CORESTREET APPLICATION NOTE

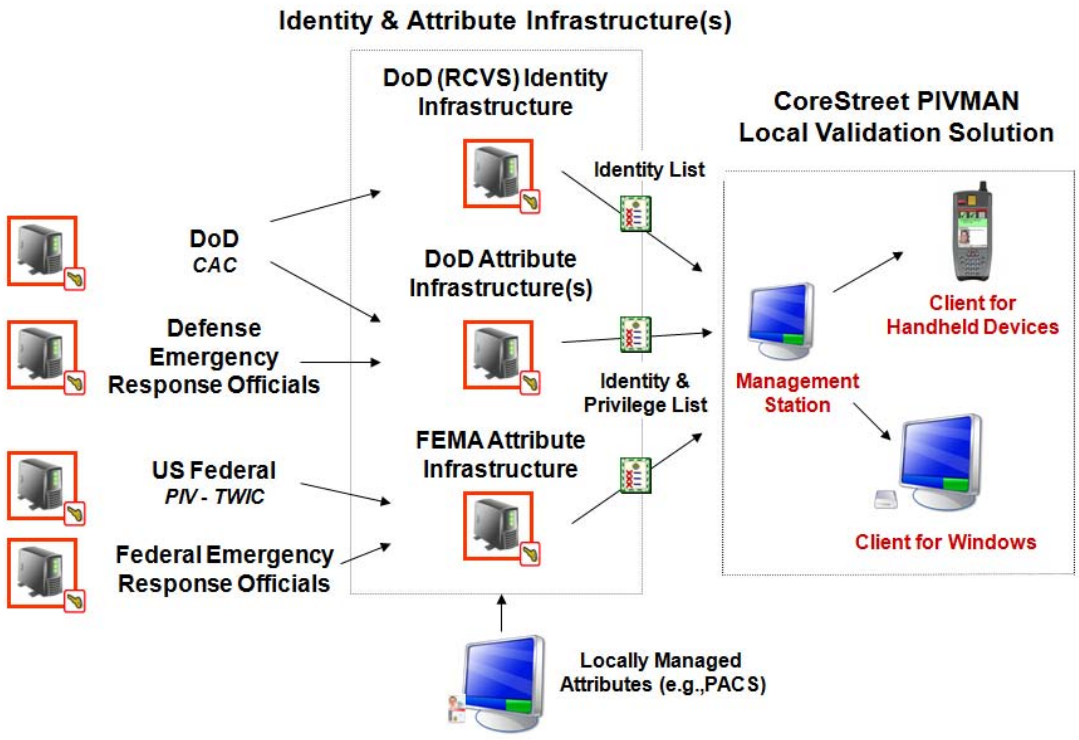
Secure DoD Installation Access with the CoreStreet PIVMAN Solution

Proven Mobile Credential Validation and Authorization Solution Leverages DoD and National Response Framework Architectures

With the full scale deployment of FIPS 201 credentials nearly complete across the US Government, CoreStreet products provide a secure electronic solution to:

- *Validate credentials* including the DoD Common Access Cards (legacy CAC, CAC-NG, CAC-EP), Personal Identity Verification (PIV) cards, Transportation Worker Identification Credentials (TWIC), First Responder Authentication Credentials (FRAC), State-issued Driver Licenses, and/or proximity cards according to FIPS 201, SP 800-116[1], and the TWIC Reader Specifications; and
- *Assign authorizations and privileges* to any credential such as type of access (unescorted or escorted), escort qualifications, responsibilities, emergency response designation, and specific locations as called out in the DoD Interim Policy Guidance for DoD Physical Access Control.[2]

The solution, as shown in the figure below, has two distinct components: 1) Identity and Attribute Infrastructure components that are the trusted source(s) for identity and privilege data and 2) the CoreStreet PIVMAN Solution that validates credentials and displays their privileges based on data from the trusted sources.



[1] NIST Special Publication 800-116, "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)," available at http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf.

[2] DoD Directive-Type Memorandum (DTM) 08-059, "Interim Policy Guidance for DoD Physical Access Control"

The **CoreStreet IPL Publisher** is robust and scalable Identity and Attribute infrastructure software that consolidates existing identity and privilege data for Defense Emergency Response Officials, US Federal PIV cardholders, Federal Emergency Response Officials, local facility physical access control systems (PACS), etc. The CoreStreet IPL Publisher securely stores and distributes credential validation data and assigned authorizations and privileges as a highly compressed, digitally signed identity and privilege list (IPL). In this way, privilege and identity information about millions of cardholders from the DoD and other organizations is readily available.

The **CoreStreet PIVMAN Solution** is a complete local validation solution and consists of CoreStreet PIVMAN Client software running on mobile handheld devices and computer workstations that store identity and privilege data from the trusted sources such as DoD (RCVS), DoD Attribute Infrastructure, FEMA Attribute Infrastructure, and local physical access control systems (PACS). Handhelds running the CoreStreet PIVMAN Client software (PIVMAN Client) quickly validate identity and display privileges to provide security personnel at entry points with information to make an access decision for a wide range of credential populations and card types. All PIVMAN Clients are centrally managed by the CoreStreet PIVMAN Management Station (PIVMS) server software. The PIVMS enables installation commanders and security directors to centrally set authorization and privilege requirements for access to facilities based on factors such as Force Protection Condition, Threat Condition, or Maritime Security Level. PIVMAN Clients also provide authorized operators the ability to change the factors locally on the device.

