

**FICAM Transitional Reader
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	12/05/12	Document creation	Limited
Draft	0.0.2	12/07/12	First team edit	Limited
Draft	0.0.3	12/08/12	Second team edit	Limited
Draft	0.0.4	12/20/12	Third team edit	Limited
Draft	0.0.5	1/3/13	Fourth team edit	Limited
Draft	0.0.6	1/8/13	Full team edit	Limited
Draft	0.0.7	1/13/13	Initial basic QA	Limited
Draft	0.0.8	1/17/13	QA fixes	Limited
Draft	0.0.9	1/22/13	QA	Limited
Draft	0.1.0	1/23/13	Team review	EPTWG

DRAFT

Table of Contents

1	Introduction.....	1
1.1	Overview.....	1
1.2	Category Description.....	1
1.3	Purpose.....	2
2	Application Package Content.....	3
3	Evaluation Procedure for a FICAM Transitional Reader (FTR).....	4
3.1	Requirements.....	4
3.2	Approval Mechanism Matrix.....	7
3.3	Evaluation Criteria.....	7
3.3.1	Vendor Documentation Review.....	8
3.3.2	ICAM Lab Test Data Report.....	8
3.3.3	Attestation.....	9
	Appendix A— Document Release Summary of Changes.....	10

List of Tables

Table 1 - FICAM Transitional Reader Technology Requirements.....	2
Table 2 - FICAM Transitional Reader Requirements.....	4
Table 3 – Legacy Credential Number Transform Rules.....	6
Table 4 - Approval Mechanism Matrix.....	7

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 which 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 FICAM Transitional Reader (hereafter referred to as "Product") for evaluation must follow the *Suppliers Policies and Procedures Handbook*. In addition to this handbook, Suppliers also need to refer to this Approval Procedure, 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). Products that successfully complete testing in this category will be listed on the APL under two categories: FICAM Transitional Reader and FICAM Reader.

1.2 Category Description

The FICAM Transitional Reader is a Physical Access Control System (PACS) reader. It provides agencies with a bridge from deployed technologies, such as 125 KHz Prox and iClass, to full FICAM Reader capabilities that support PIV authentication mechanisms described by *FICAM PIV in Enterprise PACS Guidance Draft version 2.0.2 (PIV in E-PACS)*. Specifically, this transition is a migration from traditional Prox or FASC-N/UUID authentication, up to *PIV in E-PACS*-conformant PKI-CAK, BIO, PKI-AUTH, PKI-AUTH+BIO authentication methods. Many buildings have older wiring cable plant and can only support the uni-directional Wiegand protocol. Some buildings have bi-directional cable plant (i.e. RS-485), but the PACS is not upgraded yet to support FICAM authentication methods. Some buildings or access points will be updated to support full bi-directional communications and the FICAM authentication methods. The FICAM Transitional Reader provides a capability for agencies to install a PACS reader that preserves their investment in the reader as they transition from deployed technologies to the end-state FICAM Reader mechanisms. This drives new requirements for a FICAM Transitional Reader as shown in

39 Table 1.
40
41
42
43

DRAFT

44

Table 1 - FICAM Transitional Reader Technology Requirements

At least one Legacy Credential	Both APL Transparent Modes	At least one FICAM Mode	At least one reader to panel interface
125 KHz Prox	FASC-N	PKI-CAK	Wiegand and RS-485
iClass	UUID	BIO	Secure wireless
		PKI-AUTH	
		PKI-AUTH+BIO	

45

The **Technology Requirements** include the following legacy credential and reader-to-panel interface capabilities:

47

48

49

50

51

52

53

54

55

1. 125 KHz Prox
2. iClass
3. FASC-N (PIV)
4. UUID (PIV-I)
5. Support both uni-directional Wiegand and bi-directional RS-485 communications
6. Support secure wireless communications

56

The Product being tested must have a minimum of one legacy credential technology of items 1-2 listed above. The Product shall support items 3-4 listed above. If the Product is hard wired, it must support item 5 listed above. A Product may be wireless as defined by item 6 listed above in lieu of or in addition to item 5 listed above.

57

58

59

60

61

The following **FICAM Reader Mode Requirements** support the transition from Legacy to FICAM operations:

62

63

64

65

66

67

68

7. PKI-CAK
8. BIO (if the Product has a PIN pad and fingerprint sensor)
9. PKI-AUTH (if the Product has a PIN pad)
10. PKI-AUTH+BIO (if the Product has a PIN pad and fingerprint sensor)

69

The Product being tested must have at least one of the FICAM Reader modes 7-10 above.

