



**Unified PACS with PKI Authentication, to Assist US
Government Agencies in Compliance with NIST SP 800-116
(HSPD-12) in a Trusted FICAM Platform**

In Partnership with:



Introduction

Monitor Dynamics (Monitor) is working with several US Military locations on a physical access control system (PACS) that is compliant with the NIST SP800-116 exclusion access controls capabilities using 3-factor authentication. The effort is a net-new install but can also be used when a location is instructed to remove the existing PACS.

As these installations are considered the flagship for the organization that Monitor is working with, successful deployment of the new Unified PACS with PKI Authentication will guide future installs at similar sites.

Monitor has been successfully providing integrated, high-security PACS solutions to Federal Government Agencies and the Department of Defense since 1979. It has partnered with CoreStreet, Certipath and Veridt, to deliver an industry leading, best-in-class partnership that can deliver a complete solution to any and all US Government agencies or DoD bases needing to comply with FIPS 201 and NIST SP 800-116 as it relates to physical access control systems. We have labeled this unified solution as the High Assurance, Trusted FICAM Platform.

To deliver a complete, end-to-end systems solution, Monitor has the training, certifications, capabilities and past performance necessary to be the prime Systems Integrator for the entire unified PACS, which will include CoreStreet F5 hardware, the Monitor Dynamics SAFEnet PACS management platform, Certipath PKI authentication and Veridt readers.

The combined team offers decades of systems expertise, market leading delivery capabilities, a thorough understanding of all of the policies and standards by which the solution will be measured and the ability to scale and grow the solution to meet future safety, security and identity needs as mandated by the United States Government.

The Team Approach

The team's approach to PIV enabling a PACS is shown in Figure 1 below. In this approach, the PIV enabling functionality is added by augmenting the existing door controller and panel functionality.

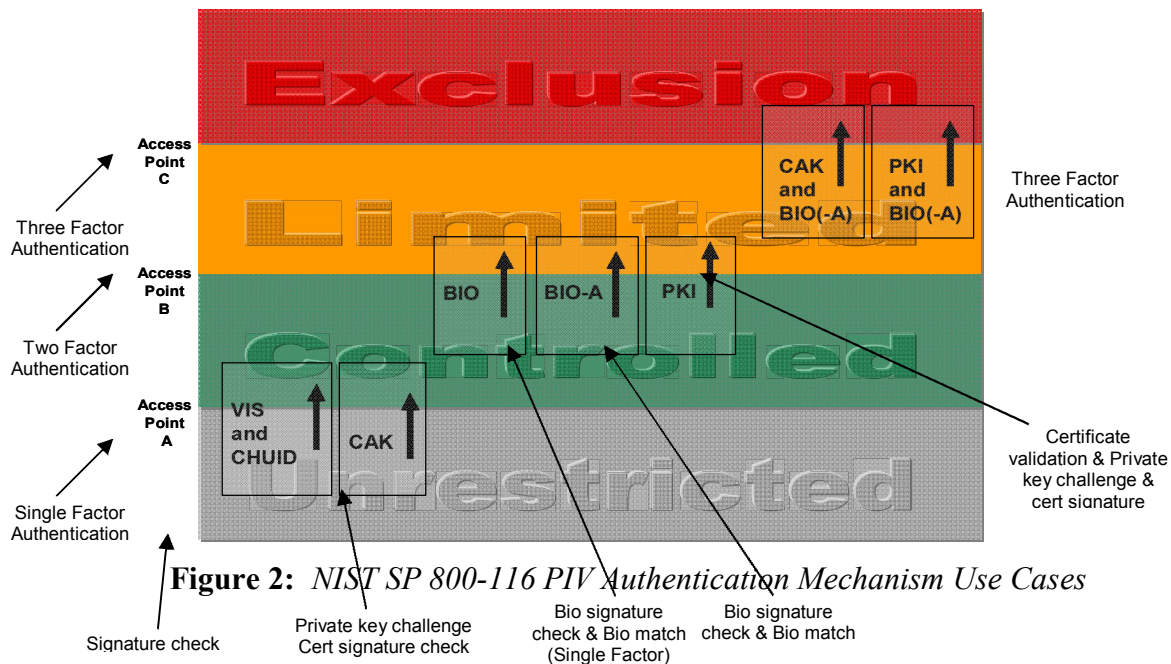
It requires two changes: replacing existing card readers with PIV enabled readers and inserting a CoreStreet FIPS-201 F5 Module between the reader and the door controller. The F5 Module contains all the PKI validation functions executed at the time-of-access.

