GSA U.S. General Services Administration

**FICAM Reader
Approval Procedure**
VERSION 0.1.0

DRAFT

FIPS 201 EVALUATION PROGRAM

January 23, 2013

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	1/4/13	Document creation	Limited
Draft	0.0.2	1/10/13	Updates per full team edit	Limited
Draft	0.0.3	1/13/13	Initial basic QA	Limited
Draft	0.0.4	1/17/13	QA fixes	Limited
Draft	0.0.4	1/22/13	QA	Limited
Draft	0.1.0	1/23/13	Team review	EPTWG

Table of Contents

List of Tables

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 regarding 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 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 of the applicable FICAM Testing Program Approved Products List (APL) category.

A Supplier submitting a FICAM Reader (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 APL.

1.2   Category Description

The FICAM Reader is a Physical Access Control System (PACS) reader. It provides agencies with a reader that solely supports *FICAM PIV in Enterprise PACS Guidance Draft version 2.0.2* (*PIV in E-PACS*) conformant PKI-CAK, PKI-AUTH, BIO, PKI-AUTH+BIO authentication methods. The FICAM Reader category is a target architecture category where legacy card and communication technologies not utilizing PIV or PIV-I are no longer supported within a given PACS infrastructure. This category requires bi-directional communications between the FICAM Reader and secure controllers that are part of a Validation System.

The following FICAM Reader modes are required:

1. PKI-CAK
2. BIO (if the reader has a PIN pad and fingerprint sensor)
3. PKI-AUTH (if the reader has a PIN pad)
4. PKI-AUTH+BIO (if the reader has a PIN pad and fingerprint sensor)

The Product being tested must have at least one of the FICAM Reader modes listed above. The Product must be tested against applicable *PIV in E-PACS* requirements for modes 1-4.

42 ## 1.3   Purpose
43 The purpose of this document is to:
44
45 • Provide a list of artifacts and/or documentation that need to be submitted to the ICAM
46   Test Lab as part of the application package submission.
47 • Document the list of the requirements that apply to this category.
48 • Specify the evaluation criteria along with their approval mechanisms that will be used by
49   the ICAM Test Lab to verify compliance of the Product against the requirements that
50   apply to this category.
51
52

2   Application Package Content

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

1. The Product itself. This should be delivered to the 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 vendor 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 the 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 are user guides, technical specifications, and white papers.

3   Evaluation Procedure for a FICAM Reader

3.1   Requirements

In order to approve a Product as conformant with FICAM Reader (FR) Requirements, the Product must be compliant with all the requirements in Table 1. The 'Approval Mechanism' column describes the technique utilized by the ICAM Test Lab to evaluate compliance to that particular requirement.

Table 1 - FICAM Reader Requirements

Identifier #	Interface	Requirement Description	Source	Requirement #	Approval Mechanism
Interface Requirements					
R-FR-1	Reader to Controller	Product shall support Reader to Panel communications using bi-directional RS-485.	*PIV in E-PACS*	PCM-3	ICAM Test Lab
R-FR-2	Reader to Controller	Product may support secure wireless communications in lieu of or in addition to R-FR-1.	*PIV in E-PACS*	PCM-3, PIA-3.2, PIA-3.4	ICAM Test Lab
FICAM Reader Requirements					
R-FR-3	Contact	The contact interface of the reader, if present, shall be tested in accordance with *ISO/IEC 13073-3:2010* Sections 4, 7, and 8.	FIPS 201-1		ISO Lab Test Data Report
R-FR-4	Contactless	The contactless interface of the reader, if present, shall be tested in accordance with *ISO/IEC 13073-6:2011* Sections 4, 5, 6.1, 7.1 and 8.1, and *ISO/IEC 13073-6:2011/Amd.4:2012*.	FIPS 201-1		ISO Lab Test Data Report
R-FR-5		The Product shall be capable of supporting at least one of the following PIV Authentication Modes: 1. PKI-CAK 2. PKI-AUTH 3. BIO 4. PKI-AUTH+BIO	*PIV in E-PACS*	PIA-2	ICAM Test Lab
R-FR-6		Identity Factor Authentication.	*PIV in E-PACS*	PIA-3	ICAM Test Lab
R-FR-7		Accepting Device (AD).	*PIV in E-PACS*	PIA-3.1	ICAM Test Lab
R-FR-8		Validation of Trusted Origin (VTO).	*PIV in E-PACS*	PIA-3.2	ICAM Test Lab

Comment [FICAM1]: We would like to know if there is a strong desire from industry to support Ethernet?

