monitordynamics

Unified PACS with PKI Authentication, to Assist US Government Agencies in Compliance with NIST SP 800-116, FIPS 201 and OMB M 11-11 in a High Assurance Trusted FICAM Platform

TrustedFICAM PLATFORM
IDENTITY MANAGEMENT

In Partnership with:

CertiPath

HID®

4 I B I F
INNOVATIVE PKI AWARD WINNER
TrustedFICAM PLATFORM IDENTITY MANAGEMENT

TrustedFICAM PLATFORM IDENTITY MANAGEMENT
PLATINUM AWARD WINNER
Security Products
GOVIES
2012 Government Security Awards
ACCESS CONTROL

GSA APL CERTIFIED

SECURITY UL® LISTED

The Leader in Unified Access and Intrusion

12500 Network Blvd., Suite 303 • San Antonio, TX 78249 • P: (210) 477-5400 • F: (210) 477-5401 www.mondyn.com

Introduction

Monitor Dynamics (MonDyn) has implemented the Trusted FICAM Platform (Platform) at numerous US Military and Federal Government Agency locations as a PIV/I enabled physical access control system (PACS) with full PKI authentication. This PKI-based PACS platform is compliant with the NIST SP800-116 exclusion access controls capabilities using 3-factor authentication. These platform implementations are primarily net-new installs but can also be implemented seamlessly when a location is instructed to remove the existing PACS due to lack of capabilities or non-compliance with mandated HSPD-12 requirements.

These installations, which have implemented and are running the Platform, are considered flagships for those forward-thinking, security conscious government organizations that MonDyn is working with. Successful deployment of the Trusted FICAM PACS with PKI-based Authentication will guide future installs at similar sites.

MonDyn has been successfully providing integrated, high-security PACS solutions to Federal Government Agencies and the Department of Defense since 1979. It has partnered with HID and numerous other GSA APL Approved hardware manufacturers to offer an industry leading, best-in-class product Platform that delivers a complete solution to any and all US Government agencies or DoD facilities requiring FIPS 201, HSPD-12, NIST SP 800-116 and OMB M 11-11 compliance as it relates to physical access control systems reading PIV/I in Government. MonDyn has branded this FIPS-201 compliant, unified PACS solution as the Trusted FICAM Platform.

The FICAM Platform supports a host of additional software modules that include but are not limited to; video surveillance, intrusion detection, time and attendance, biometric identity and automated smart card enrollment. An example of the time and attendance module, which was developed for organizations with security guards on location, is provided at the end of this whitepaper. The time and attendance module can be customized based on specific site, regional or enterprise requirements by the customer, or used out-of-the-box with standard features. The module integrates with the Monitor Dynamics FICAM Platform, to deliver a completely FIPS-201 compliant system to the end user. This solution can be installed and operated at an unlimited number of sites, with top-down management and bottom-up reporting capabilities throughout.

A mobile hand-held identity verification capability branded as SpotCheck, manufactured by MonDyn, is also available as part of the Platform. SpotCheck allows for multi-factor mobile PIV/I and all smart card validation and is perfect for gate entrances requiring ID verification for every individual within an entering automobile.

To deliver a complete, end-to-end systems solution, MonDyn has the training, certifications, capabilities and past performance necessary to design, test and implement the entire unified PACS, which will include authentication and validation hardware and software along with the Monitor Dynamics SAFEnet PACS management platform and (two or) three factor certified and approved readers.

The MonDyn 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.

12500 Network Blvd., Suite 303 • San Antonio, TX 78249 • P: (210) 477-5400 • F: (210) 477-5401 www.mondyn.com

Monitor Dynamic's Trusted FICAM Platform has recently received multiple prestigious industry-wide awards for capabilities and innovation. It received the Govies Platinum Award for Best Access Control System in the Government Security Market. The Govies Award is sponsored by the GovSec Conference and Security Products Magazine. The second award, sponsored by the Four Bridges Forum (4BF) is for the most innovative uses of Public Key Infrastructure (PKI) and the PKI Bridge serving the United States Federal Government.

The 4BF Awards recognize innovative uses of high assurance digital identities in the public and private sectors. The 4BF is a coalition of the nation's leading federated identity trust hubs, which joined forces to facilitate trusted electronic business transactions across major Federal Agencies, U.S.-based Pharmaceutical and Healthcare industries, Aerospace, Defense, Colleges and Universities. These organizations utilize the 4BF member trust hubs to ensure the integrity of on-line transactions, reduce identity misrepresentation and lower costs associated with identity management. Each member trust hub asserts the identity of participants across the entire federation.

The Government Security Awards (Govies) are sponsored by the GovSec Security Conference and Security Products Magazine. Security Products Magazine is the leading product specific publication in the global security marketplace, providing new product and technology information and solutions for security professionals. GovSec is the world's leading forum for securing our homeland against 21st century threats and preparing for national security emergencies. The Govies Awards honor outstanding government products in a variety of categories and are coveted by manufacturers around the globe and recognized as industry standards for professionals using the technology. The Trusted FICAM Platform, by being recognized as the Platinum Award winner, has set the standard for High-Security Access Control Systems in Government.

The Team Approach

The MonDyn team's approach to PIV/I enabling a PACS is shown in Figure 1 below. In this approach, the PIV/I enabling functionality is added by augmenting the existing door controller and panel functionality. This requires two changes: replacing existing card readers with PIV/I enabled readers and inserting an HID FIPS-201 PAM (pivCLASS Authentication Module) between the reader and the door controller. The PAM Module contains all the PKI validation functions executed at the time-of-access.