70

71

The Product must be tested against *PIV in E-PACS* for Technology Requirements 5-6 listed above and Mode Requirements 7-10 listed above.

72

73

1.3 Purpose

74

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

75

76

77

78

79

80

81

82

- Provide a list of the artifacts and/or documentation that needs to be submitted to the Industry and ICAM Labs 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 Industry and ICAM Labs to verify compliance of the Product against the requirements that apply to this category.

83 2 Application Package Content

84 Application Package Content includes the artifacts, documentation, and the Product itself that
85 needs to be submitted to the Industry and ICAM Labs so that evaluation can be performed.
86 Application Package Content for this category includes the following:
87

- 88 1. The Product itself. This should be delivered to an Industry testing lab as well as the
89 ICAM Test Lab (addresses can be found at <http://fips201ep.cio.gov/labs.php>) using a
90 secure delivery method that requires acknowledgement of receipt (e.g., FedEx, UPS,
91 hand delivery). The Supplier shall provide installation and configuration support as
92 appropriate.
- 93 2. Completed Application Form, provided on the FIPS 201 EP website. (This form will be
94 available through the web interface once users have been assigned a login credential.)
- 95 3. Completed and signed Lab Service Agreement (found in the application submission
96 package ZIP file). The Lab Service Agreement should be completed and scanned into a
97 document to be uploaded to the FIPS 201 EP website.
- 98 4. Completed and signed Attestation Form (found in the application submission package
99 ZIP file). The Attestation Form should be completed and scanned into a document to be
100 uploaded to the FIPS 201 EP website.
- 101 5. All necessary Supplier documentation providing proof that the Product complies with the
102 requirements (as outlined in Section 3.1 of this document) for this category, which has
103 Supplier documentation review as its approval mechanism. Examples of specific
104 documentation includes user guides, technical specifications, white papers, and test cards.

105 **3 Evaluation Procedure for a FICAM Transitional Reader (FTR)**

106 **3.1 Requirements**

107 In order to approve the Product as conformant with FICAM Transitional Reader (FTR)
 108 Requirements, it at a minimum must be certified as a Transparent Reader and be listed on the
 109 APL in the transparent reader category. The FTR must be compliant with all the requirements
 110 listed in Table 2. The approval mechanism column describes the technique utilized by the ICAM
 111 Test Lab to evaluate compliance to that particular requirement.

112

113 **Table 2 - FICAM Transitional Reader Requirements**

Identifier #	Interface	Requirement Description	Source	Requirement #	Approval Mechanism
Legacy Requirements					
R-FTR-1	Contact and/or Contactless	Product shall be certified and listed on the APL under the Transparent Reader category	FICAM Testing Program		Lab Test Data Report
R-FTR-2	Contactless	Product shall support at least one legacy credential technology using 125 KHz Prox and/or iClass	FICAM Testing Program		ICAM Test Lab
R-FTR-3	Contact and/or Contactless	Transparent FASC-N (PIV)	FICAM Testing Program		ICAM Test Lab
R-FTR-4	Contact and/or Contactless	Transparent UUID (PIV-I)	FICAM Testing Program		ICAM Test Lab
R-FTR-5		Product shall support credential number transform rules based on Table 3	FICAM Testing Program		ICAM Test Lab
Interface Requirements					
R-FTR-6	Reader to Controller	Product shall support Reader to Panel communications using uni-directional Wiegand	FICAM Testing Program		ICAM Test Lab
R-FTR-7	Reader to Controller	Product shall support Reader to Panel communications using bi-directional RS-485	<i>PIV in E-PACS</i>	PCM-3	ICAM Test Lab
R-FTR-8	Reader to Controller	Product may support secure wireless communications in lieu of or in addition to both R-FTR-6 and R-FTR-7	<i>PIV in E-PACS</i>	PCM-3, PIA-3.2, PIA-3.4	ICAM Test Lab
FICAM Reader Requirements					