The PIVMAN clients synchronize automatically with the PIVMS using wired or wireless connections, when such a connection is available, to store all required validation and privilege data locally. This feature allows them to function with or without network connectivity. This mobile capability allows security personnel to perform random anti-terrorism measures (RAMs) as part of roving patrols or to simply validate credentials for access into areas where standard PACS implementations are prohibited (such as, leased or historic facilities). In addition, all PIVMAN Client events are logged and uploaded to the PIVMS during synchronization. These logs are used to create comprehensive activity and after-action reports.

The system can be set to operate at the full range of assurance levels from high assurance, 4-factor authentication of a cardholder to simple ID card scans, or any assurance level in-between, including:

- CAC/PIV FASC-N scan
- CAC/PIV CHUID validation
- Driver License 2D bar code scan
- Driver license magnetic stripe scan
- TWIC CHUID validation
- TWIC Card Authentication Certificate validation
- TWIC CHUID plus Biometric validation
- TWIC Card Authentication Certificate plus Biometric validation
- CAC/PIV Card Certificate validation without PIN Entry
- CAC/PIV Card Certificate plus PIN validation and display of cardholder facial image
- CAC/PIV Card Certificate plus PIN and Fingerprint Biometric validation and display of cardholder facial image
- Proximity (PROX) card scan

The system performs:

- Full validation of the digital certificates representing the cardholder's identity including credential status checks
- Private key validation (ensuring that the card has not been copied or cloned)
- Validation of the certificate(s) used to sign the fingerprint and facial image templates
- On-card cardholder PIN verification (cardholder authentication)
- Biometric verification
- Display of the picture from the contact interface on the card

While attributes are often assigned locally such as in a facility's PACS, DoD and FEMA have been working together to provide a framework for use by local security personnel and incident commanders with the electronic capability to make informed decisions for granting emergency and/or routine access to controlled perimeters. For this effort, FEMA has established a multi-jurisdictional First Responder Trust Model, leveraging existing standards such as HSPD-12 and NIMS Guidance for Identity, National Response Framework ESF codes and NIPP Sector numbers for Attributes, and FIPS-201 for Technology. DoD has worked with FEMA to ensure that Defense-specific attributes are represented within this national framework.

To achieve a standardized Credential & Attribute Validation process, FEMA is standing up an Attribute Infrastructure to support Federal Agency, State, and Local entities. DoD RCVS can be leveraged directly for

CAC validation only requests, or Commands/Services/ Agencies can leverage the attribute infrastructure currently supporting the Pentagon Force Protection Agency (PFPA).

The benefits of this complete solution include:

- Validation – Immediate validation of identity and attributes even in power out and network down situations
- Privacy – Organizations maintain attribute information separately and locally while leveraging information on the credential to confirm identity, thus eliminating the requirement for large centralized identity databases
- Auditing – Audit information captured locally and available for post-mortem reviews
- Always Up-to-date – Automatic updates occur when a connection is available
- FIPS 201 Interoperable – Validation of any Federal, State, Local credentials issued from FIPS 201 compliant or interoperable infrastructure

CoreStreet PIVMAN Suite Overview

The CoreStreet PIVMAN Solution is a proven mobile identity verification solution for CAC and PIV credentials, as well as FRAC and TWIC cards. The solution is operational even in power out and network down environments, supports Windows-based handheld devices from multiple vendors as well as PCs, and leverages existing DoD and FEMA infrastructures.

The solution has been tested in server DHS FEMA disaster simulations and has also been deployed in support of programs within numerous Federal agencies, both defense and intelligence, as well as civilian and state first responder initiatives. The CoreStreet PIVMAN Solution is on the FIPS-201 Approved Products List and is reimbursable under several DHS grant programs.

Solutions in the CoreStreet PIVMAN Suite include:

- CoreStreet PIVMAN for TWIC Solution - consists of a stand-alone portable TWIC reader running the CoreStreet PIVMAN Client software. The device is able to read the TWIC card and uses the TSA TWIC hotlist to determine if the TWIC is still valid. Supported handheld devices currently include:

  - o Cross Match Technologies Be.U Mobile SMC800
  - o Datastrip DSV2+TURBO
  - o MaxID iDLMax
  - o Motorola MC70
  - o Roper Mobile Technologies DAP CE3240B / BWE

- CoreStreet PIVMAN Solution - is a more comprehensive solution that adds in support for other standard credentials such as CAC, PIV, FRAC, drivers' licenses and provides a robust management and reporting suite. The CoreStreet PIVMAN Solution allows customers to tap into $1B+ Federal government investment in its credentialing programs to determine validity and access rights.

- CoreStreet PIVMAN for Lenel Solution - expands the system capabilities to allow Lenel users to have CoreStreet PIVMAN Client devices automatically synchronize with OnGuard for centralized management, monitoring, and reporting. CoreStreet PIVMAN for Lenel also allows the reader operator to see privileges from OnGuard (access levels) displayed on the screen. This functionality allows a relying party to determine not only if a TWIC is valid, but also if the cardholder has the access rights specific for the local facility.

Product Information

To learn more about the CoreStreet PIVMAN Suite of products that are available to implement the solutions that will address your specific mobile ID verification requirements, contact us or visit the our website at: www.corestreet.com/pivman