Approved PACS Wireless Reader Topology (PACS 20.01)

FRTC VERSION 1.3.3 Rev G

FIPS 201 EVALUATION PROGRAM

November 17, 2020

Version 1.0.0

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

Document History

Status	Version	Date	Comment	Audience
Funal	1.0	11/17/2020	Initial release	Public

Table of Contents

1. Background

As agencies upgrade and deploy physical access as mandated within federal facilities, the demand for wireless locksets has increased. Wireless locksets offer some benefits over wired card readers in that no cabling is required, allowing for placement of readers in situations where conduit may not be possible or expensive (e.g., historical facilities, difficult locations, remote locations, the door frame was grouted without a wire conduit). Historically, GSA has employed a rigorous testing process for certifying card readers and validation engines. This testing regimen assumed the attack surface between the card reader and the validation infrastructure required physical access to the wiring. Thus protections were of physical means such as physical tampers, cable in conduit, etc. Wireless connected readers introduce an additional, non-physical attack surface resulting in solely physical protections being insufficient to mitigate the risk of signal interception and replay.

Commonly, wireless locksets operate in the same frequency ranges WiFi devices operate. While there are no standards for securing wireless locksets presently, there is an abundance of standards around WiFi security. GSA via the Approved Products List Program is approaching the security of wireless locksets in a similar fashion to how the government handles WiFi security. NIST [SP 800-97] outlines wireless security around devices operating in a multiple of IEEE approved modes.

Current best practice for securing readers includes the physical monitoring of the reader itself. This is typically done through security mechanisms such as physical tamper devices; this practice must continue to be employed within wireless readers. Monitoring of the cables connecting the reader to the validation infrastructure has traditionally been protected through physical means and monitored through physical aspects as well. Safeguards such as armored conduit and voltage line monitoring of the wire are all commonplace. Wireless connections need to achieve similar levels of security for the protection of data transmission and integrity across their wireless medium.

When dealing with protecting data transmitted through wireless means there are defined NIST requirements. While not explicit to wireless PACS card readers, these standards are applicable to any wireless devices deployed for Federal use in general. Further, FISMA itself defines a few controls in [SP 800-53] which call for security around deployed wireless devices:

- The control AC-18 deals specifically with wireless access, AC-18(1) thus applies to wireless readers, requiring devices to authenticate to the system using encryption to reduce susceptibility to threats.
- SC-8 deals with Transmission Confidentiality and Integrity of transmitted information,

- SC-18(1) specifically adds cryptographic protection to protect information from unauthorized disclosure and modification, referencing SC-13 to specify FIPS-validated cryptography and NSA-approved cryptography.

NIST [SP 800-97] defines requirements for devices operating in a variety of wireless ranges and specific IEEE standards associated with various frequencies. A common requirement for all devices transmitting data wirelessly is found in Section 7.1. Specifically, requirements for devices defined in [SP 800-97] as either an Access Point (AP) or Station (STA) must have [FIPS 140] certification or use a crypto module that is [FIPS 140] certified and operating in a FIPS mode. Wireless locksets and any associated communications hardware are subject to these requirements.

2. Objectives

With this in mind, GSA is putting the following requirements around wireless readers or locksets) being submitted to the lab for testing.

1. Wireless locksets or wireless readers must transmit data using FIPS validated or NSA-approved cryptography.
    a. [FRTC] Test Cases 7.02.02 and 7.07.01
2. Devices performing cryptography must submit [FIPS 140] Level 2 certification and operate in FIPS mode.
    a. [FRTC] Test Case 7.09.05
3. Card reader to card interaction for wireless devices is no different than their wired counterparts. Time of access test cases will be performed against wireless devices in the exact same fashion a wired reader would be tested. The lab expects no difference in test results for these test cases between the two reader types.
    a. All time of access test cases ([FRTC] Section 5.0, 7.06, 7.07)
4. The device must have FCC appropriate certification for the wireless frequency it utilizes.

