product's ability to recognize invalid signature on the End Entity certificate.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-4, PIA-9	ICAM Test Lab
R-VS-5	V	Verify Product's ability to reject a credential when notBefore date of the intermediate CA certificate is sometime in the future.	*PIV in E-PACS*	PIA-3.4, PIA-5, PIA-9	ICAM Test Lab
R-VS-6	V	Verify Product's ability to reject a credential when notBefore date of the End Entity certificate is sometime in the future.	*PIV in E-PACS*	PIA-3.5, PIA-9	ICAM Test Lab
R-VS-7	V	Verify Product's ability to reject a credential when notAfter date of the intermediate certificate is sometime in the past.	*PIV in E-PACS*	PIA-3.5, PIA-9	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-8	V	Verify Product's ability to reject a credential when notAfter date of the End Entity certificate is sometime in the past.	*PIV in E-PACS*	PIA-3.5, PIA-9	ICAM Test Lab
R-VS-9	V	Verify Product's ability to reject a credential when common name portion of the of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-9	ICAM Test Lab
R-VS-10	V	Verify Product's ability to reject a credential when common name portion of the of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-9	ICAM Test Lab
R-VS-11	V	Verify Product's ability to recognize when the intermediate CA certificate is missing basicConstraints extension.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-9	ICAM Test Lab
R-VS-12	V	Verify Product's ability to recognize when the basicConstraints extension is present and critical in the intermediate CA certificate but the CA component is false.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-9	ICAM Test Lab
R-VS-13	V	Verify Product's ability to recognize when the basicConstraints extension is present and not critical in the intermediate CA certificate but the CA component is false.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-9	ICAM Test Lab
R-VS-14	V	Verify Product's ability to recognize when the first certificate in the path includes basicConstraints extension with a pathLenConstraint of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-9	ICAM Test Lab
R-VS-15	V	Verify Product's ability to recognize when the intermediate certificate includes a critical keyUsage extension in which keyCertSign is false.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-9	ICAM Test Lab
R-VS-16	V	Verify Product's ability to recognize when the intermediate certificate includes a non-critical keyUsage extension.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-9	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-17	V	Verify Product's ability to recognize when the intermediate certificate includes a critical keyUsage extension in which cRLSign is false.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-9	ICAM Test Lab
R-VS-18	V	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy will be set to PIV Hardware.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-9	ICAM Test Lab
R-VS-19	V	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate path. The explicit policy will be set to an arbitrary value that is not present in the certificate path (ex., OID value 1.2.3.4).	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-9	ICAM Test Lab
R-VS-20	V	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the Commercial Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate in a bridged trust environment. The explicit policy will be set to Medium Hardware.Test Condition: production PIV passes.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-9	ICAM Test Lab
R-VS-21	V	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the Commercial Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate in a bridged trust environment. The explicit policy will be set to an arbitrary value that is not present in the certificate chain (ex., OID value 1.2.3.4).	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-9	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-22	V	With Common Policy anchor, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate - however, is present somewhere in the certificate path. The explicit policy will be set to a value that is present in the certificate path, but does not map to the end entity certificate (ex, High Hardware).	*PIV in E-PACS*	PIA-3.2, PIA-5, PIA-9	ICAM Test Lab
R-VS-23	V	The first intermediate certificate asserts NIST-test-policy-1 and includes a policyConstraints extension with inhibitPolicyMapping set to 0. The second intermediate certificate asserts Policy A and maps Policy A to Policy B. The end entity certificate asserts Policy A and Policy B	*PIV in E-PACS*	PIA-3.2, PIA-5, PIA-9	ICAM Test Lab
R-VS-24	V	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.	*PIV in E-PACS*	PIA-3.2, PIA-5, PIA-9	ICAM Test Lab
R-VS-25	V	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.	*PIV in E-PACS*	PIA-3.2, PIA-5, PIA-9	ICAM Test Lab
R-VS-26	V	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and subjectAltName with a DN that falls outside that subtree.	*PIV in E-PACS*	PIA-3.5, PIA-5, PIA-7, PIA-9	ICAM Test Lab
R-VS-27	V	The system recognizes when no revocation information is available for the End Entity certificate.	*PIV in E-PACS*	PIA-3.5, PIA-5, PIA-7, PIA-9	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-28	V	The system recognizes when a second intermediate CA certificate is revoked.	*PIV in E-PACS*	PIA-3.5, PIA-5, PIA-7, PIA-9	ICAM Test Lab
R-VS-29	V	The system recognizes when the End Entity certificate is revoked.	*PIV in E-PACS*	PIA-3.5, PIA-5, PIA-7, PIA-9	ICAM Test Lab
R-VS-30	V	The system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the certificate.	*PIV in E-PACS*	PIA-3.5, PIA-5, PIA-7, PIA-9	ICAM Test Lab
R-VS-31	V	The system recognizes when a certificate in the path points to a CRL with an expired nextUpdate value.	*PIV in E-PACS*	PIA-3.5, PIA-5, PIA-7, PIA-9	ICAM Test Lab
R-VS-32	V	The system recognizes when a certificate in the path points to a CRL with a notBefore Date in the future.	*PIV in E-PACS*	PIA-3.5, PIA-5, PIA-7, PIA-9	ICAM Test Lab
R-VS-33	V	The system recognizes when a certificate in the path has an incorrect distribution point.	*PIV in E-PACS*	PIA-3.2, PIA-4, PIA-9	ICAM Test Lab
R-VS-34	V	The system recognizes when the CHUID signature is invalid and does not verify.	*PIV in E-PACS*	PIA-3.6, PIA-5, PIA-9	ICAM Test Lab
R-VS-35	V	The system recognizes when the CHUID signer certificate is expired.	*PIV in E-PACS*	PIA-3.6, PIA-9	ICAM Test Lab
R-VS-36	V	The system recognizes when the CHUID is expired.	*PIV in E-PACS*	PIA-3.2, PIA-9	ICAM Test Lab
R-VS-37	V	The system recognizes when the FASC-N in the CHUID does not equal the FASC-N in the PIV Auth Cert.	*PIV in E-PACS*	PIA-3.2, PIA-9	ICAM Test Lab
R-VS-38	V	The system recognizes when the UUID in the CHUID does not equal the UUID in the PIV Auth Cert.	*PIV in E-PACS*	PIA-3.2, PIA-4, PIA-9	ICAM Test Lab
R-VS-39	V	The system recognizes when the Facial Image signature is invalid and does not verify.	*PIV in E-PACS*	PIA-3.2, PIA-4, PIA-9	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-40	V	The system recognizes when the Fingerprint signature is invalid and does not verify.	*PIV in E-PACS*	PIA-3 – PIA-7 and PIA-9	ICAM Test Lab
R-VS-41	V	The system recognizes when the Security Object signature is invalid and does not verify.	*PIV in E-PACS*	PIA-3 – PIA-7 and PIA-9	ICAM Test Lab
R-VS-42	V	The system successfully validates a good credential using an OCSP response with a good signature.	*PIV in E-PACS*	PIA-3.2, PIA-4, PIA-9	ICAM Test Lab
R-VS-43	V	Validation fails using an OCSP response with an expired signature for a good card.	*PIV in E-PACS*	PIA-3 – PIA-7 and PIA-9	ICAM Test Lab
R-VS-44	V	Validation succeeds using an OCSP response with a revoked signature for a good card with PKIX_OCSP_NOCHECK present.	*PIV in E-PACS*	PIA-3.2, PIA-3.5, PIA-5, PIA-9	ICAM Test Lab
R-VS-45	V	Validation fails using an OCSP response with a revoked signature for a good card without PKIX_OCSP_NOCHECK present.	*PIV in E-PACS*	PIA-3.2, PIA-3.6, PIA-5, PIA-9	ICAM Test Lab
R-VS-46	V	Validation fails using an OCSP response with a malformed signature for a good card.	*PIV in E-PACS*	PIA-3.2, PIA-4, PIA-5, PIA-9	ICAM Test Lab
R-VS-47	V	Verify Product's ability to recognize invalid signature on an intermediate CA in the certification path.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-4, PIA-5	ICAM Test Lab
R-VS-48	V	Verify Product's ability to recognize invalid signature on the End Entity certificate.	*PIV in E-PACS*	PIA-3.2, PIA-3.4, PIA-4, PIA-5	ICAM Test Lab
R-VS-49	V	Verify Product's ability to reject a credential when notBefore date of the intermediate CA certificate is sometime in the future.	*PIV in E-PACS*	PIA-3.6, PIA-5	ICAM Test Lab
R-VS-50	V	Verify Product's ability to reject a credential when notBefore date of the End Entity certificate is sometime in the future.	*PIV in E-PACS*	PIA-3.6	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-51	V	Verify Product's ability to reject a credential when notAfter date of the intermediate certificate is sometime in the past.	*PIV in E-PACS*	PIA-3.6, PIA-5	ICAM Test Lab
R-VS-52	V	Verify Product's ability to reject a credential when notAfter date of the End Entity certificate is sometime in the past.	*PIV in E-PACS*	PIA-3.6	ICAM Test Lab
R-VS-53	V	Verify Product's ability to reject a credential when common name portion of the of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate.	*PIV in E-PACS*	PIA-3.2, PIA-3.3, PIA-5	ICAM Test Lab
R-VS-54	V	Verify Product's ability to recognize when the intermediate CA certificate is missing basicConstraints extension.	*PIV in E-PACS*	PIA-3.2, PIA-3.3, PIA-5	ICAM Test Lab
R-VS-55	V	Verify Product's ability to recognize when the basicConstraints extension is present and critical in the intermediate CA certificate but the CA component is false	*PIV in E-PACS*	PIA-3.2, PIA-3.3, PIA-5	ICAM Test Lab
R-VS-56	V	Verify Product's ability to recognize when the basicConstraints extension is present and not critical in the intermediate CA certificate but the CA component is false.	*PIV in E-PACS*	PIA-3.2, PIA-3.3, PIA-5	ICAM Test Lab
R-VS-57	V	Verify Product's ability to recognize when the first certificate in the path includes basicConstraints extension with a pathLenConstraint of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate.	*PIV in E-PACS*	PIA-3.2, PIA-3.3, PIA-5	ICAM Test Lab
R-VS-58	V	Verify Product's ability to recognize when the intermediate certificate includes a critical keyUsage extension in which keyCertSign is false.	*PIV in E-PACS*	PIA-3.1, PIA-4, PIA-5	ICAM Test Lab
R-VS-59	V	Verify Product's ability to recognize when the intermediate certificate includes a non-critical keyUsage extension.	*PIV in E-PACS*	PIA-3.1, PIA-4, PIA-5	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-60	V	Verify Product's ability to recognize when the intermediate certificate includes a critical keyUsage extension in which cRLSign is false.	*PIV in E-PACS*	PIA-3.1, PIA-4, PIA-5	ICAM Test Lab
R-VS-61	V	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy will be set to PIV Hardware.	*PIV in E-PACS*	PIA-5, PIA-6	ICAM Test Lab
R-VS-62	V	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate path. The explicit policy will be set to an arbitrary value that is not present in the certificate path (ex., OID value 1.2.3.4).	*PIV in E-PACS*	PIA-5, PIA-6	ICAM Test Lab
R-VS-63	V	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the Commercial Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate in a bridged trust environment. The explicit policy will be set to Medium Hardware.Test Condition: production PIV passes.	*PIV in E-PACS*	PIA-5, PIA-6	ICAM Test Lab
R-VS-64	V	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the Commercial Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate in a bridged trust environment. The explicit policy will be set to an arbitrary value that is not present in the certificate chain (ex., OID value 1.2.3.4).	*PIV in E-PACS*	PIA-5, PIA-6	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-65	V	With Common Policy anchor, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate - however, is present somewhere in the certificate path. The explicit policy will be set to a value that is present in the certificate path, but does not map to the end entity certificate (ex, High Hardware).	*PIV in E-PACS*	PIA-5, PIA-6	ICAM Test Lab
R-VS-66	V	The first intermediate certificate asserts NIST-test-policy-1 and includes a policyConstraints extension with inhibitPolicyMapping set to 0. The second intermediate certificate asserts Policy A and maps Policy A to Policy B. The end entity certificate asserts Policy A and Policy B.	*PIV in E-PACS*	PIA-5	ICAM Test Lab
R-VS-67	V	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.	*PIV in E-PACS*	PIA-3.5, PIA-5, PIA-7	ICAM Test Lab
R-VS-68	V	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.	*PIV in E-PACS*	PIA-3.5, PIA-5, PIA-7	ICAM Test Lab
R-VS-69	V	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and subjectAltName with a DN that falls outside that subtree.	*PIV in E-PACS*	PIA-3.5, PIA-5, PIA-7	ICAM Test Lab
R-VS-70	V	The system recognizes when no revocation information is available for the End Entiry certificate.	*PIV in E-PACS*	PIA-3.5, PIA-5, PIA-7	ICAM Test Lab
R-VS-71	V	The system recognizes when a second intermediate CA certificate is revoked.	*PIV in E-PACS*	PIA-3.5, PIA-5, PIA-7	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-72	V	The system recognizes when the End Entity certificate is revoked.	*PIV in E-PACS*	PIA-3.5, PIA-7	ICAM Test Lab
R-VS-73	V	The system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the certificate	*PIV in E-PACS*	PIA-3.2, PIA-3.5, PIA-5, PIA-7	ICAM Test Lab
R-VS-74	V	The system recognizes when a certificate in the path has an expired nextUpdate value.	*PIV in E-PACS*	PIA-3.5, PIA-3.6, PIA-5, PIA-7	ICAM Test Lab
R-VS-75	V	The system recognizes when a certificate in the path points to a CRL with a notBefore Date in the future.	*PIV in E-PACS*	PIA-3.5, PIA-3.6, PIA-5, PIA-7	ICAM Test Lab
R-VS-76	V	The system recognizes when a certificate in the path has an incorrect distribution point.	*PIV in E-PACS*	PIA-3.2, PIA-3.5, PIA-5, PIA-7	ICAM Test Lab
R-VS-77	V	The system recognizes when the CHUID signature is invalid and does not verify.	*PIV in E-PACS*	PIA-3.2	ICAM Test Lab
R-VS-78	V	The system recognizes when the CHUID signer certificate is expired.	*PIV in E-PACS*	PIA-3.6	ICAM Test Lab
R-VS-79	V	The system recognizes when the CHUID is expired.	*PIV in E-PACS*	PIA-3.6	ICAM Test Lab
R-VS-80	V	The system recognizes when the FASC-N in the CHUID does not equal the FASC-N in the PIV Auth Cert.	*PIV in E-PACS*	PIA-3.6	ICAM Test Lab
R-VS-81	V	The system recognizes when the UUID in the CHUID does not equal the UUID in the PIV Auth Cert.	*PIV in E-PACS*	PIA-3.6	ICAM Test Lab
R-VS-82	V	The system recognizes when the Facial Image signature is invalid and does not verify.	*PIV in E-PACS*	PIA-3, PIA-3.2, PIA-3.3, PIA-4	ICAM Test Lab
R-VS-83	V	The system recognizes when the Fingerprint signature is invalid and does not verify.	*PIV in E-PACS*	PIA-3, PIA-3.2, PIA-3.3, PIA-4	ICAM Test Lab
R-VS-84	V	The system recognizes when the Security Object signature is invalid and does not verify.	*PIV in E-PACS*	PIA-3.2, PIA-4	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-85	V	The system successfully validates a good credential using an OCSP response with a good signature.	*PIV in E-PACS*	PIA-3.5, PIA-3.6, PIA-4, PIA-7	ICAM Test Lab
R-VS-86	V	Validation fails using an OCSP response with an expired signature for a good card.	*PIV in E-PACS*	PIA-3.5, PIA-3.6, PIA-4, PIA-7	ICAM Test Lab
R-VS-87	V	Validation succeeds using an OCSP response with a revoked signature for a good card with PKIX_OCSP_NOCHECK present.	*PIV in E-PACS*	PIA-3.5, PIA-3.6, PIA-4, PIA-7	ICAM Test Lab
R-VS-88	V	Validation fails using an OCSP response with a revoked signature for a good card without PKIX_OCSP_NOCHECK present.	*PIV in E-PACS*	PIA-3.5, PIA-3.6, PIA-4, PIA-7	ICAM Test Lab
R-VS-89	V	Validation fails using an OCSP response with an malformed signature for a good card.	*PIV in E-PACS*	PIA-3.5, PIA-3.6, PIA-4, PIA-7	ICAM Test Lab
R-VS-90	V	- Shall be able to define: Challenge and verification program for each population. - Shall be able to define: Authentication approach for each population and each zone/point of access in accord with NIST SP 800-116.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3, PIA-2	ICAM Test Lab
R-VS-91	V	No credential shall be registered for which there is no valid trust path per the relying party PKI policy.	*PIV in E-PACS*	PIA-5, PIA-8, PIA-9	ICAM Test Lab
R-VS-92	V	Shall provide the means to select which x.509 constraints are evaluated such as policy constraints, name constraints and key usage. This configuration will reflect the customer's PKI relying party policy.	*PIV in E-PACS*	PIA-5, PIA-6	ICAM Test Lab
R-VS-93	V	The Product shall provide auditing/logging of Card activity (e.g., 3 days of card activity).	*PIV in E-PACS*	PAU-1, PAU-2, PAU-3, PAU-4	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-94	V	The Product shall provide auditing/logging of individual and group reporting of alarms (e.g., door force, door prop).	*PIV in E-PACS*	PAU-3	ICAM Test Lab
R-VS-95	H,V	With fingerprint checking enabled, a good credential is presented to the system with a valid fingerprint.	*PIV in E-PACS*	PIA-3 – PIA-7 and PIA-9	ICAM Test Lab
R-VS-96	H,V	With fingerprint checking enabled, a good credential is presented to the system with an invalid fingerprint.	*PIV in E-PACS*	PIA-3 – PIA-7 and PIA-9	ICAM Test Lab
R-VS-97	H,V	Various valid PIV and PIV-I cards work in the system (PKI-AUTH).	*PIV in E-PACS*	PIA-2 – PIA-7 and PIA-9	ICAM Test Lab
Time of Access					
R-VS-98	H,V,R	Verify products ability to validate signatures in the certificates found in the certification path for a PIV credential.	*PIV in E-PACS*	PIA-2 – PIA-7 and PIA-9	ICAM Test Lab
R-VS-99	H,V,R	Verify products ability to validate signatures in the certificates found in the certification path for a PIV-I credential.	*PIV in E-PACS*	PIA-2 – PIA-7 and PIA-9	ICAM Test Lab
R-VS-100	H,V,R	With fingerprint checking enabled, a good credential is presented to the system with a valid fingerprint.	*PIV in E-PACS*	PIA-3, PIA-3.2, PIA-3.3, PIA-4	ICAM Test Lab
R-VS-101	H,V,R	With fingerprint checking enabled, a good credential is presented to the system with an invalid fingerprint.	*PIV in E-PACS*	PIA-3, PIA-3.2, PIA-3.3, PIA-4	ICAM Test Lab
R-VS-102	H,V,R	Various valid PIV and PIV-I cards work in the system (PKI-AUTH).	*PIV in E-PACS*	PIA-2 – PIA-7	ICAM Test Lab
R-VS-103	H,V,R	The network connection is dropped to all boards within a panel.	*PIV in E-PACS*	PCP-1.5, PCP-1.7	ICAM Test Lab
R-VS-104	H,V,R	The network connection is dropped from the server(s).	*PIV in E-PACS*	PCP-1.5, PCP-1.7	ICAM Test Lab
R-VS-105	H,V,R	The services have stopped on the server.	*PIV in E-PACS*	PCI-1.5, PCP-1.7, PCP-1.6	ICAM Test Lab
R-VS-106	H,V,R	A/C Power loss to panel.	*PIV in E-PACS*	PPE-1	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-107	H,V,R	...all security relevant processing shall be performed on the secure side of the door. No security relevant decisions shall be made by system components that do not belong to the cardholder's credential when they are on the attack side of the door.	*PIV in E-PACS*	PPE-1	ICAM Test Lab
R-VS-108	H,V,R	- Shall support, at a minimum, three specific groups: guests, visitors and regular access. - Shall be able to define: User populations: Guests, Visitors, Regular Access.	*PIV in E-PACS*	PPE-1	ICAM Test Lab
R-VS-109	H,V	- The system shall allow for integrated provisioning once a positive determination of a credential's suitability has been made for all credentials. - Shall provide access grant functionality to evaluate credentials to determine binding with the bearer.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-VS-110	H,V	Shall provide access grant functionality to evaluate credentials to determine binding with the bearer.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-VS-111	H,V,R	Shall provide the means to select which biometrics are used to link bearer to credential.	*PIV in E-PACS*	PIA-3.3	ICAM Test Lab
R-VS-112	H,V	Workflow shall include sponsor approval and security administrator approval; No credential shall be granted authorization privileges to a Trusted PACS without approval.	*PIV in E-PACS*	PIA-3.3	ICAM Test Lab
R-VS-113	H,V	Shall support: signed CHUID.	*PIV in E-PACS*	PCM-1, PCM-2	ICAM Test Lab
R-VS-114	H,V,R	Shall support: Card Authentication Key.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-VS-115	H,V,R	Shall support: PIV Authentication Key + PIN.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-VS-116	H,V,R	Shall support: PIV Authentication Key + PIN + BIO.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-VS-117	H,V,R	Shall support: Card Authentication Key + PIN + BIO.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-118	H,V,R	Where multiple authentication modes are supported, readers shall support bi-directional communications with the system.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-VS-119	H,V,R	For multi-factor readers, applicant's system must allow modification of an individual reader or groups of readers' authentication mode from the server or a client/workstation to the server.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-VS-120	H,V,R	For multi-factor readers, the site administrator arbitrarily decides that all readers or a subset of readers must require either more or fewer authentication factors than the readers are presently configured for.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-VS-121	H,V,R	For multi-factor readers, based on temporal access rules the administrator set, the system should support dynamic assignment of individuals (or groups of individuals) and resources (doors) on a time based schedule.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-VS-122	H,V,R	For multi-factor readers, based on FPCON, MARCON or other similar structured emergency response protocol for which the vendor claims support, in no case shall there be a requirement for an administrator's physical presence at a reader be considered compliant.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-VS-123	H,V,R	For multi-factor readers, if a time delay of longer than 120 seconds is required for a reader to change modes; this too shall be considered non-compliant.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-VS-124	H,V	Granularity of auditing records shall be to the card and individual transaction. These shall be easily verifiable through a reporting tool or any other log and audit viewing capability.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-VS-125	H,V	The product shall provide auditing/logging of all PKI processing to include: - Nonce generation - Challenges - Responses - PDVAL - Revocation status	*PIV in E-PACS*	PAU-1, PAU-2, PAU-3, PAU-4	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-126	H,V	The Product shall provide auditing/logging of all software-driven configuration changes.	*PIV in E-PACS*	PAU-1, PAU-2, PAU-3, PAU-4	ICAM Test Lab
R-VS-127	H,V	The Product shall provide auditing/logging of periodic certificate PDVAL and status checking.	*PIV in E-PACS*	PAU-5, PAU-6, PAU-7	ICAM Test Lab
R-VS-128	H,V	The Product shall provide auditing/logging of a card's whereabouts in system.	*PIV in E-PACS*	PAU-4, PAU-5, PAU-6, PAU-7	ICAM Test Lab
R-VS-129	H,V	The Product shall provide auditing/logging of a card's whereabouts in system.	*PIV in E-PACS*	PAU-1, PAU-2, PAU-3	ICAM Test Lab
R-VS-130	H,V	The Product shall provide auditing/logging of PKI policies for name constraints, path constraints, validity checks.	*PIV in E-PACS*	PAU-4, PAU-5, PAU-6, PAU-7	ICAM Test Lab
R-VS-131	H,V	The Product shall provide auditing/logging of what date individuals were provisioned or de-provisioned and by whom.	*PIV in E-PACS*	PAU-4	ICAM Test Lab
R-VS-132	H,V	The Product shall provide auditing/logging of all readers and their modes.	*PIV in E-PACS*	PAU-5, PAU-6	ICAM Test Lab
R-VS-133	H,V	The Product shall provide auditing/logging of configuration download status to system components.	*PIV in E-PACS*	PAU-5, PAU-6	ICAM Test Lab
R-VS-134	H,V	Each component in the system shall have, at a minimum, a UL 249 listing.	*PIV in E-PACS*	PCA-1, PCA-2	ICAM Test Lab
R-VS-135	H,V	Each component in the system shall have APL status, as applicable.	*PIV in E-PACS*	PCA-3	ICAM Test Lab
R-VS-136	H,V,R	Each component in the system shall have FIPS 140-2 certification, as applicable.	*PIV in E-PACS*	PCA-4	ICAM Test Lab
R-VS-137	H,V,R	Biometric identifiers shall be encrypted at rest and in transmission throughout the system.	*PIV in E-PACS*	PSC-1	ICAM Test Lab
R-VS-138	H,V,R	The system shall have the ability to manage the system through software controlled configuration management methods. Initial configuration of hardware settings (e.g., DIP switches) is allowed at installation only and not for management of the hardware tree.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-139	H,V,R	Each physical component shall be separately defined and addressable within the server user interface.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-VS-140	H,V,R	The system shall support configuration downloads to each component.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-VS-141	H,V	At time of registration, the Validation System shall support the credential number transform rules defined in Table 2 for registration into the Head-End record	FICAM Testing Program		ICAM Test Lab
R-VS-142	H,V,R	At time of access, the Validation System shall support the credential number transform rules defined in Table 2.	FICAM Testing Program		ICAM Test Lab
R-VS-143	V	The system shall support RSA PKCS#1 v1.5 (1024, 2048, or 3072)	*NIST SP 800-78-3 Table 3-1; NIST SP 800-78-3 Table 3-3; FPKI CP v1.17 Section 6.1.5*		ICAM Test Lab
R-VS-144	V	The system shall support RSASSA - PSS (1024, 2048, or 3072)	*NIST SP 800-78-3 table 3-1; NIST SP 800-78-3 Table 3-3; FPKI CP v1.17 Section 6.1.5*		ICAM Test Lab
R-VS-145	V	The system shall support RSA key transport (2048)	*NIST SP 800-78-3 Table 3-1*		ICAM Test Lab
R-VS-146	V	The system shall support RSA key transport (1024, 3072)	*Derived from NIST SP 800-78-3 Table 3-1 and FPKI CP v1.17 Section 6.1.5*		ICAM Test Lab
R-VS-147	V	The system shall support ECDSA (P-256 or P-384)	*NIST SP 800-78-3 Table 3-1; NIST SP 800-78-3 Table 3-3; FPKI CP v1.17 Section 6.1.5*		ICAM Test Lab
R-VS-148	V	The system shall support ECDH (P-256 or P-384)	*NIST SP 800-78-3 Table 3-1; FPKI CP v1.17 Section 6.1.5*		ICAM Test Lab
R-VS-149	V	The system shall support SHA-1, SHA-256 and SHA-384	*NIST SP 800-78-3 Table 3-7; FPKI CP v1.17 Section 6.1.5*		ICAM Test Lab

Comment [FICAM1]: We anticipate dropping this requirement as we are unaware of industry solutions that use the KMK for PACS. Are there live use cases for this key?

Comment [FICAM2]: We anticipate dropping this requirement as we are unaware of industry solutions that use the KMK for PACS. Are there live use cases for this key?

Comment [FICAM3]: We anticipate dropping this requirement as we are unaware of industry solutions that use the KMK for PACS. Are there live use cases for this key?

Identifier #	Required Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-VS-150	V	The system shall support AES-128, AES-192, and AES-256	*NIST SP800-78-3 table 3-1; FPKI CP v1.17section 6.1.5*		ICAM Test Lab
R-VS-151	V	The system shall support 2TDEA and 3TDEA	*NIST SP 800-78-3 Table 3-1; FPKI CP v1.17 Section 6.1.5*		ICAM Test Lab
R-VS-152	V	The system shall support RSA public key exponents in the range of 65,537 (2^16+1) through 2^256-1	*NIST SP 800-78-3 Table 3-2*		ICAM Test Lab

Comment [FICAM4]: Optional SYM-CAK. We anticipate dropping this requirement as we are unaware of interoperable solutions from industry that leverage SYM-CAK. Are there live interoperable solutions using this key?

Could also be used in TLS between infrastructure components. Is this done today?

Comment [FICAM5]: Optional SYM-CAK. We anticipate dropping this requirement as we are unaware of interoperable solutions from industry that leverage SYM-CAK. Are there live interoperable solutions using this key?

Could also be used in TLS between infrastructure components. Is this done today?

Table 2 provides a mapping of credential numbers that are read from a particular card, what format the original number is, what the reader must do to send it to a panel configured for a specific bit-length.

Table 2 – Credential Number Transform Rules

Credentials		Secure Controller Rules	Panel configuration
FICAM PIV	FASC-N	Transmit 48-bit FASC-N ID	128-bit
	FASC-N	Transmit 200-bit FASC-N	200-bit
	UUID[1]	Pass thru	128-bit
	UUID	Pass thru	200-bit
FICAM PIV-I	UUID	Pass thru	128-bit
	UUID	Pass thru	200-bit

[1] UUID is referenced in the FICAM PIV credential number model based on the Draft FIPS 201-2 intention to mandate the UUID for PIV. In this environment, it is anticipated the FASC-N may be retired and both PIV and PIV-I will rely upon the UUID for the credential number in all cases.

Table 3 - Specifications for the End-Entity's Keys on their PIV Card

Source	Section	Page	Requirements		
NIST SP 800-78-3	3.1, Table 3-1	4	PIV Authentication Key	Through 12/31/2013	RSA (1024 or 2048 bits) ECDSA (Curve P-256)
				After 12/31/2013	RSA (2048 bits) ECDSA (Curve P-256)
			Card Authentication Key	Through 12/31/10	2TDEA 3TDEA AES-128, AES-192, or AES-256 RSA (1024 or 2048 bits) ECDSA (Curve P-256)
				1/1/2011 through 12/31/2013	3TDEA AES-128, AES-192, or AES-256 RSA (1024 or 2048 bits) ECDSA (Curve P-256)
				After 12/31/2013	3TDEA AES-128, AES-192, or AES-256 RSA (2048 bits) ECDSA (Curve P-256)
			Digital Signature Key	After 12/31/2008	RSA (2048 bits) ECDSA (Curves P-256 or P-384)
			Key Management Key	After 12/31/2008	RSA key transport (2048 bits); ECDH (Curves P-256 or P-384)

Table 4 - Minimum and Maximum RSA Public Key Exponents

Source	Section	Page	Requirements		
NIST SP 800-78-3	3.1, Table 3-2	6	RSA (1024)	65,537 (2^16 + 1) minimum	2^256-1 maximum
			RSA (2048)	65,537 (2^16 + 1) minimum	2^256-1 maximum

Table 5 - Signatures Covering Objects Placed on the Card by the Issuer

Source	Section	Page	Requirements			
NIST SP 800-78-3	3.2.1, Table 3-3	7	Through 12/31/2010	RSA (2048 or 3072)	SHA-1 SHA-256 SHA-256	PKCS #1 v1.5 PKCS #1 v1.5 PSS
				ECDSA (Curve P-256) ECDSA (Curve P-384)	SHA-256 SHA-384	N/A N/A
			After 12/31/2010	RSA (2048 or 3072 bits)	SHA-256 SHA-256	PKCS #1 v1.5 PSS
				ECDSA (Curve P-256) ECDSA (Curve P-384)	SHA-256 SHA-384	N/A N/A

Table 6 - Hash Algorithm Used by the Issuer For and Within the Security Object

Source	Section	Page	Requirements
NIST SP 800-78-3	3.2.3, Table 3-7	9	SHA-1 SHA-256 SHA-384

Table 7 - FPKI Common Policy: section 6.1.5 Key Sizes

Source	Section	Page	Requirements		
FPKI CP v1.17	6.1.5	49		RSA PKCS #1 v1.5 RSASSA-PSS ECDSA	
FPKI CP v1.17	6.1.5	49	Trusted Certificates (self-signed root) shall contain public key and be signed by corresponding private key using	expire before 1/1/2031	RSA (2048 or 3072) ECDSA (P-256 or P-384)
				expire after 1/1/2031	RSA (3072) ECDSA (P-256 or P-384)
FPKI CP v1.17	6.1.5	49	CA signature keys for certificates and CRLs	expire before 12/31/2010	RSA (1024, 2048 or 3072) ECDSA (P-256 or P-384)
				expire after 12/31/2010	RSA (2048 or 3072) ECDSA (P-256 or P-384)

Source	Section	Page	Requirements		
				expire after 1/1/2031	RSA (3072) ECDSA (P-256 or P-384)
FPKI CP v1.17	6.1.5, FIPS 201 Practice Note	50	CA signature keys for certificates, CRLs or OCSP certificates	issued on or after 1/1/2008	RSA (2048 or 3072) ECDSA (P-256 or P-384)
			CA signature keys for CRLs		RSA (1024) for certificates signed with RSA (1024)
			CA signature keys for OCSP responder certificates	before 12/31/2010	RSA (1024)
FPKI CP v1.17	6.1.5	50	Certificates and CRLs issued by CAs	expire before 12/31/2010	SHA-1, SHA-256, SHA-384 SHA-1 for CRLs when certificate signed using SHA-1
				expire after 12/31/2010	SHA-256, SHA-384 SHA-1 for CRLs issued before 1/1/2014 when certificate signed using SHA-1
				ECDSA	SHA-256 or SHA-384
			Certificates issued to OCSP responder	issued before 12/31/2013	SHA-1 when certificate signed using SHA-1
			Certificate Status Servers	Use same signing algorithm and hash algorithm from certificate after 12/31/2010	OCSP response using SHA-1 only if pre-produced
			id-fpki-common-devices	expire before 12/31/2010	RSA (1024, 2048, or 3072) ECDSA (P-256 or P-384)
			id-fpki-common-devices and id-fpki-common-devicesHardware	expire after 12/31/2010	RSA (2048, or 3072) ECDSA (P-256 or P-384)
			id-fpki-common-devices and id-fpki-common-devicesHardware	expire after 12/31/2030	RSA (3072) ECDSA (P-256 or P-384)