7

Identifier #	Interface	Requirement Description	Source	Requirement #	Approval Mechanism
R-FR-9		Active Authentication (AA).	*PIV in E-PACS*	PIA-3.3	ICAM Test Lab
R-FR-10		Protection of Authenticator (POA).	*PIV in E-PACS*	PIA-3.4	ICAM Test Lab
R-FR-11		Revocation Check (RC).	*PIV in E-PACS*	PIA-3.5	ICAM Test Lab
R-FR-12		Expiration Check (EC).	*PIV in E-PACS*	PIA-3.6	ICAM Test Lab
R-FR-13		Signature Validation.	*PIV in E-PACS*	PIA-4	ICAM Test Lab
R-FR-14		Full Path Validation.	*PIV in E-PACS*	PIA-5	ICAM Test Lab
R-FR-15		Cross-Agency Interoperable Authentication.	*PIV in E-PACS*	PIA-6	ICAM Test Lab
R-FR-16		Card Revocation Check Mechanisms.	*PIV in E-PACS*	PIA-7	ICAM Test Lab
R-FR-17		Communication between System Elements.	*PIV in E-PACS*	PSC-1	ICAM Test Lab
R-FR-18		Component Installation and Configuration.	*PIV in E-PACS*	PCM-2	ICAM Test Lab
R-FR-19		Configuring Reader Authentication Modes.	*PIV in E-PACS*	PCM-3	ICAM Test Lab
R-FR-20		Secure Processing Protection	*PIV in E-PACS*	PPE-1	ICAM Test Lab
R-FR-21		UL 294 Certification	*PIV in E-PACS*	PCA-2	ICAM Test Lab
R-FR-22		Each component in the system shall have FIPS 140-2 certification, as applicable	*PIV in E-PACS*	PCA-4	ICAM Test Lab

80

81 ## 3.2 *Approval Mechanism Matrix*

82 Table 2 shows the total number of requirements applicable to the Product, and provides a
83 breakdown of how the evaluation will be conducted based on the different approval mechanisms
84 available to the ICAM Test Lab.
85
86 **Table 2 – Approval Mechanism Matrix**
87

Total Requirements	Approval Mechanisms						
	SV	**LTDR**	**IL- TDR**	**VDR**	**C**	**A**	**ISO-TDR**
22	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							

88

89 ## 3.3 Evaluation Criteria

90 This section details the process employed by the ICAM Test Lab for evaluating the Product
91 against the requirements enumerated in Section 3.1.
92
93 For this category, there are four elements of testing performed in two stages:
94
95 **Stage 1: Industry Testing**
96   a. Independent Lab testing and evaluation for *ISO 7816* compliance by an *ISO 17025*
97   certified Lab for testing in accordance with *ISO/IEC 10373-3:2010* per R-FR-3.
98   b. Independent Lab testing and evaluation of Product compliance to *ISO 14443* by an
99   *ISO 17025* certified lab for testing in accordance with *ISO/IEC 10373-6:2011* and
100   *ISO/IEC 10373-6 Amendment 4:2012* per R-FR-4.
101
102 **Stage 2: ICAM Testing**
103   a. ICAM Test Lab evaluation and certification for compliance to R-FR-1 through
104   R-FR-2 (Interface requirements).
105   b. ICAM Test Lab evaluation and certification for compliance to R-FR-5 through
106   R-FR-22 (FICAM Reader requirements).
107
108 An Independent Lab, if certified by the appropriate authority, may perform any combination of
109 the industry testing requirements.
110

111   ### 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 the *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-FR-1 through R-FR-22. 3. The ICAM Test Lab will conduct a design review if Supplier claims to support R-FR-1 through R-FR-22. 4. The ICAM Test Lab will update the status to "VDR Complete" as instructed in the *Web-enabled Tool Laboratory User Guide*.
Expected Results:	Submitted documentation and design information demonstrates that the requirements are met by the product.

112   ### 3.3.2 ICAM Test 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 the *Web-enabled Tool Laboratory User Guide*. 2. The ICAM Test Lab will execute test procedures for this category in accordance with *FICAM Reader Test Procedures*. 3. The ICAM Test Lab will update the status to "IL-TDR Complete" as instructed in the *Web-enabled Tool Laboratory User Guide*.
Expected Result:	The Product successfully passes all the test cases documented within the test procedure.

113

114

115   **3.3.3 Attestation**

Evaluation Procedure:	1. ICAM Test Lab will update the status in the Web-Enabled Tool to "A Begun" as instructed in the *Web-enabled Tool Laboratory User Guide*. 2. 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. ICAM Test Lab will verify that person signing the Attestation Form has the authority to do so (e.g., CSO, CEO, CIO, CFO, Vice-President, President, Business Partner, Owner). 4. ICAM Test Lab will update the status in the Web-Enabled Tool to "A Complete" as instructed in the *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