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

Identifier #	Interface	Requirement Description	Source	Requirement #	Approval Mechanism
R-FTR-9	Contact	The contact interface of the Product, if present, shall be tested in accordance with <i>ISO/IEC 13073-3:2010</i> Sections 4, 7, and 8.	FIPS 201-1		ISO Lab Test Data Report
R-FTR-10	Contactless	The contactless interface of the Product, if present, shall be tested in accordance with <i>ISO/IEC 13073-6:2011</i> Sections 4, 5, 6.1, 7.1, and 8.1, and <i>ISO/IEC 13073-6:2011/Amd.4:2012</i> .	FIPS 201-1		ISO Lab Test Data Report
R-FTR-11		The Product shall be capable of supporting at least one of the following PIV Authentication Modes: <ol style="list-style-type: none"> 1. PKI-CAK 2. PKI-AUTH 3. BIO 4. PKI-AUTH+BIO 	<i>PIV in E-PACS</i>	PIA-2	ICAM Test Lab
R-FTR-12		Identity Factor Authentication	<i>PIV in E-PACS</i>	PIA-3	ICAM Test Lab
R-FTR-13		Accepting Device (AD)	<i>PIV in E-PACS</i>	PIA-3.1	ICAM Test Lab
R-FTR-14		Validation of Trusted Origin (VTO)	<i>PIV in E-PACS</i>	PIA-3.2	ICAM Test Lab
R-FTR-15		Active Authentication (AA)	<i>PIV in E-PACS</i>	PIA-3.3	ICAM Test Lab
R-FTR-16		Protection of Authenticator (POA)	<i>PIV in E-PACS</i>	PIA-3.4	ICAM Test Lab
R-FTR-17		Revocation Check (RC)	<i>PIV in E-PACS</i>	PIA-3.5	ICAM Test Lab
R-FTR-18		Expiration Check (EC)	<i>PIV in E-PACS</i>	PIA-3.6	ICAM Test Lab
R-FTR-19		Signature Validation	<i>PIV in E-PACS</i>	PIA-4	ICAM Test Lab
R-FTR-20		Full Path Validation	<i>PIV in E-PACS</i>	PIA-5	ICAM Test Lab
R-FTR-21		Cross-Agency Interoperable Authentication	<i>PIV in E-PACS</i>	PIA-6	ICAM Test Lab
R-FTR-22		Card Revocation Check Mechanisms	<i>PIV in E-PACS</i>	PIA-7	ICAM Test Lab
R-FTR-23		Communication between System Elements	<i>PIV in E-PACS</i>	PSC-1	ICAM Test Lab

Identifier #	Interface	Requirement Description	Source	Requirement #	Approval Mechanism
R-FTR-24		Component Installation and Configuration	<i>PIV in E-PACS</i>	PCM-2	ICAM Test Lab
R-FTR-25		Configuring Reader Authentication Modes	<i>PIV in E-PACS</i>	PCM-3	ICAM Test Lab
R-FTR-26		Secure Processing Protection	<i>PIV in E-PACS</i>	PPE-1	ICAM Test Lab
R-FTR-27		UL 294 Certification	<i>PIV in E-PACS</i>	PCA-2	ICAM Test Lab
R-FTR-28		Each component in the system shall have FIPS 140-2 certification, as applicable	<i>PIV in E-PACS</i>	PCA-4	ICAM Test Lab

114

115 Table 3 provides a mapping of credential numbers that are read from a particular card, what
 116 format the original number is, and what the reader must do to send it to a panel configured for a
 117 specific bit-length.

118

Table 3 – Legacy Credential Number Transform Rules

Credentials		Reader Rules	Panel Configuration
Prox	26-bit	Pass thru	26-bit
	32-bit	Pass thru	32-bit
	48-bit	Pass thru	48-bit
iClass	26-bit	Pass thru	26-bit
	32-bit	Pass thru	32-bit
	34-bit	Pass thru	34-bit
	37-bit	Pass thru	37-bit
	40-bit	Pass thru	40-bit
	56-bit	Pass thru	56-bit
Transparent PIV	FASC-N	Transmit 48-bit FASC-N ID	48-bit
	CHUID	Transmit GSA 75-bit format	75-bit
	FASC-N	Transmit 48-bit FASC-N ID	96-bit
	FASC-N	Transmit 48-bit FASC-N ID	128-bit
	FASC-N	Transmit 200-bit FASC-N	200-bit
Transparent PIV-I	UUID	Transmit low order 48-bits	48-bit
	UUID	Transmit low order 75-bits	75-bit
	UUID	Transmit low order 96-bits	96-bit
	UUID	Pass thru	128-bit
	UUID	Pass thru	200-bit