into a standard file format for bulk upload into the Monitor Dynamics SAFEnet PACS. The F5 provides seamless integration with SAFEnet PACS management platform, which automates the synchronization of cardholder records between the F5 System and the SAFEnet PACS.

Once cards are enrolled, the F5 Modules validate cards according to its assurance level setting, construct the badge ID from data on the card and then passes the badge ID to the SAFEnet PACS panel for an access decision. The SAFEnet PACS head-end maintains the user access authorizations as is currently done. For invalid cards, the F5 Module can be configured to send a preset badge ID to the SAFEnet PACS panel and/or close an output relay.

Cardholder data is captured automatically the first time a card is presented for access and then stored at the F5MS. Please note that what is captured is the certificate. Once the signature has been checked and the cert chains to a trusted root, the public key is stored so that the next time the card is presented, the certificate does not need to be read, the signature checked nor the chain validation performed. Of course, a private key challenge is done at this point. This happens even if the card is not enrolled. To gain access the card must be enrolled and on the F5 Access Control List (FACL). This feature allows traditional enrollment of cardholders using existing PACS enrollment functionality, integration with an identity management system (IDMS) or use of a third party enrollment package such as visitor software or the FIPS-201 PACS Enroller.

A prerequisite for planning and implementing a solution to PIV enable a PACS is to determine just how much security is required and where. NIST's Special Publication 800-116 provides excellent guidance in answering this question. Figure 2 below is taken from this document and shows the recommended segmentation of access control points in terms of security based risks.



In the diagram above, the unrestricted area is considered public with no restrictions as to who has access. Access to the Controlled area is restricted to those who can prove affiliation. For example, possession of an Agency's badge could be sufficient to gain access at an outer perimeter of a facility. Access to the Limited area is restricted to members of a group who are fulfilling a specific role. Finally, access to the Exclusion area is restricted by individual authorization, analogous to the "need-to-know" requirement in the classified world.

SP 800-116 defines and describes the authentication methods shown in Figure 2. The PIV card is designed to support each of these methods which are intended to provide different levels of assurance of the identity of the user. Which authentication method should be used depends upon the security requirements at the point of access. As stated previously, the F5 System supports the implementation of all of these authentication modes.

Features and Benefits

The team's Unified PACS with PKI Authentication approach enables an agency to PIV enable their existing PACS system in a cost effective and secure manner that meets all of the previously defined criteria:

- **Maximizes reuse** – the solution can minimize cost by augmenting the capability of existing panels and door controllers and requires no changes to the existing system other than adding PIV compatible readers.
- **Minimizes custom modifications** – the solution does not require any custom modifications to existing PACS components. Future upgrades to the existing PACS can be done without requiring any custom modifications.
- **Supports certified PACS** – although SAFEnet is the recommended system, meeting all necessary certifications and criteria, the solution is PACS make and model independent, as long as the right certifications and capabilities are in place.
- **Supports multiple authentication mechanisms** – the solution provides dynamically configurable support for all authentication mechanisms defined in SP 800-116 (CHUID, CAK, PKI, BIO and combinations).
- **Supports PIV-I** – the F5 solution supports a variety of identity credentials in use today, including PIV, PIV-I, TWIC, FRAC and CAC (legacy, NG, EP). All four TWIC authentication modes as defined in the TWIC reader specification are supported. The solution also provides support for using the GUID from the PIV-I as the cardholder identifier.
- **Improves security** – the Solution provides a complete PKI validation approach to support strong authentication of the card holder. This includes configurable periodic status checking via OCSP, CRL or TWIC hot list and validation of contractor and visitor identities via certificate path discovery and validation through the Federal Bridge.

The F5 supports multiple authentication mechanisms in accordance with NIST SP800-116 and the defined TWIC authentication modes. A summary of these modes and the protections provided by the implementation of each is provided in the figure below.

Auth Modes ↓	Secures against cards that are				Auth Factors	SP800-116 Security Area	TWIC Auth Mode
	Counterfeit or Altered	Revoked	Copied or Cloned	Lost or Stolen			
FASC-N		✓				Uncontrolled	1
CHUID+VIS	✓	✓			1	Controlled	1
CAK	✓	✓	✓		1	Controlled	2
CHUID+BIO	✓	✓		✓	2	Limited	3
PKI+PIN	✓	✓	✓	✓	2	Limited	N/A
CAK+BIO	✓	✓	✓	✓	2	N/A	4
PKI+PIN+BIO	✓	✓	✓	✓	3	Exclusion	N/A

Please note that a CHUID signature check at enrollment does not secure against counterfeit or altered cards being used at the time-of-access and is only for uncontrolled areas per SP800-116.

The F5 Solution enables the SAFEnet PACS to validate any FIPS-compliant card making them enterprise-centric.

Monitor Dynamics – SAFEnet PACS Overview

Monitor Dynamics is the manufacturer of the SAFEnet Physical Access Control System. Monitor is also capable of acting as the prime Systems Integration services provider that will support delivery, project management, installation, acceptance testing, training and ongoing maintenance of the SAFEnet PACS system.

Monitor's SAFEnet solution has set the standard for Government access control and intrusion detection/alarm management, since its introduction in 1979. Monitor Dynamics was the pioneer in Government security and remains the leader in high-security applications. The company has remained at the forefront for over thirty years with assistance from Government Security Managers. These Government security forces have in a sense been the Product Manager for SAFEnet, and provided the hundreds of customized requirements necessary to keep SAFEnet as the most feature rich and scalable physical access control system to date. The end result is that

SAFEnet is capable of meeting the complete customization needs of all Government and DoD organizations, yesterday, today and in the future.

SAFEnet was designed as an open-architecture and backwards compatible system to make sure it will always remain the perfect investment for Government applications. Investing in SAFEnet and in Professional Integration and Maintenance services from the Monitor Dynamics team assures that your people, facilities and assets will be secure, remain secure and be capable of changing to meet the demands of a dynamic Government Security mandates, identity requirements and integrated third party application purchases.

SAFEnet - Physical Access Control System Specifications

SAFEnet utilizes the power and security of the Microsoft operating system. The system's operational database, Microsoft SQL Server, provides complete SQL structures, functions and report generation. It offers the most flexible yet simple-to-use relational database features while providing standard ODBC interface capabilities for easy data importing and exporting with external third-party systems.

SAFEnet is an integrated security management system designed for easy control and administration of complex, large-scale, multi-site security management requirements. SAFEnet gives Government Security Professionals comprehensive and integrated tools to do their jobs more effectively and efficiently.

SAFEnet incorporates access control, alarm management, video surveillance and video recording all into a seamlessly integrated platform. SAFEnet software incorporates an easy-to-use graphical user interface (GUI) with simple point-and-click database editing and system monitoring controls. It utilizes the power and standardization in the Government of the Microsoft® Windows® operating system. The system's operational database, Microsoft® SQL Server, provides complete SQL structures, functions and dynamic, real-time report generation. It offers the most flexible yet simple-to-use relational database features while providing standard ODBC interface capabilities for easy data importing and exporting with external third-party systems.

SAFEnet enables users to make bulk database changes. It eliminates tedious and time-consuming manual editing of large numbers of records without requiring the user to learn the SQL programming language. It allows custom unlimited customer card holder information to be added to the database; enabling the user to create their own display screens, incorporate user memo fields, format data, adjust font and color control and define drop boxes. The customizable Badging System has a dossier feature used to display certain user information. The system can be configured to provide simple local access control and alarm monitoring, or it can be expanded to meet the high security needs of mission critical applications on wide area networks.

SAFEnet can be configured for single-user or multiuser systems with full-featured operator workstations on commercially available LAN/WAN backbones. The modular design and scalable architecture is configured for security management systems ranging from medium sized facilities to large-scale multi-site, high-end security applications.

Trusted FICAM Platform - Response to PACS System Requirements

The following sections are based on sample requirements from existing clients.

Credentials

The solution set supports all of the required, and locally optional, card formats specified, including:

- DoD CAC – all variants
- Federally issued PIV credentials
- Transportation Worker Identification Credential (TWIC)
- First Responder Authentication Credential (FRAC) for approved mutual aid responders
- PIV Interoperable (PIV-I) credentials for Non-Federal Issuers

Populations

The solution set will easily support the quantity, transaction volume, and types of access credentials identified for either a stand-alone or enterprise-level PACS for Regular and Visitor Access. The Guest Access paper badges do not provide a credential interface that is electronically readable by this system.

Scalability

The solution set can easily be scaled to support the stated growth anticipated for the system from as small as 8 doors and ~700 individuals initially, to subsequent registration exceeding 1,300 individuals on an 8 door system, to over 2,000 doors and over 4,000 individuals within a single building. This scalability is easily supported by both the F5 components and the SAFEnet PACS. SAFEnet supports over 4096 cardreaders per server and more than one million card holders.

Regarding the mix of Controlled and Limited areas and Exclusion areas, there is no limitation on the number of access points or authentication modes that can be supported by the system. The performance of authentication at one door does not impact the performance or authentication mode at other doors as the access requirements are defined for each door, and managed centrally, via the F5 Management Station. Growth to support peak loads of ~4,000 transactions per shift change is also easily supported. Entry and exit access controls, by FPCON level and tap, respectively, is also configurable in the F5 Management Station and fully supported today.

Roles and Responsibilities

SAFEnet incorporates security access control, alarm management, video badging, personnel administration, video and audio monitoring and recording, all into a seamlessly unified platform.

In most Government organizations, the security landscape is continuously changing. Moreover, security risks and Government security mandates continue to evolve and change. Selecting and implementing the right technologies in the appropriate design and function is critical to securing people, facilities and assets effectively. As more complex, fully-integrated systems become necessary, the time required in the delivery process grows significantly, as does the need for experienced professionals to run large projects efficiently.

Monitor Dynamics' Certified Professionals have specific experience and training in all facets of the security industry and bring knowledge of current security technologies, the latest updates and newest modules to Monitor Dynamics manufactured systems and overall industry best practices. With Monitor Dynamics Certified experts engaged on specific security projects, your organization's in-house staff can stay focused on direct objectives while security installations take place, on time and on budget.

On every project, Monitor Dynamics thoroughly examines each facility, its threats and its vulnerabilities, and designs a customized, best practices-based security solution to fit the risk profile. Monitor Dynamics consultants work closely with internal Security and Information Technology teams to understand an organization's exact security needs, network requirements, building designs and security plans. Our goal is to assist clients in selecting the most appropriate solutions, manage projects through to completion, and provide ongoing maintenance, support and training, to maximize productivity throughout the lifecycle of the system.

For every project, Monitor Dynamics is the single point of contact for managed services, field installation and warranty maintenance. Through this arrangement, our customers benefit from the overall project management provided by Monitor Dynamics and the specific security solutions knowledge that our Certified Professionals offer. Monitor Dynamics can also engage existing "client-preferred" installation companies for the project, at the request of the client, for inclusion into all projects as sub contractors. Monitor Dynamics is also capable of utilizing security technologies from multiple vendors and manufacturers for high level custom integrated security projects, like those commonly found in an enterprise government environment.

Registration to PACS

The solution set fully supports the validation of each credential as part of the registration process of loading the cardholder information into the F5 System. As part of each registration, the system is checked to prevent duplicate registrations of the Unique Person ID related to the credential type. The system will support multiple credentials for an individual based on status changes (e.g., leave military and become a contractor).

Unique Person ID

For DoD CAC, the unique Person ID shall be the EDIPI or the UPN. The offeror shall explain their selection and why it is a best fit to this installation.