3. FIPS 201 Evaluation Program Defined Categories

The PACS 20.01 Topology adds requirements around Wireless PACS PIV readers. The Wireless PACS PIV readers topology is not defined as a single object, but as part of a solution, and to be procured as part of an approved solution using an approved topology. Devices defined in this document are intended to supplement PACS systems and their associated validation infrastructures. There are no Validation Infrastructure restrictions placed on these devices and could potentially be submitted with any approved Validation Infrastructure topology.

3.1 Wireless PACS PIV Reader Category

A wireless PACS PIV Reader consists of two components.

- Wireless Transmission Bridge - A device which interacts with the reader wirelessly and the PACS Validation Infrastructure through a wired connection.
- Wireless PIV Reader - PACS PIV reader or integrated lockset which communicates to the transmission device wirelessly.

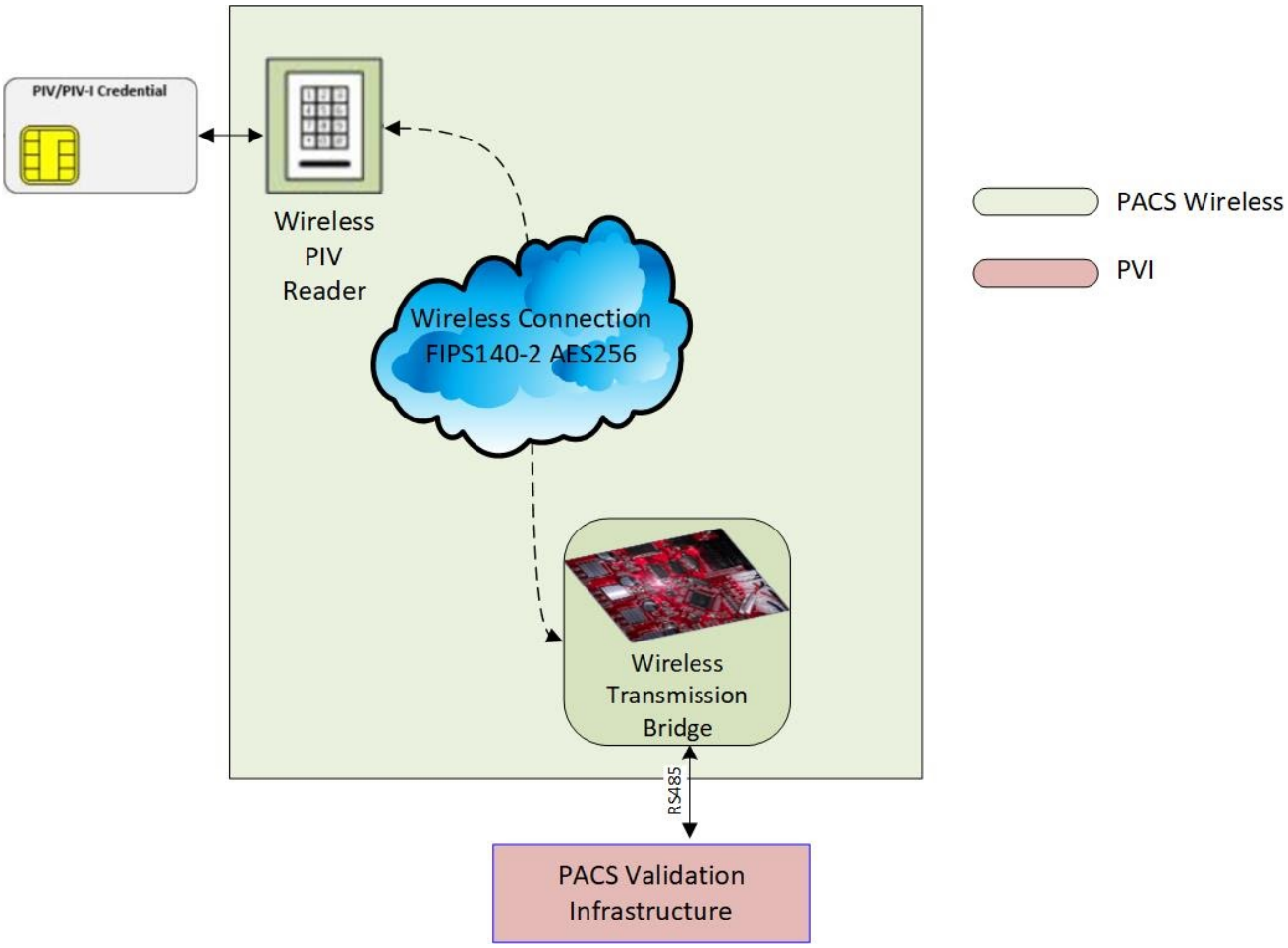
The Transmission device shall be capable of interacting with the wireless reader and the PACS Validation Infrastructure. While this document is not defining how devices should communicate, it is putting requirements on how they should be secured. The transmission device should have a [FIPS 140] Level two certification, and operate in the [FIPS 140] mode. This is to ensure all communications between the transmission device and wireless reader and encrypted to a minimum of an approved cryptographic algorithm. Protection of the communication between the PACS and Transmission Device need to also be taken into consideration. If such communication is also occurring through wireless methods, the same standards also apply.

