

CoreStreet FIPS-201 F5 Solution

FIPS 201 Solution for PACS

A FIPS 201 Solution requires two primary capabilities:

1. Enrollment of PIV Cards (Credentials) into the PACS

– This capability is typically provided directly by the PACS manufacturer as a feature of their product or via integration to an Identity Management System (IDMS) for bulk enrollment capability. CoreStreet has developed and licensed card library and validation technology to a number of PACS companies. The technology enables interoperability by validating PIV cards from the local agency as well as from visitors from other government agencies or non-federal organizations. At the time of enrollment and on a recurring interval thereafter, the status of enrolled PIV cards is checked, also referred to as periodic re-validation to prohibit access for revoked cards.

2. Validation of PIV Cards at the Time-of-Access –

Validating cards when they are presented to the reader at an access point is necessary, per the guidance in NIST SP800-116, to check that the card is not counterfeit, cloned, or copied, lost or stolen. NIST FIPS-201 and SP 800-116 define authentication mechanisms (CHUID, CAK, PKI, and BIO) and their application one or more at a time for increasing levels of authentication for access to uncontrolled, controlled, limited, and exclusion areas. The F5 Solution adds time-of-access validation for all PIV card types at all levels of authentication to FIPS-201 enable a PACS without requiring significant modification of the existing system.

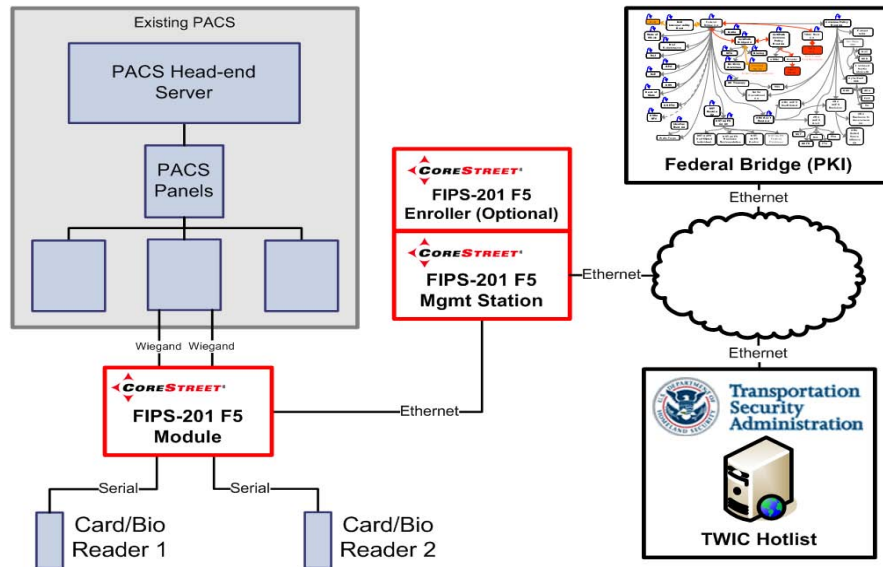
FIPS 201 Background

HSPD-12 mandates that all government agencies use Personal Identity Verification (PIV) cards for physical access control as a way to improve security and to ensure an interoperable approach. To establish standards and guidance for HSPD-12, NIST has published FIPS 201 and Special Publications 800-73, 800-76, and 800-116 that apply to all government agencies. The TSA has published the TWIC Reader Hardware and Card Application Specification and the United States Coast Guard is in the process of issuing rules that will apply to all Maritime Transportation Security Act (MTSA) regulated facilities. And, the Federal CIO Council has released guidance for PIV Interoperability for Non-Federal Issuers, also referenced as PIV-Interoperable (PIV-I) cards, that applies to all contractors, first responders, etc that will require identity cards that must interoperate and be trusted by Federal Government PIV systems. For all of the government agencies, organizations, and facilities affected by HSPD-12, upgrading existing physical access control systems (PACS) requires innovative new solutions and technologies.

Solution Overview

The CoreStreet FIPS-201 F5 Solution upgrades PACS for HSPD-12 compliance without the need for wholesale rip and replacement of existing equipment. The CoreStreet FIPS-201 F5 Solution consists of:

- The **CoreStreet FIPS-201 F5 Module** is a hardware module that contains all the functionality required by FIPS-201, Special Publication 800-116 and the TWIC Reader Specification.
- The **CoreStreet FIPS-201 F5 Management Station** software provides centralized control of assurance level settings and distribution of validation data such as card revocations and trusted issuers.
- The **CoreStreet FIPS-201 F5 Enroller** software validates and captures data from PIV cards that is required to validate that they are from a trusted issuer and to perform periodic status checks to identify revoked cards.



Solution Architecture

The solution components connect to a PACS system as shown in solution architecture diagram. CoreStreet FIPS-201 F5 Modules are installed between any existing PACS panel and a supported card or biometric reader. Readers are selected based on assurance level requirements – contactless or contact readers for low and medium assurance level areas and full biometric readers for high assurance areas. Each F5 Module supports one or two readers. All F5 Modules are managed by a CoreStreet FIPS-201 F5 Management Station (F5MS) for centralized control of assurance level settings and distribution of validation data such as card revocations and trusted issuers.

Concept of Operations

The F5 Module validates cards according to the assurance level setting, extracts the badge ID from data on the card, and then passes the badge ID to the PACS panel for an access decision and logging. For invalid cards, the F5 Module is configurable to send a preset badge ID to the PACS panel and/or close an output relay. Cardholder data is captured automatically the first time a card is presented to any F5 reader for validation and then stored and distributed to all other F5 Modules by the F5MS. This feature allows traditional enrollment of cardholders using existing PACS enrollment functionality, integration with an identity management system (IDMS) or card management system (CMS), or use of a third party enrollment package such as visitor software or the CoreStreet FIPS-201 F5 Enroller.

Solution Features and Benefits

- Cards: PIV, TWIC, Legacy CAC, CAC-NG, CAC-EP, PIV-Interoperable
- All TWIC Authentication Modes
- All PIV Authentication Mechanisms
- Inter-agency/Inter-company path discovery and validation (OCSP/SCVP)
- Supports a range of commercially available readers (contactless, contact, PIN, fingerprint)
- Re-uses existing wiring for serial connection to supported readers
- Functions offline if communications with the F5MS is interrupted

Further Information

To learn more about the CoreStreet FIPS-201 F5 Suite of products please reference the F5 Module and F5MS product datasheets found on our website at www.corestreet.com/F5 or contact us.