For non-CAC credentials, the offeror shall provide a unique Person ID solution. The offeror may consider:

- For Federally issued PIV credentials -- use of FASC-N's Agency Code concatenated with the PI field
- For other credentials – Use of the DN within the PIV Auth Certificate
- For PIV-I credentials – the F5 Solution will be configured to extract a unique Person ID for use as the badge ID from the Universal Unique Identifier (UUID) embedded in the PIV Auth Certificate. The system provides the ability to configure the size of the badge ID to match the capabilities of the PACS head end being used.

Unique Credential Numbers

The solution set currently supports the FASC-N and the UUID in accord with NIST SP800-73-3. For DoD CAC credentials, the 16 digits extracted from the FASC-N fields of Agency Code, System Code, Credential Number, Individual Issue Code, Credential Series are concatenated to form the unique credential number.

For Federally issued PIV credentials the 14 digits extracted from the FASC-N fields of Agency Code, System Code, and Credential Number are concatenated to form the unique credential number. This includes FRAC and TWIC credentials.

For NFI credentials such as PIV-I, the F5 System supports the determination of the UUID based on SP800-73-3. This capability was demonstrated at Exostar for the CertiPath demo. To differentiate between a PIV vs PIV-I credential, the F5 System evaluates the Agency Code, and if it is found to contain all 9's, then the UUID from the GUID is used. Additionally, the F5 System can configure the size of the UUID based badge ID requirements of the PACS head-end software. For example, the 128 bits of the UUID is too large to be accommodated by most PACS headends. Therefore, the F5 System utilizes a 64 bit subfield as the identifier. So, if the PACS can only handle a 56 bit badge ID, the F5 System provides the option to configure the system to truncate the 64 bit field to fit into 56 bits.

Biometrics

The F5 Solution is configurable to require 1:1 biometric verification of an individual against the fingerprint biometric stored in the PIN-protected PIV container of the contact chip. After PIN verification, the container is opened, a private key challenge is issued to the card to prove that the certificate (and public key) that has been validated and is therefore trusted is indeed bound to the card to which it was issued and not copied onto a different card. Upon successful completion of this challenge, the digital signature protecting the signed objects in the container (facial image and fingerprint biometrics) is validated prior to those objects being made available for use. If

any of these validation steps fails, then the credential is not trusted for access and the transaction is aborted. Please note that there is no central store of these biometric templates.

While not part of the offered solution for this effort, CoreStreet has worked with Global Rainmaker LLC to integrate the F5 System with their IrisGate offering. This integration validates the individual's credential, parses the FASCN, and passes the FASCN to IrisGate for an indexed lookup of the stored iris template to the image captured as the individual approached the reader.

This same approach can easily be integrated with other biometric modalities assuming a Weigand interface exists to those reader(s). These types of integrations are the recommended approach for persons without usable fingerprint biometrics.

The High Assurance, Trusted FICAM Platform integrates third party products such as biometrics and video surveillance via SAFEnet. SAFEnet unifies security point products, systems and subsystems into a command and control management platform. It delivers an open architecture environment that adapts each individual application and device into its platform - promoting global collaboration as ONE system.

The open architecture design of the SAFEnet system is coupled with an emphasis on emerging technologies for high security facilities, plants, ports, airports and other critical infrastructure resources. These designs are implemented to provide port security forces with the capability to "See First, Understand First, and Act First", in relationship to operational and situational awareness.

Access Management

SAFEnet is an integrated security management system designed for easy control, reporting and administration of complex, large-scale, multi-site security management requirements. SAFEnet gives Government Security Professionals comprehensive and integrated management tools to do their jobs more effectively and efficiently.

The system supports updates to custom selection lists even while editing, allows user record recycling, and accommodates unique requirements on PIN numbers and special fields such as Social Security Numbers.

Force Protection Condition (FPCON) Levels

The solution set is capable of supporting multiple FPCON level authentication modes. Currently, the system provides centralized management of authentication modes only through the F5 Management Station. Through an integration effort that is currently underway, this capability is being enhanced to allow the PACS head-end to centrally update these modes. As available today, the admin would effect the authentication mode switch from a central F5 Management Station for each of the readers under its control, without the need to physically touch each reader.

The Veridt MultiMode reader, in combination with the F5 board and firmware to be deployed for the PACS, is capable of supporting all threat level authentication modes.

Access levels

The Veridt MultiMode reader, in combination with the F5 board and firmware to be deployed for the PACS, is capable of supporting all the authentication modes specified in NIST SP800-116. Configuration for each reader's authentication mode is performed via the F5 Management Station.

Specifically, the system can be configured to meet the access levels requirements specified in the SOW, as follows:

1. One factor - Signed CHUID (contact or contactless)
2. One factor - CAK (contact or contactless)
3. Two factor - PKI+PIN (contact)
4. Three factor - PKI+PIN+Biometric (contact)

The SAFEnet PACS supports 64,000 access control classes and 999 access control levels

Workflow

The access system shall provide workflow tools to assist in managing (but not limited to):

- Registration (both centralized at the security office and decentralized at local administrator)
- Visitor registration for offsite visitors
- Time and schedule management
- Group management
- Data integration and import and export
- Approval cycles
- Revocation cycles
- Certificate validation and verification services
- Locally developed workflows

PKI integration

The F5 Solution implements both the PKI integration specified in the GSA Federated PACS Specification v1.0 as well as all of the authentication modes found within NIST SP800-116. The certificate validation processes support the use of CRLs, OCSP, and SCVP, as appropriate, for the validation of all credentials both as they are registered in the system as well as at scheduled intervals to ensure that only valid credentials may be used to access a facility.

Registration

The enrollment process ensures that no credential is registered to the PACS that does not pass full path discovery and validation of the PKI credentials.

Keys Required

The F5 Solution supports the following PKI credentials as selected by the Security Administrator to support an appropriate threat condition and access requirement:

- Card Authentication Key (CAK)
- PIV Authentication Key (PAK)

For older CAC cards, the Identification Key can be used in place of the PAK.

Related to the protection of the data being communicated between the components, we use symmetric keys to encrypt our data channels to and from the F5 Management Station. The PACS elements also use symmetric keys for encryption of their channels. These keys are generated by the system.

Modes of Authentication

The following modes of authentication are supported by the F5 System:

- Contact and Contactless Signed CHUID. Upon validation of PKI credentials and digital signature on the CHUID, the Unique Credential Number is transmitted. However, the system can only be configured to use the contact or contactless interface, at the exclusion of the other interface. The requirement as stated is being considered for a feature enhancement but no timeframe has been established for the delivery of this capability. Performance: Transaction less than 1 second is supported.
- Contact and contactless CAK (PKI). Upon validation of PKI credentials and challenge response, the Unique Credential Number is transmitted. However, the system can only be configured to use the contact or contactless interface, at the exclusion of the other interface. The requirement as stated is being considered for a feature enhancement but no timeframe has been established for the delivery of this capability. Performance: Transaction time less than 2 seconds is supported, which is measured after the card is acquired by the reader as this acquisition process depends on how the user presents the card.
- Contact PIV Authentication (PKI+PIN). Upon validation of PKI credentials and challenge response, the Unique Credential Number is transmitted. Performance: Transaction time less than 2 seconds (after PIN entry) is supported.
- Contact PIV Authentication + Biometric. Upon validation of PKI credentials and challenge response, the biometric template is read off the card, its digital signature validated, and then the biometric is compared to a local sample. Upon validation, the Unique Credential Number is transmitted. Performance: Transaction time less than 2 seconds (after PIN entry and biometric sample) is supported. Additionally, CoreStreet is currently working with DMDC on a new protocol that can be used to improve physical access performance of multiple authentication factor transaction times to less than one second.

With the exception of the biometric match, all the security relevant functions are performed on the secure side of the door. F5 Modules do all the credential validation processing and are installed on the secure side, typically in the same tamper protected enclosure as the PACS panels. The readers are used as transparent readers.

Service Levels and Training

The SAFEnet PACS will stay up in the event of a building power loss for a minimum of 24 hours. Components will fail gracefully and stay operational in the event of segmented power or system losses. This system will be operational 7x24x365. System will have one year installation and hardware warranty.

Warranty repairs for failed hardware or software will be within 72 hours of failure. The team will provide technical telephone support 24x7 for one year with no charge to the customer. The team will provide full and complete system training for operations and maintenance prior to certification for operational use and acceptance.