Source	Section	Page	Requirements		
			id-fpki-common-authentication or id-fpki-common-cardAuth	expire before 1/1/2014	RSA (1024 or 2048) ECDSA (P-256)
			id-fpki-common-authentication or id-fpki-common-cardAuth	expire after 1/1/2014	RSA (2048) ECDSA (P-256)
FPKI CP v1.17	6.1.5	51	id-fpki-common-policy, id-fpki-common-hardware, and id-fpki-common-High		RSA (2048 or 3072) ECDSA (P-256 or P-384)
			TLS to interact with CA and its CSS	through 12/31/2010	3TDEA AES
				after 12/31/2010	AES
				through 12/31/2008	RSA (1024) ECC > 163-bit
				after 12/31/2008	RSA (2048) ECC > 224-bit
				after 12/31/2030	RSA (3072) ECC > 256-bit

3.2 Approval Mechanism Matrix

Table 8 provides an indication of the total number of requirements applicable for the Product and provides a breakup of how the evaluation will be conducted based on the different approval mechanisms available to the Lab.

Table 8 - Approval Mechanism Matrix

Total Requirements	Approval Mechanisms						
	SV	LTDR	IL- TDR	VDR	C	A	ISO-TDR
152	N/A	N/A	✓	✓	N/A	✓	N/A
Legend: SV – Site Visit; LTDR – Lab Test Data Report; IL-TDR – ICAM Lab Test Data Report; VDR – Vendor Doc. Review; C – Certification; A – Attestation; ISO-TDR – ISO Certified Lab Test Data Report							

3.3 Evaluation Criteria

This section provides details on the process employed by the ICAM Test Lab for evaluating the Product against the requirements enumerated above.

For this category, the ICAM Test Lab will perform end-to-end system testing of the Product for compliance to R-VS-1 through R-VS-152. Testing will be done in accordance with the *FICAM PACS Master Test Procedures*.

3.3.1 Vendor Documentation Review

Evaluation Procedure:	1. The ICAM Test Lab will update the status in the Web-Enabled Tool to “VDR Begun” as instructed in *Web-enabled Tool Laboratory User Guide*. 2. The ICAM Test Lab will review documentation submitted by the Supplier to determine if Supplier claims to support R-VS-1 through R-VS-152. 3. The ICAM Test Lab will conduct a design review if Supplier claims to support R-VS-1 through R-VS-152. The ICAM Test Lab will update the status to “VDR Complete” as instructed in *Web-enabled Tool Laboratory User Guide*.
Expected Results:	Submitted documentation and design information demonstrates that the requirements are met by the product.

153 3.3.2 ICAM Lab Test Data Report

Test Procedure:	1. The ICAM Test Lab will update the status in the Web-Enabled Tool to "LTDR Begun" as instructed in *Web-enabled Tool Laboratory User Guide*. 2. The ICAM Test Lab will execute test procedures for this category in accordance with the *Validation System Test Procedures*. 3. The ICAM Test Lab will update the status to "IL-TDR Complete" as instructed in *Web-enabled Tool Laboratory User Guide*.
Expected Result:	The Product successfully passes all the test cases documented within the test procedure.

154 3.3.3 Attestation

Evaluation Procedure:	1. The ICAM Test Lab will update the status in the Web-Enabled Tool to "A Begun" as instructed in *Web-enabled Tool Laboratory User Guide*. 2. The ICAM Test Lab will review the Attestation Form provided by the Supplier, confirming that the Product, to the best of their knowledge, conforms to all the necessary requirements of the category under which the Product applies. 3. The ICAM Test Lab will verify that person signing this Attestation Form has the authority to do so (e.g., CSO, CEO, CIO, CFO, CTO, Vice-President, President, Business Partner , Owner). 4. The ICAM Test Lab will update the status in the Web-Enabled Tool to "A Complete" as instructed in *Web-enabled Tool Laboratory User Guide*.
Expected Results:	The Attestation Form has been signed by an authorized individual (e.g., CSO, CEO, CIO, CFO, CTO, Vice-President, President, Business Partner, Owner).

Appendix A—Document Release Summary of Changes

Identifier #	Reference	Description of Change