119

120

121

122 **3.2 Approval Mechanism Matrix**

123 Table 4 summarizes the total number of requirements applicable for the Product and provides a
 124 breakdown of how the evaluation will be conducted based on the different approval mechanisms
 125 available to the Lab.
 126

127 **Table 4 - Approval Mechanism Matrix**

Total Requirements	Approval Mechanisms						
	SV	LTDR	IL- TDR	VDR	C	A	ISO-TDR
28	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							

128 **3.3 Evaluation Criteria**

129 This section provides details on the process employed by the ICAM Test Lab for evaluating the
 130 Product against the requirements enumerated above.
 131

132 For this category, there are five elements of testing performed in two stages:
 133

134 **Stage 1: Industry Testing**

- 135 a. Independent Lab testing and evaluation by a FIPS 201 *National Voluntary Laboratory Accreditation Program* (NVLAP) certified Lab for conformance and listing on the APL under the Transparent Reader category per R-FTR-1.
- 136 b. Independent Lab testing and evaluation for *ISO 7816* compliance by an *ISO 17025* certified Lab for testing in accordance with *ISO/IEC 10373-3:2010* per R-FTR-9.
- 137 c. Independent Lab testing and evaluation of Product compliance to *ISO 14443* by an *ISO 17025* certified lab for testing in accordance with *ISO/IEC 10373-6:2011* and *ISO/IEC 10373-6 Amendment 4:2012* per R-FTR-10.

143 **Stage 2: ICAM Testing**

- 144 a. ICAM Test Lab evaluation and certification for compliance to R-FTR-2 through R-FTR-8 (Legacy and Interface requirements).
- 145 b. ICAM Test Lab evaluation and certification for compliance to R-FTR-11 through R-FTR-28 (FICAM Reader requirements).

146 An Independent Lab, if certified by the appropriate authority, may perform any combination of
 147 the industry testing requirements.
 148
 149

150
 151
 152

153 **3.3.1 Vendor Documentation Review**

Evaluation Procedure:	<ol style="list-style-type: none"> 1. The ICAM Test Lab will update the status in the Web-Enabled Tool to “VDR Begun” as instructed in <i>Web-enabled Tool Laboratory User Guide</i>. 2. The ICAM Test Lab will review documentation submitted by the Supplier to determine if Supplier claims to support R-FTR-1. 3. The ICAM Test Lab will review documentation submitted by the Supplier to determine if Supplier claims to support R-FTR-2 through R-FTR-8. 4. The ICAM Test Lab will review documentation submitted by the Supplier to determine if Supplier claims to support R-FTR-9 and R-FTR-10. 5. The ICAM Test Lab will conduct a design review if Supplier claims to support R-FTR-11 through R-FTR-28. 6. The ICAM Test Lab will update the status to “VDR Complete” as instructed in <i>Web-enabled Tool Laboratory User Guide</i>.
Expected Results:	Submitted documentation and design information demonstrates that the requirements are met by the product.

154 **3.3.2 ICAM Lab Test Data Report**

Test Procedure:	<ol style="list-style-type: none"> 1. The ICAM Test Lab will update the status in the Web-Enabled Tool to “LTDR Begun” as instructed in <i>Web-enabled Tool Laboratory User Guide</i>. 2. The ICAM Test Lab will execute test procedures for this category in accordance with the <i>FICAM Transitional Reader Test Procedures</i>. 3. The ICAM Test Lab will update the status to “IL-TDR Complete” as instructed in <i>Web-enabled Tool Laboratory User Guide</i>.
Expected Result:	The Product successfully passes all the test cases documented within the test procedure.

155

156

157 **3.3.3 Attestation**

<p>Evaluation Procedure:</p>	<ol style="list-style-type: none"> 1. The ICAM Test Lab will update the status in the Web-Enabled Tool to “A Begun” as instructed in <i>Web-enabled Tool Laboratory User Guide</i>. 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, Owner). 4. The ICAM Test Lab will update the status in the Web-Enabled Tool to “A Complete” as instructed in <i>Web-enabled Tool Laboratory User Guide</i>.
<p>Expected Results:</p>	<p>The Attestation Form has been signed by an authorized individual (e.g., CSO, CEO, CIO, CFO, Vice-President, President, Business Partner, Owner).</p>

DRAFT

158 **Appendix A—Document Release Summary of Changes**

159

Identifier #	Reference	Description of Change

160

DRAFT