12500 Network Blvd., Suite 303 • San Antonio, TX 78249 • P: (210) 477-5400 • F: (210) 477-5401 www.mondyn.com

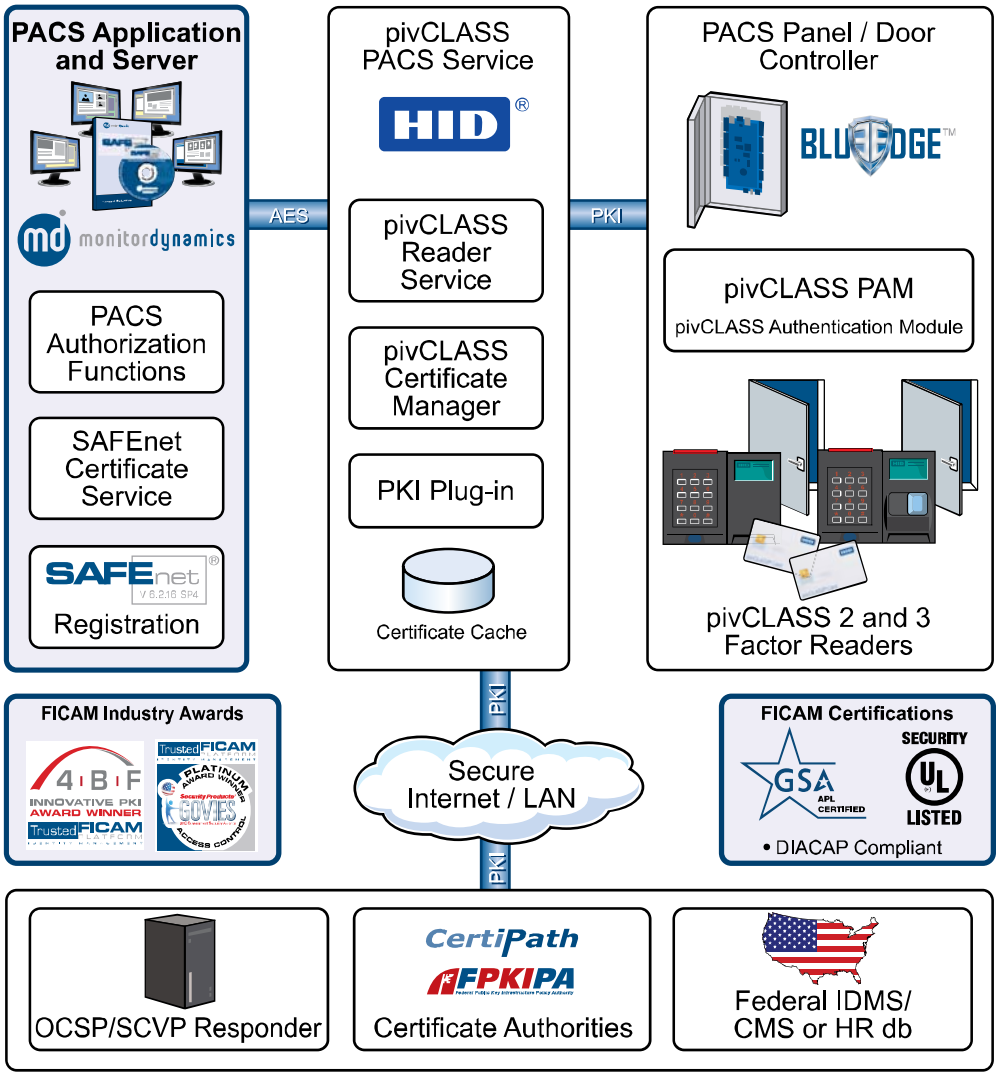


Figure 1: *PIV Enabled PACS using the Panel Augmentation Approach*

Inserting the PAM Module requires no modification or replacement of any non-reader component in an existing PACS. It provides all the validation functionality required by FIPS 201 in compliance with HSPD-12. PAM Modules are installed between any existing PACS panel and any number of supported reader types: contact card-only, contactless card-only, contact and contactless card-only, card + PIN, card + bio or card + PIN + bio. Reader types are selected based on assurance level requirements. The PAM Module-reader combination supports Signed CHUID, CAK, PKI+PIN, and PKI+PIN+BIO authentication methods as described in SP 800-116. Each PAM Module can support one or two readers.

PAM Modules are managed by a FIPS-201 Validation Server that provides centralized control of assurance level settings and distribution of dynamic validation data such as credential revocations and trusted issuers. The Validation Server is also used to efficiently push firmware updates to PAM Modules if firmware updates become necessary to address new or changing Government standards.

The PAM Enroller is a client application that is used to validate and register PIV cards for use with the PAM System. Once cards are enrolled at the PAM Enroller, cardholder records can be exported into a standard file format for bulk upload into the Monitor Dynamics SAFEnet PACS. The PAM provides seamless integration with SAFEnet PACS management platform, which automates the synchronization of cardholder records between the PAM System and the SAFEnet PACS.

Once cards are enrolled, the PAM 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 PAM 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 Validation Server. 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 PAM Access Control List (ACL). This feature allows traditional enrollment of cardholders using existing PACS enrollment functionality, unification with an identity management system (IDMS) or use of a third party enrollment package such as visitor software or the FIPS-201 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.

12500 Network Blvd., Suite 303 • San Antonio, TX 78249 • P: (210) 477-5400 • F: (210) 477-5401 www.mondyn.com

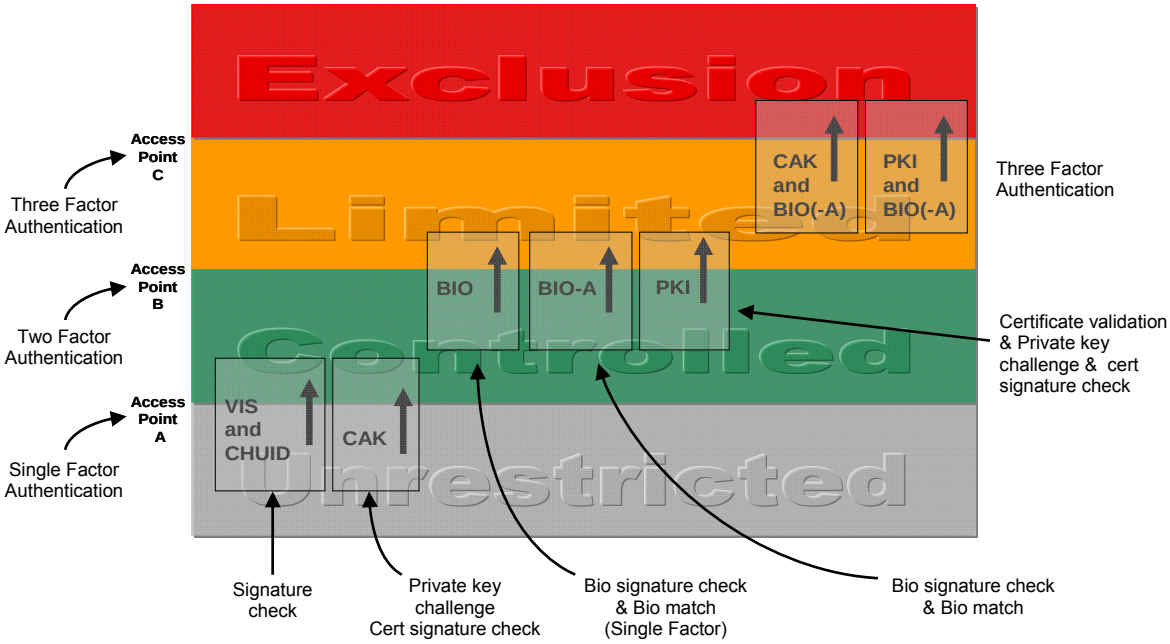


Figure 2: *NIST SP 800-116 PIV Authentication Mechanism Use Cases*

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.

NIST 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 Platform 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/I enable their organization 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/I 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** – SAFEnet is the recommended PACS system, meeting all necessary certifications and criteria; however the complete 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 SAFEnet PIV/PKI Solution supports a variety of identity credentials in use today, including PIV, PIV-I, TWIC, FRAC, CIV 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 PAM 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.

Meet Any Assurance Level			Secures against cards that are...				
Security Area (per NIST SP800-116 & Risk Assessment)	Authentication Factors	Authentication Modes	Revoked	Counterfeit or Altered	Copied or Cloned	Lost or Stolen	Shared
Uncontrolled	None	FASC-N	✓				
Controlled	1	CHUID + VIS	✓	✓			
Controlled	1	CAK	✓	✓	✓		
Limited	2	PIV + PIN	✓	✓	✓	✓	
Exclusion	3	PIV + PIN + BIO	✓	✓	✓	✓	✓

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 NIST SP 800-116.

12500 Network Blvd., Suite 303 • San Antonio, TX 78249 • P: (210) 477-5400 • F: (210) 477-5401 www.mondyn.com

The Platform's PIV/PKI Solution enables the SAFEnet PACS to validate any FIPS-compliant card making them enterprise-centric.

Monitor Dynamics – Trusted FICAM Platform: PACS Overview

Monitor Dynamics is the manufacturer of the SAFEnet Physical Access Control System within the Platform. Monitor is capable of supporting design, delivery, project management, field engineering, acceptance testing, training and technical maintenance of the SAFEnet PACS system.

MonDyn'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, with an off-the-shelf modular platform.

SAFEnet was designed as an open-architecture and backwards compatible system to ensure it will always remain the perfect investment for Government applications. Investing in SAFEnet and in Professional Engineering and Support 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.

The SAFEnet platform delivers a centralized unified security management solution for installations of all sizes. Individual applications can be unified into the platform as optional standalone modules or can be deployed as a customized unified end-to-end security solution. The SAFEnet platform seamlessly unifies all of the critical components necessary to manage and monitor multi-site facilities including access control, intrusion detection, identity management and video surveillance. The platform is built using a robust open architecture model that meets the performance demands of mission critical infrastructure applications running across multiple systems and locations.

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.

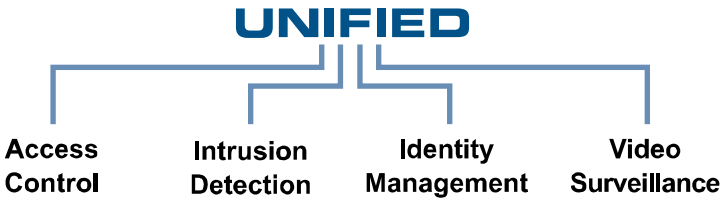
SAFEnet is an integrated security management system designed for easy control and administration of complex, large-scale, multi-site security management requirements. SAFEnet gives Government Security Professionals comprehensive and integrated tools to do their jobs more effectively and efficiently.

SAFEnet incorporates access control, intrusion detection, video surveillance and identity management all into a seamlessly unified 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.



The Trusted FICAM Platform - Response to PACS System Requirements

The Trusted FICAM Platform (Federated Identity Credential and Access Management) is a military-grade high assurance PACS (Physical Access Control) System delivering end-to-end trust by leveraging PKI-based identity credentials, across the PKI Bridge Infrastructure in a unified approach to physical access control. The Platform utilizes PKI credentials that are resistant to fraud, meet federal standards, minimize risk and protect critical assets while simultaneously complying with a broad range of identity mandates driven by HSPD-12 such as FIPS-201, DTM 09-012 and OMB M 11-11.

The Platform's support for and validation of PKI technology, deployed in a bridged environment, forms the core of the PACS system's trust model for PIV and PIV-I credentials. This extension of the highest assurance ID forms and the ability to validate them across the trust infrastructure at a card reader mounted beside a door delivers performance similar to a standard transparent PACS card reader while utilizing a cryptographic challenge/response for increased security.

This "PKI at the Reader" structure can be combined with biometric authentication, which ties the credential to the holder, adding to the high assurance and non-transferability of the credential. The Trusted FICAM Platform is aimed at an audience wishing to support PIV, CAC and PIV-I with full support for validation across the US Federal Bridge, managed by CetiPath. The platform also has support for locally validated credentials such as

CIV, FRAC and TWIC. It was the first access control system on the market to pass the stringent CertiPath Trusted PACS Certification. It is currently on the CertiPath Certified Products List (CPL) as a compliant PACS system utilizing FIPS-201 approved components and was chosen by CertiPath as the test platform for certification of all PIV-I credential issuers. The Platform acts as the "lock" through which all entrants must pass and ensures that PIV-I credential "keys" work while meeting all required identity and facility security mandates. With the Platform in place, the Federated One Badge concept becomes a reality for disparate organizations.

The Platform's authorized credential holders can use a single enterprise issued, digitally certified smartcard badge to enter the building. That same badge is used to securely log on to their personal workstation or laptop. The platform's support for PKI provides critical capabilities never before available in a PACS system.

Utilizing the power of the platform, user are able to:

- Know if the credential has been revoked in near real time
- Know if the issuer or any other authority serving as basis for trust in a credential has been revoked
- Rely on a visitor's own credentials and to receive near real time status information as to the visitor's current company affiliation. This is a key differentiator for the Government PACS market.

The Trusted FICAM Platform was the first and is currently the only government industry PACS system reading PIV-I utilizing FIPS 201 approved three-factor authentication readers (smart card, biometric and PIN number) in a live Department of Defense operating environment. It has been deployed to numerous Federal Government Agencies and DoD sites across the nation.

In addition to its PACS capabilities, the Trusted FICAM Platform unifies intrusion detection, video surveillance and identity management into a centralized command and control dashboard environment with global management and reporting functionality.

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 HID 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 Validation Server. 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 Validation Server and fully supported today.

Roles and Responsibilities

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.

MonDyn's 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 MonDyn manufactured systems and overall industry best practices. With MonDyn 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.

MonDyn 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. MonDyn's 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, MonDyn is the single point of contact for product specific information. Through this arrangement, our customers benefit from the overall product engineering provided by MonDyn and the specific security solutions knowledge that our Certified Professionals offer. MonDyn is also capable of utilizing security technologies from multiple vendors and manufacturers into the Platform for high level custom Unified 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 PAM 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 SAFEnet PIV/PKI 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 PAM System supports the determination of the UUID based on SP800-73-3. To differentiate between a PIV vs. PIV-I credential, the PAM 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 PAM 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 head-ends. Therefore, the PAM System utilizes a 64 bit subfield as the identifier. So, if the PACS can only handle a 56 bit badge ID, the PAM System provides the option to configure the system to truncate the 64 bit field to fit into 56 bits.

Biometrics

The Biometrics 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.

The High Assurance, Trusted FICAM Platform unifies third party products such as biometrics and video surveillance via SAFEnet. SAFEnet unifies security point products, systems and subsystems into a central 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 a unified security management system designed for centralized global control, reporting and administration. 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 Validation Server. 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 affect the authentication mode switch from a central Validation Server for each of the readers under its control, without the need to physically touch each reader.

The FIPS-201 approved readers, in combination with the PAM Module and firmware to be deployed for the PACS, is capable of supporting all threat level authentication modes.

Access levels

The FIPS-201 approved readers, in combination with the PAM Module 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 Validation Server.

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 Trusted FICAM Platform implements "PKI @ the Reader" using 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.

12500 Network Blvd., Suite 303 • San Antonio, TX 78249 • P: (210) 477-5400 • F: (210) 477-5401 www.mondyn.com

Keys Required

The Trusted FICAM Platform 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 Validation Server. 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 PAM 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, ActivIdentity 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. PAM 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.

SAFEnet PACS Time & Attendance Module

The Monitor Dynamics SAFEnet PACS system is a COTS (commercial off-the-shelf) system, with a variety of modules that can be plugged into the system to deliver a host of complimentary solutions, many of which can be customized to fit the special or unique requirements necessary for large Government-wide systems and to comply with specific security mandates. One of these modules is the SAFEnet Time & Attendence module.

This time and attendance module can be customized based on specific requirements by the customer, or used out-of-the-box with standard features. The module integrates with the Monitor Dynamics FICAM Platform, to deliver a completely FIPS-201 compliant system to the end user. This solution can be installed and operated at an unlimited number of sites, with top-down management and bottom-up reporting capabilities throughout.

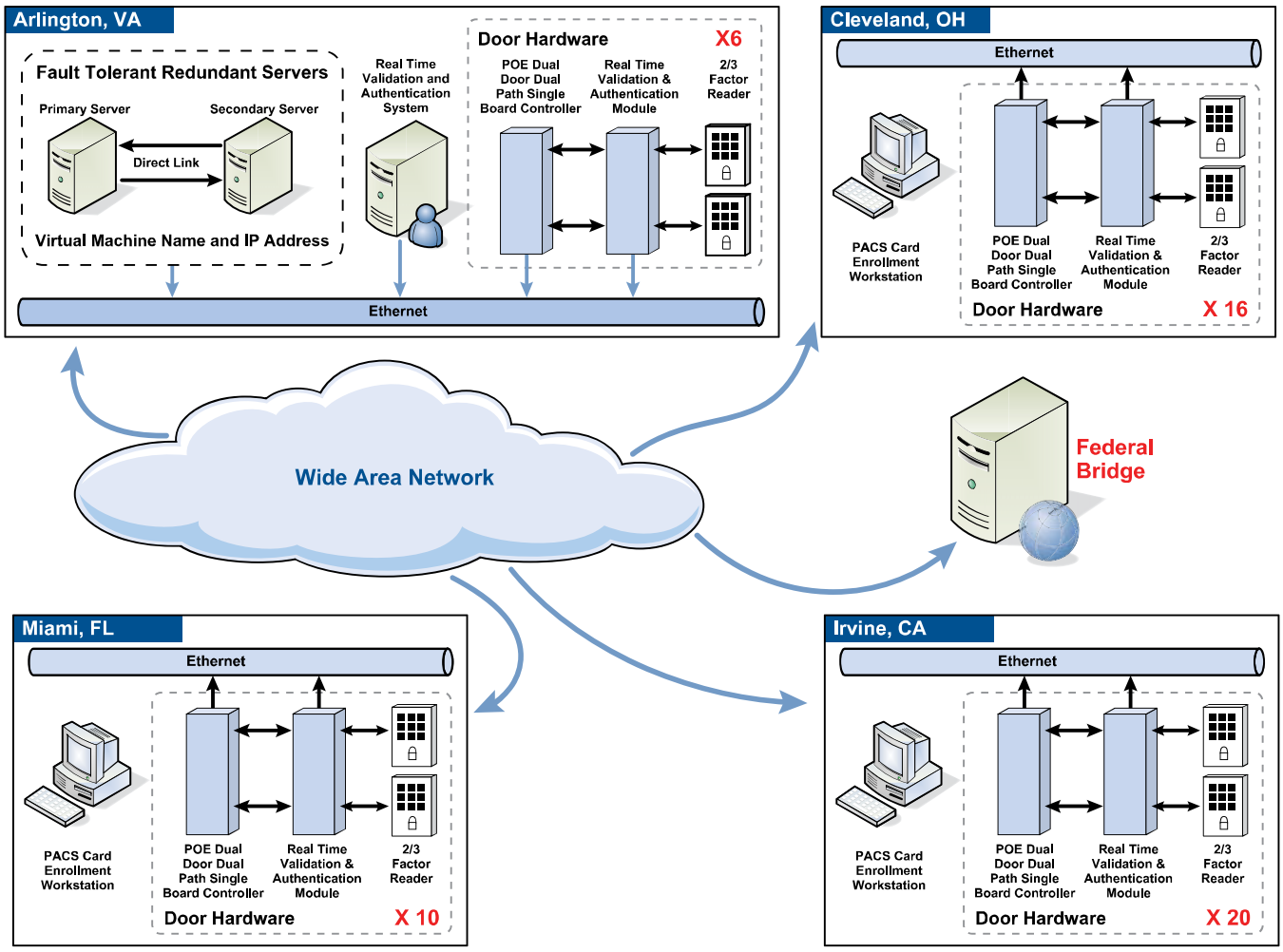
The SAFEnet time and attendance module utilizes the power of smart card technology as the identifying factor for all employees (or contractors, etc.). By utilizing the biometric, over the high-assurance PKI infrastructure of the FICAM Platform, an end user is guaranteed the validity of the employee that is clocking in and clocking out. The SAFEnet time and attendance module gives Security Managers the ability to administer local schedules, as well as enterprise schedules across the organization. The central management capability of the FICAM Platform enables Security Officers to manage all schedules, whether enterprise-wide or local, from one central point of command and control.

The software module provides a list of pre-populated reports and also contains a customer reporting engine that allows the Security Manager to create custom reports as needed. It is designed to synchronize with third-party IP based time and attendance clocking devices, or other sanctioned external time sources within the organization.

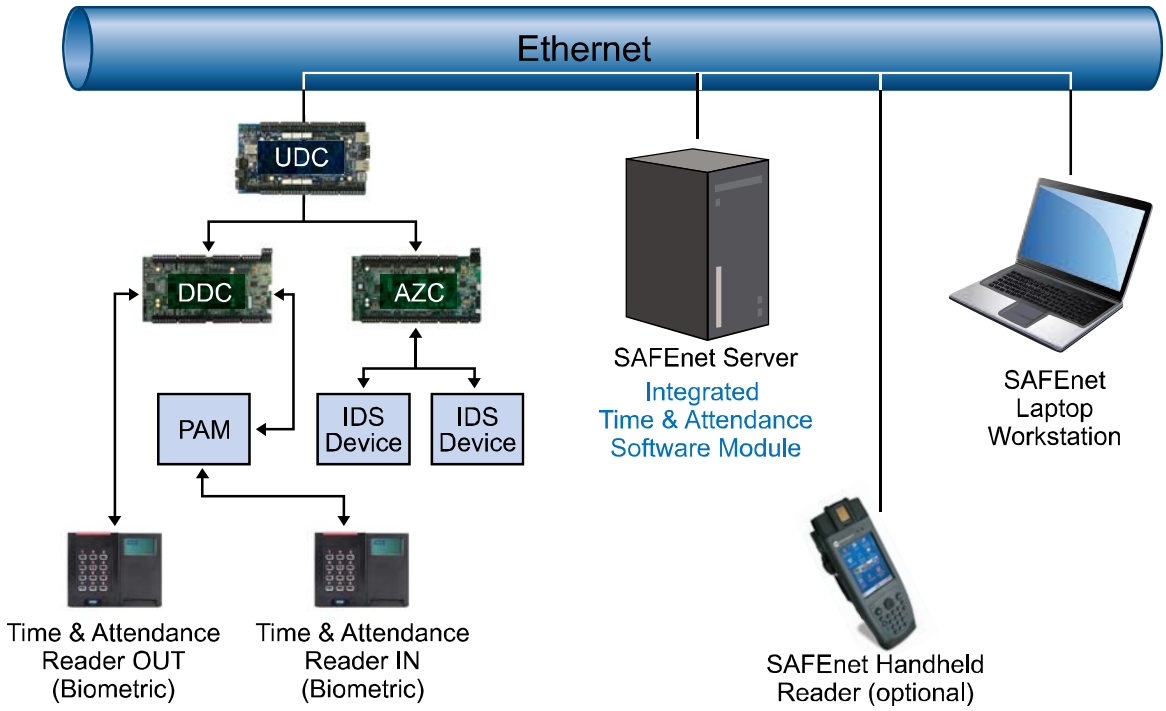
The system provides a snapshot of the status of each employee. At any given point in time, a Security Manager can identify who is present in a certain location, and who is not. Holiday scheduling is another key feature. When an employee or contractor does not comply with their work schedule, which includes either not clocking in on time or not clocking out on as scheduled, the system has the ability to automatically notify the Supervisor in charge. This alert can be tuned as needed by each location and is sent via email or SMS notification.

12500 Network Blvd., Suite 303 • San Antonio, TX 78249 • P: (210) 477-5400 • F: (210) 477-5401 www.mondyn.com

Sample System Site Diagrams:



Sample System Site Diagrams *(continued):*



Glossary for Diagram Above:

UDC – Unified Digital Controller. Part of the BlueEdge Intelligent Control Equipment line offering dual IP with POE+ power and zero degraded mode stand-alone operation for access and intrusion.

DDC – Dual Door Controller board, part of the IDC hardware suite.

AZC – Alarm Zone Controller board.

PAM– GSA APL Approved Board which transmits and receives FIPS-201 compliant communications.

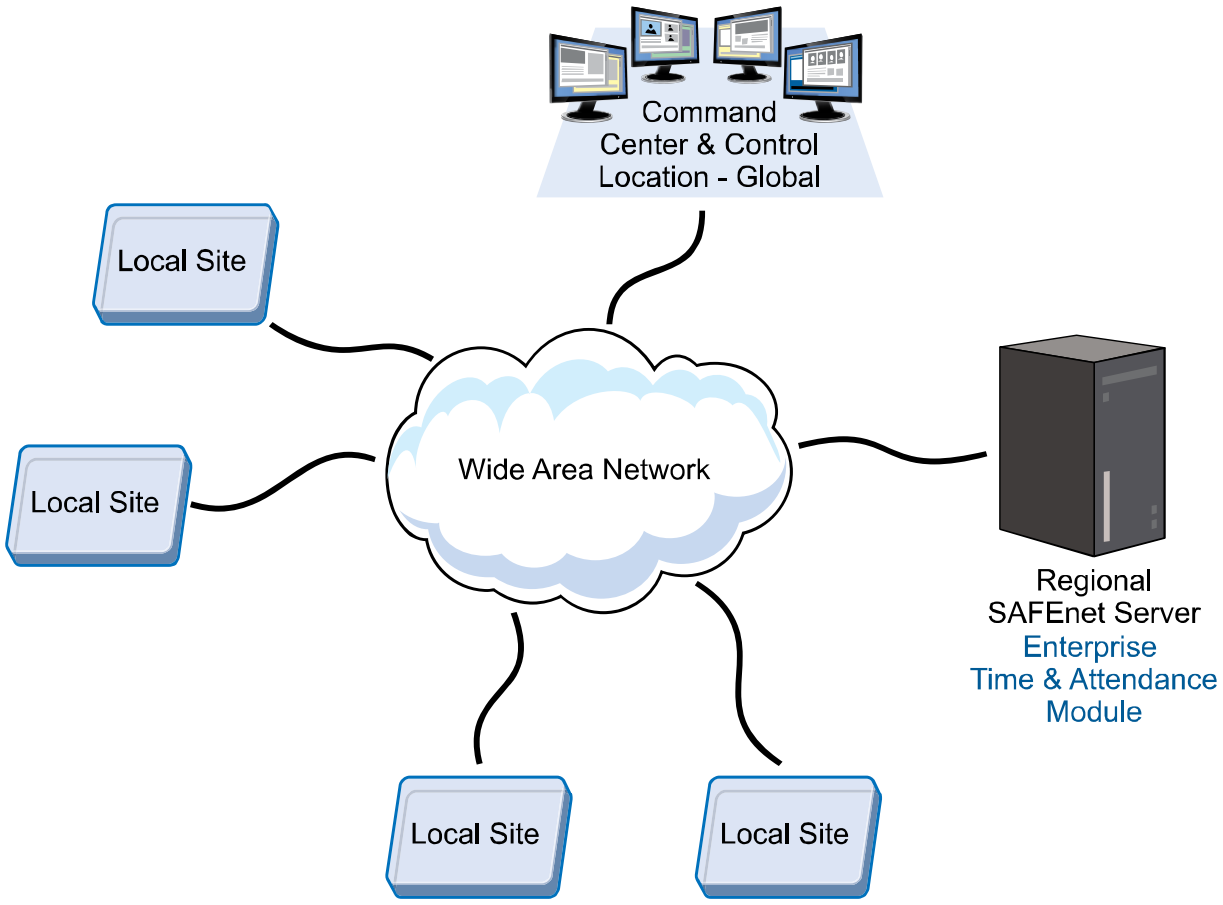
IDS Device – Alarm points being monitored.

SAFEnet Server – Primary site server for head-end PACS software and associated modules.

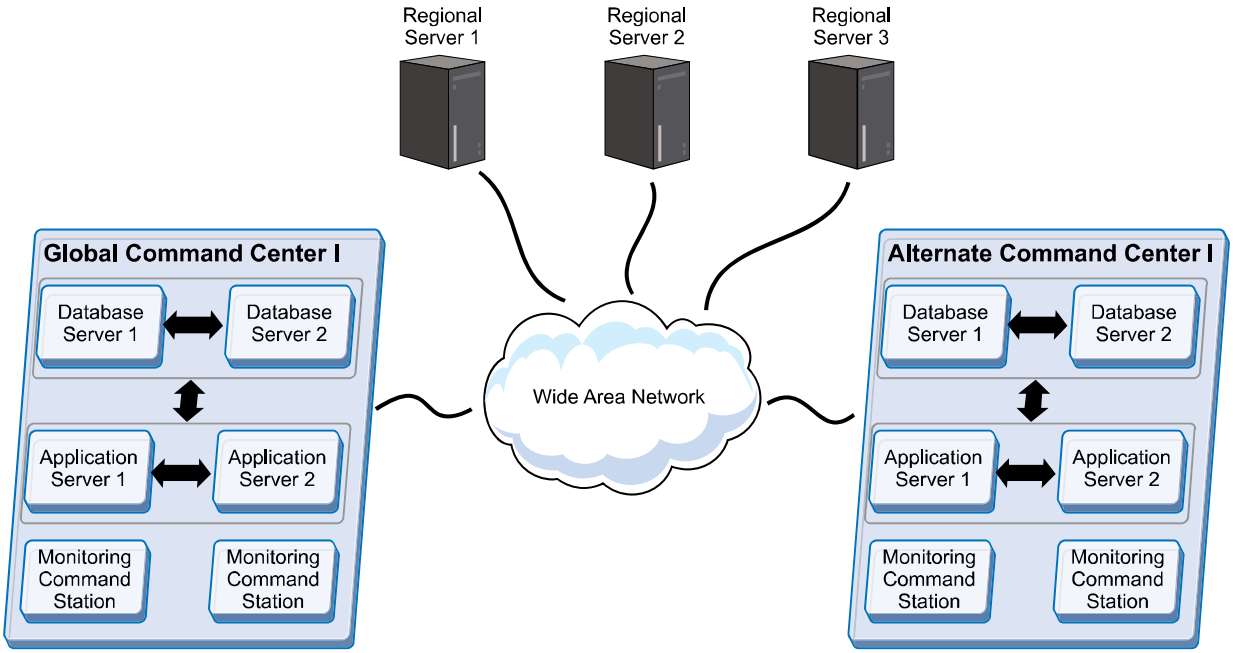
SAFEnet Workstation – Computer used by administrators to perform daily system functions.

SAFEnet Handheld Reader – Optional wireless identity readers for use by mobile guards or guard personnel at front gate.

Sample Regional System Connection Diagram:



Sample Command Center with Optional Alternate Command Center Diagram:



Contact Information

For additional information on the Trusted FICAM Platform or any additional Monitor Dynamics product solutions, please contact the Monitor Dynamics Marketing Department at 210-477-5400. You may also email your request to info@mondyn.com for a prompt reply.

monitordynamics

Trusted FICAM PLATFORM
IDENTITY MANAGEMENT

GSA APL Certified - DIACAP Compliant - UL Listed

FIPS-201 Approved PACS Platform

SAFEnet (GSA Certified Validation System and PACS Infrastructure)

- Uses HID FIPS 201 SDK
- FIPS 140 Level 1
- PD-VAL, OCSP or SCVP client
- Nonce generation
- Signature verification
- Hash computing
- Identifier cross-checking
- Unified Access Intrusion & Video Management

pivCLASS PACS Service (Validation component)

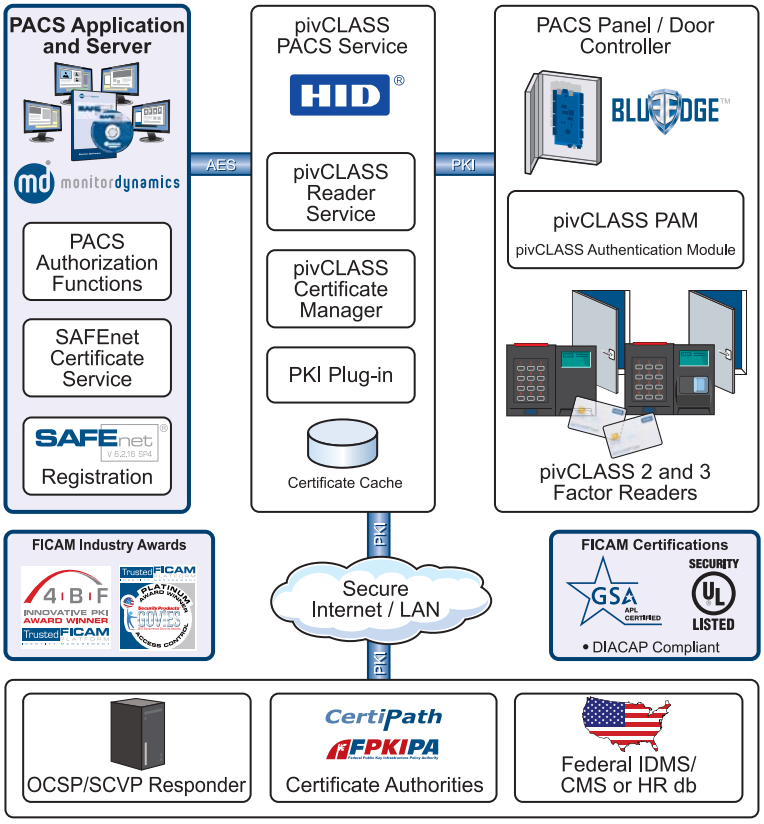
- Manages registration engines
- Manages PACS plug-in(s)
- Manages certificate cache
- Manages reader services
- Manages Certificate Mgr
- Manages IDPublisher
- Manages audit logs
- Manages debug/ diagnostic logs

pivCLASS PACS Plug-in (PACS Infrastructure component)

- Maps PIV/PIV-I credential data elements to PACS database fields for provisioning/de-provisioning as well as activating and deactivating PACS credential records
- System Communication

PKI Plug-in (Validation System component)

- FIPS 140-2 Level 1
- PD-VAL, OCSP or SCVP client
- Nonce generation
- Signature verification
- Hash computing



Path Builder OCSP/SCVP Responder (Validation System component)

- FIPS 140-2 Level 2 (with HSM)
- FIPS 140-2 Level 1 (default)
- PD-VAL, OCSP client to CAs
- OCSP, SCVP server
- Signing
- Hash computing

pivCLASS Certificate Manager (Validation System and PACS Infrastructure component)

- Deactivates (de-provisions) credentials in PACS based on:
  - PD-VAL results
  - Activates credentials when certificate revocation status transitions from unknown to known.

pivCLASS PAM Secure Controller (Validation System and PACS Infrastructure component)

- FIPS 140-2 Level 1
- Nonce generation
- Signed nonce verification
- Hash computing
- Identifier cross-checking
- Outputs identifier to panel
- Monitors LED and buzzer lines from panel
- Sends LCD prompts to reader
- Sends LED color changes to reader
- Sends beep commands to reader

pivCLASS 2 and 3 Factor Readers (FICAM Reader category)

- Passes APDUs between PAM and smart card
- Passes responses to APDUs back to PAM
- Displays LCD prompts generated by PAM
- Varies LED color, based on commands from PAM
- Supports CAK, PKI + PIN, PKI + BIO

pivCLASS Reader Service (Validation System component)

- FIPS 140 Level 1
- Manages PAM configuration
- Manages PAM cache
- Extracts PAM logs

The Monitor Dynamics® Trusted FICAM Platform™: Utilizing HID® pivCLASS®

The Trusted FICAM Platform is a military-grade high assurance Physical Access Control System that delivers end-to-end trust by leveraging PKI-based identity credentials, across a secure PKI Bridge Infrastructure, in a unified approach to physical access control. The Platform utilizes PKI credentials that are resistant to fraud, meet federal standards, minimize risk and protect critical assets while simultaneously complying with a broad range of identity mandates driven by HSPD-12 such as FIPS-201, DTM 09-012 and OMB M-11-11.

www.monitordynamics.com

monitordynamics

12500 Network Blvd. • Suite 303 • San Antonio, TX 78249-3307
Tel: 210-477-5400 • Fax: 210-477-5401 • Toll-free: 866-435-7634