U.S. General Services Administration

PACS Head-End 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	1/2/13	Document creation	Limited
Draft	0.0.2	1/3/13	Added Requirements Matrix	Limited
Draft	0.0.3	1/4/13	First team edit	Limited
Draft	0.0.4	1/11/13	Edits 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	1/22/13	QA	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 government. A set of approval and test procedures have been developed which outline the evaluation criteria (requirements), approval mechanisms, and test processes employed by industry and ICAM laboratories during their evaluation of a Supplier's product or service against the requirements for that category.

A Supplier submitting a PACS Head-End (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

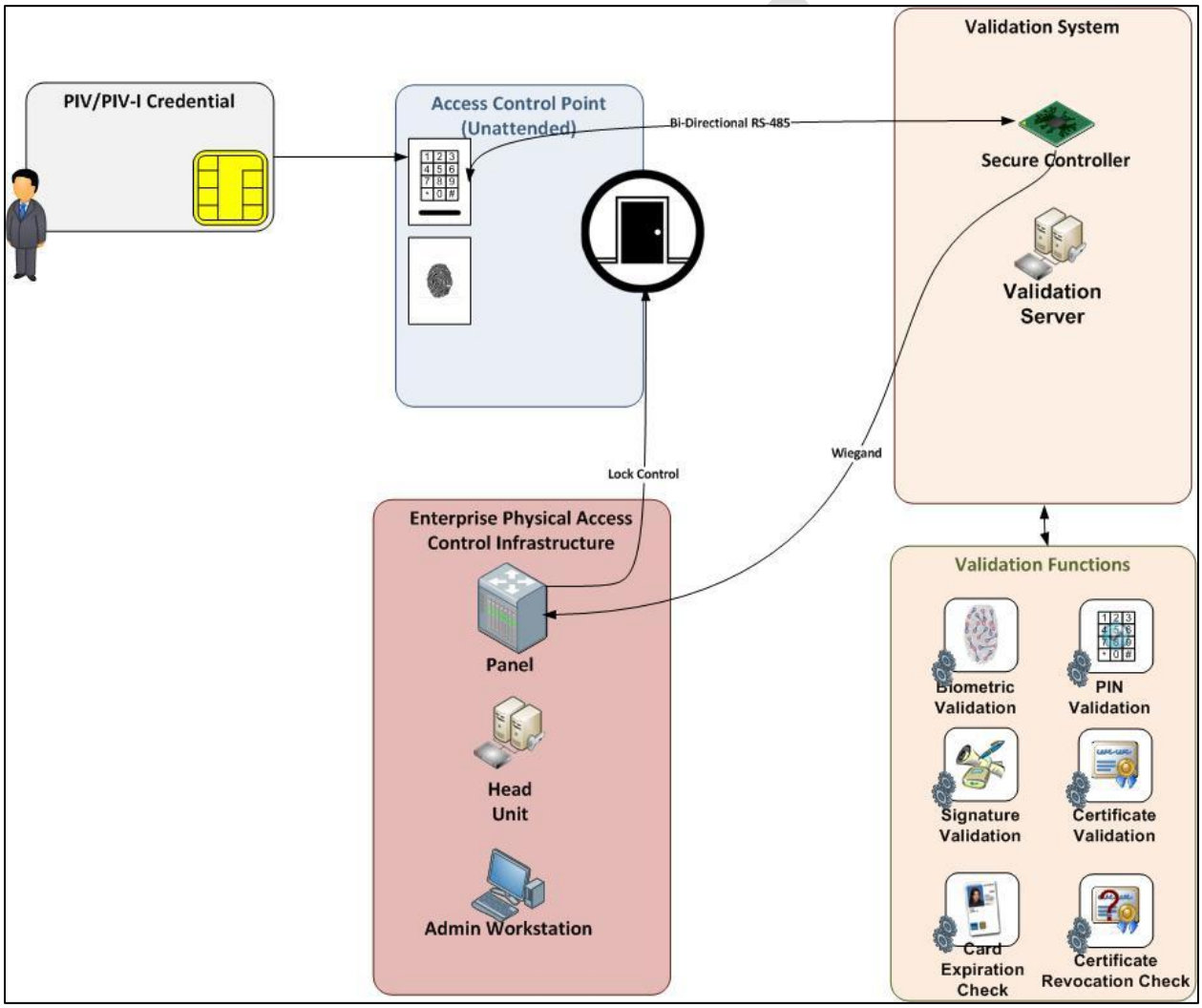
A PACS Head-End is comprised of software and hardware that tie credential numbers to persons with access to a facility. The Head-End confirms their assigned schedules and clearances, and electronically actuates door locks. Often the Head-End is integrated with other security-relevant features such as video monitoring and an Intrusion Detection System (IDS). A basic Head-End system interfaces with the following components:

- Head-End service
  - Administrative workstations
- Field Panel
  - Door controller
  - Lock hardware
  - Door position sensor
- Validation System
  - Secure Controller (sometimes integrated into a Field Panel)
  - Registration Station (sometimes integrated with Head-End administrative workstations)
- Card reader/Bio capture for registration
  - Transparent USB Card Reader
  - Single Fingerprint Capture Device
  - Integrated Card Reader/Writer and Single Fingerprint Capture Device
- Card Reader for Access

- Transparent Reader
- FICAM Transitional Reader
- FICAM Reader

Figure 1 shows one way that a PACS Head-End may be integrated into a full FICAM Testing Program conformant system that is evaluated against the *FICAM PIV in Enterprise PACS Guidance Draft version 2.0.2* (*PIV in E-PACS*).

Figure 1 - Representative architecture for a PACS Head-End



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

1. The Product itself. This should 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 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) for this category. Examples of specific documentation includes user guides, technical specifications, white papers, and test cards.

3 Evaluation Procedure for a Transitional Transparent Reader (TTR)

3.1 Requirements

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

Table 1 - Head-End Requirements

Identifier #	Components	Requirement Description	Source	Requirement #	Approval Mechanism
Time of Registration					
R-HE-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	Lab Test Data Report
R-HE-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-HE-3	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-HE-4	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-HE-5	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-HE-6	H,V,R	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-HE-7	H,V,R	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-HE-8	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

Identifier #	Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-HE-9	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-HE-10	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-HE-11	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-HE-12	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-HE-13	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-HE-14	H,V,R	A/C Power loss to panel.	*PIV in E-PACS*	PPE-1	ICAM Test Lab
R-HE-15	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-HE-16	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-HE-17	H	shall be able to define: Access points for each population.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3, PAI-2	ICAM Test Lab
R-HE-18	H	shall be able to define: Temporal access rules for each population	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3, PAI-2	ICAM Test Lab
R-HE-19	H	The system shall allow for integrated provisioning once a positive determination of a credential's suitability has been made for PIV.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3, PAI-2	ICAM Test Lab

Identifier #	Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-HE-20	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-HE-21	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-HE-22	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-HE-23	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-HE-24	H,V	Shall support: signed CHUID.	*PIV in E-PACS*	PCM-1, PCM-2	ICAM Test Lab
R-HE-25	H,V,R	Shall support: Card Authentication Key.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-HE-26	H,V,R	Shall support: PIV Authentication Key + PIN.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-HE-27	H,V,R	Shall support: PIV Authentication Key + PIN + BIO.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-HE-28	H,V,R	Shall support: Card Authentication Key + PIN + BIO.	*PIV in E-PACS*	PCM-1, PCM-2, PCM-3	ICAM Test Lab
R-HE-29	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-HE-30	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

Identifier #	Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-HE-31	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-HE-32	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-HE-33	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-HE-34	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-HE-35	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-HE-36	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
R-HE-37	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-HE-38	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-HE-39	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

Identifier #	Components	Requirement Description	Source	Requirement #	Approval Mechanism
R-HE-40	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-HE-41	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-HE-42	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-HE-43	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-HE-44	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-HE-45	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-HE-46	H,V	Each component in the system shall have GSA FIPS-201-1 APL status, as applicable.	*PIV in E-PACS*	PCA-3	ICAM Test Lab
R-HE-47	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-HE-48	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-HE-49	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
R-HE-50	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-HE-51	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

96

3.2 Approval Mechanism Matrix

Table 2 provides an indication of the total number of requirements applicable for the Product and provides a breakdown of how the evaluation will be conducted based on the different approval mechanisms available to the Lab.

Table 2 - Approval Mechanism Matrix

Total Requirements	Approval Mechanisms						
	SV	LTDR	IL- TDR	VDR	C	A	ISO-TDR
51	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 the evaluation and certification for compliance to R-HE-1 through R-HE-51.

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-HE-1 through R-HE-51. 3. The ICAM Test Lab will conduct a design review if Supplier claims to support R-HE-1 through R-HE-51. 4. 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.

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 *PACS Head-End 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.

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, Vice-President, President, Business Partner, or 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, Vice-President, President, Business Partner, Owner).

Appendix A—Document Release Summary of Changes

Identifier #	Reference	Description of Change