The Wireless Reader or wireless lockset is the device typically installed within the door itself and communications with the Transmission Device and the bearer of the credential, the credential itself. This device is expected to function in the same method as wired PACS PIV card readers. The Wireless Reader must support a minimum of one FICAM authentication mode as defined in EPACS but may support multi-factor authentication. The Reader may also support optional legacy technologies and credential formats as defined in [FRTC].

3.2 Topology Diagram

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

Figure 1 - Sample 20.01 Wireless Reader Topology diagram



4. Topology Mapping

Mapping is the process of taking the functional requirements defined in [FRTC] and allocating them into the FIPS 201 Evaluation Program categories, and then indicating the specific named components within your solution that perform the operations for that requirement. For wireless readers, the applicant should focus on time of access tests around card validation [FRTC] Section 5 tests. Applicants will need to respond to test associated with the number of factors their wireless readers support within section 5. Additionally the applicant will need to specifically define how the wireless readers meet the requirements within Section 7.01, 7.02, 7.06, 7.07, 7.08, and 7.09 .

For example, if the requirement is for a product to validate signatures at time of access as defined in [FRTC] §5.01-Test 5.01.01, the Applicant should follow the example given in the table below.

FRTC Version	Classifi-cation	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Category(ies)	Components	Process
		5.0			**Authentication at Time of Access Test Cases**					
		5.01			**Signature Verification**					
1.2.0	SR-1	5.01.01	46	00	With ICAM Test Card 46 registered with the PACS, verify product's ability to validate signatures in the certificates found in the certification path for a PIV credential.	Access Granted.	PIA-2 thru PIA-7	Validation System (13.01), FICAM Reader , Mobile Handheld Validation Reader (14.02), Validation System (13.01), Wireless FICAM Reader (20.01)	PACS validation Engine, PACS control panel, PACS Reader, Wireless PACS Reader	Certificate chain is evaluated by MS CAPI/CNG, which throws an exception if one of the certificates in the chain is not within its validity period. The revalidation component generates a log and if an error is found the system denies access for the credential. If no error is found the credential remains active. MS CAPI may rely on its own CRL, CA, and Intermediate CA certificate cache.

References

[FIPS 140] Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-3, March 2019 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

[FIPS 201] Personal Identity Verification (PIV) of Federal Employees and Contractors, Federal Information Processing Standard 201-2, August 2013, or as amended http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

[FRTC] FIPS 201 Evaluation Program Functional Requirements and Test Cases, August 2018 https://www.idmanagement.gov/pacs-frtc-v1-3-3/

[SP800-53] Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Revision 4, January 2015, or as amended https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[SP800-96] PIV Card to Reader Interoperability Guidelines, NIST Special Publication (SP) 800-96, September 2006, or as amended https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-96.pdf

[SP800-97] Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, NIST Special Publication (SP) 800-97, February 2007, or as amended https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf