

The Importance and Challenges of FICAM Compliance

Abstract

When managing an unexpected event, risk, or disaster, it should be simple to verify who was in a building or location. This is where identity management comes into play, streamlining the process of confirming people are who they say they are. In 2004, the United States federal government issued a directive requiring all agencies to develop and deploy a credential system. The objective was to create a government-wide standard for secure, reliable forms of identification to be issued to all federal government workers and contractors.

At the time, concerns surrounding potential attacks were quite prevalent among all federal organizations. The U.S. government identified irregularities in the quality and security of the identification systems being used to gain access to secure facilities. From this directive, the U.S. government established its own Identity, Credential, and Access Management (ICAM) strategy, known as FICAM, or Federal ICAM. This white paper analyzes the importance of FICAM, its key constituents, and the role of physical access control systems (PACS) in helping federal organizations maintain FICAM compliance.

Introduction

Initially published in 2009, the Federal Identity, Credential, and Access Management (FICAM) regulations provide a common set of standards, best practices, and implementation guidelines for U.S. federal agencies and the contractors who work with them. FICAM compliance is top of mind of all federal security personnel, with questions including:

- Am I protecting my facility well enough?
- Am I allowing the right people into my building?
- Am I removing “bad actors” from my security systems in a timely fashion?
- Can someone clone my security credentials?
- Can I trust other government credentials?
- Will other government credentials work with my security system?
- Is the person carrying the credential really who they say they are?

In order to answer these questions, any organization working with the U.S. federal government must establish and maintain a FICAM-compliant environment to enable trust. As a result, organizations rely on authentication methods and secure access to physical and logical information, requiring planning, subject matter experts, architecture enhancements, and massive amounts of policy review and adherence.



This white paper discusses in detail the importance of FICAM compliance and how organizations can adhere to FICAM regulations through physical access control systems (PACS).

Problem Statement

The Homeland Security Presidential Directive-12 (HSPD12) mandates the establishment of a government-wide standard for identity credentials for federal employees and contractors to improve physical security in federally controlled facilities.

In February 2005, the Department of Commerce and the National Institute of Standards and Technology (NIST) released the required standard as Federal Information Processing Standards Publication (FIPS) 201 - Personal Identity Verification (PIV) of Federal Employees and Contractors. The current version is [FIPS 201-3](#), dated January 2022. The required smart card-based credential is called the PIV card, which uses microprocessor-based smart card technology. It is designed to be counterfeit-resistant, tamper-resistant, and interoperable across federal government facilities.

In February 2011, the Office of Management and Budget (OMB) released a memo stating that existing PACS must be upgraded to use PIV credentials before the agency could use development and technology funds to complete other activities. As of today, the issuance of PIV credentials is almost complete. Federal agencies are now paying attention to identifying and implementing changes to their PACS to support a PIV card. This memo also required agency PACS transition plans to be in accordance with FICAM.

The FIPS 201-based PIV credentialing program has been in place for nearly two decades along with several PACS added to various facilities around the world. As the PIV credentialing process matured, the PACS remained the same and did not perform secure authentication methods for the PIV creden-

tials. The PACS hardware architecture performance was primarily based on very small credential payloads (i.e., 26-bit) and was unable to securely process the PIV smart card containers, which contained much larger amounts of data.

Most of these legacy PACS are now in the process of being replaced with today's advanced crypto-based processors and bi-directional card readers and systems using industry protocols such as Open Supervisory Data Protocol (OSDP) and Online Certificate Status Protocol (OCSP). Therefore, FICAM's end-users can start authenticating the PIV tokens with the simple addition of a validation engine, scheduling certificate status checks, and enabling near real-time disabling of revoked PIV credentials.

Background

FICAM is the federal government's implementation of Identity, Credential, and Access Management (ICAM). ICAM is the set of tools, policies, and systems an agency uses to enable the right individual to access the right resource, at the right time, for the right reason in support of federal business objectives.

Agencies implement ICAM services and solutions to unify their IT services, improve physical access control, and improve information security and decisions. Understanding the building blocks of ICAM is key to understanding the FICAM Architecture, which includes government-wide enterprise architecture views with the flexibility to support each agency's unique business or mission requirements. Using the FICAM Architecture as a tool allows agencies to perpetually improve upon their approach and align with federal security and privacy initiatives.

In other words, FICAM is the federal government's enterprise approach to design, plan, and execute common ICAM processes. The FICAM Architecture is a framework for an agency to use in the ICAM program and solution roadmap planning. The FICAM Architecture focuses on enterprise identity processes, practices, policies, and information security disciplines. A federal enterprise identity is the unique representation of an employee, contractor, or enterprise user, which could be a mission or business partner, or even a device or technology managed by a federal agency to achieve its mission and business goals.

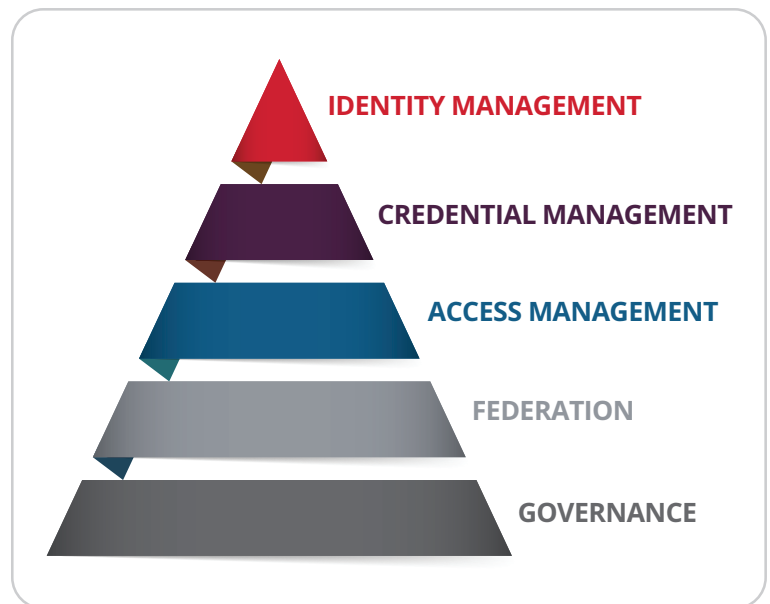
The FICAM Architecture is for agency personnel. An enterprise architecture is primarily used by:

- Senior federal IT and agency stakeholders to understand the concepts for identity and access management services and the basic use cases supporting business objectives

- Program managers to find common definitions and frameworks for use in planning
- Enterprise and application architects to use a common framework for designing and governing IT systems, applications, and implementations

FICAM Implementation

Implementation of FICAM consists of five practice areas.



1. Identity Management

Identity management is how an organization handles the identities of federal government employees, contractors, and authorized partners, not customers or members of the public. Identities will consist of a variety of attributes, such as name, contact information, and job title. An identifier for an individual must be a unique attribute and could be an assigned PIV card/number.

2. Credential Management

Credential management is how an agency issues, manages, and revokes credentials linked to specific identities. A credential is a data structure that authoritatively confirms the identity of an individual. Unlike identities, credentials can expire or be modified as necessary.

3. Access Management

Access management is how an agency authenticates enterprise identities and authorizes appropriate access to protected services. The level of required authentication most often depends on the importance of the secured resource or facility.

Authentication procedures can be as simple as having an individual self-assert an identifier or as complex as having an individual present both a physical token, such as a PIV card, and biometric information, such as fingerprints.

4. Federation

Federation is the technology, policies, standards, and processes that allow an agency to accept digital identities, attributes, and credentials managed by other agencies. To achieve federation, separate organizations must align their ICAM policies to ensure interoperability.

Organizations have to share proofing confirmations amongst each other when possible to reduce the burden on people to submit identification data to multiple organizations to access federal government resources. Appropriate consent and privacy protections should always be in effect.

5. Governance

Governance is the set of practices and systems that guides ICAM functions, activities, and outcomes. Data analytics is critical to this practice area. Real-time monitoring and periodic audits should be used to ensure employees and contractors only access resources they need. Improper access permissions should be corrected as quickly as possible. Policies should also be regularly reviewed to ensure compliance with the latest updates to FICAM standards.

Goals and Objectives of FICAM

There are three main goals of FICAM, each with its own set of objectives. The goals are aspirational statements designed for senior government leaders, agency executives, and agency ICAM program leadership responsible for setting program strategy. The objectives are action areas where agencies can develop execution strategies, action plans, and performance metrics based on alignment with the mission needs.

Goal 1

Modernize security policies and solutions to make risk-based decisions, automate identity and access management processes, and move access protections closer to government data.

- Review, update, and maintain comprehensive ICAM policies and technology solution roadmaps to inform and enforce enterprise strategic planning, risk management, and modernization.
- Adopt and use cloud-ready systems that provide an efficient and secure way to access resources.
- Monitor and respond to user behavior and events by using data as a strategic asset to make adaptive and risk-based decisions.

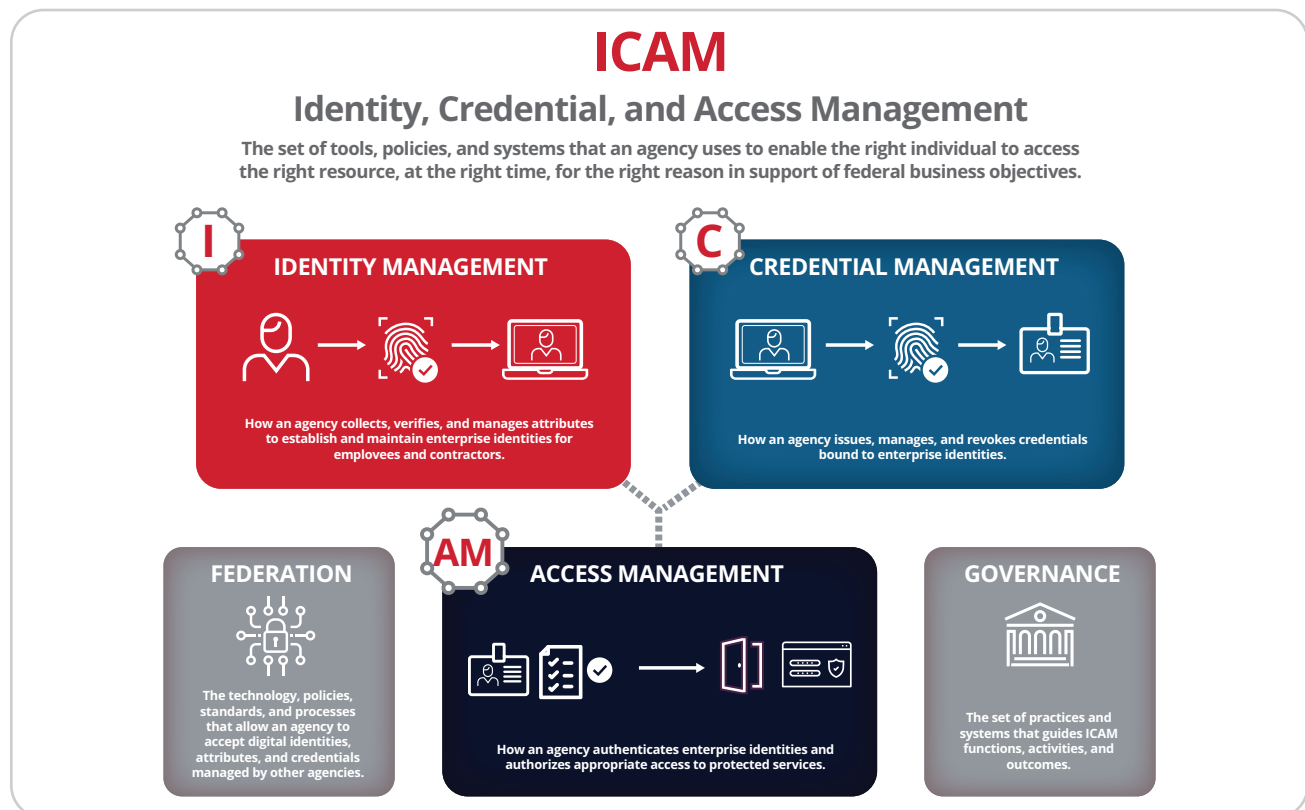


Figure 1. A high-level view of the ICAM practice areas

Goal 2

Enable missions to efficiently deliver services to federal and contractor employees and resources.

- Establish and manage identities for all enterprise users and resources.
- Design enterprise solutions to manage access to information and resources.
- Utilize enterprise identity information discovery and enterprise centralized access management.
- Leverage federated solutions to accept identity and authentication assertions made by other agencies and mission partners when efficient.

Goal 3

Provide enterprise-level solutions within agencies to improve operations and promote cost-effective and efficient use of resources.

- Streamline ICAM governance and program management within each agency to optimize execution, ensure consistency, and align intent across the enterprise.
- Evaluate, rationalize, and migrate to modern, cloud-smart solutions for ICAM services.
- Promote interoperability and efficiency across the federal government by buying and building ICAM solutions that use open, commercially adopted standards.

What Is a FICAM PACS?

At a high level, a PACS is a collection of technologies that control physical access at one or more federal agency sites by electronically authenticating employees, contractors, and visitors. Within the federal government, compliant PACS solutions are made up of three distinct components:

1. Infrastructure

The PACS Infrastructure is composed of many compatible and interoperable software and hardware components that may include the software application and server (head-end), database, panels, door controllers, and a workstation.

The PACS Infrastructure typically interoperates with Intrusion Detection Systems (IDS), Video Management Systems (VMS), and Visitor Management Systems.

2. Certificate Validation System

The Certificate Validation System provides the necessary functions to perform identification and authentication of the individual using the PIV ID card. It is composed of several compatible and interoperable components that may include servers,

validation software that acts as an interface between the card reader and the door controller, and registration and management software.

Validation Systems are generally made up of software and hardware components. They can operate on a physical server or cloud-based solution.

3. PIV Card Readers

The PIV Card Reader is an accepting device that performs functions to interact with the bearer of the credential and the credential itself via the Certificate Validation System. It is installed at an access point, door, portal, or gateway.

A PIV Card Reader may be a wholly integrated unit, or it may be an assembly of components including a smart card reader, LCD display, LED lights, audio, PIN pad, and fingerprint/biometric sensors.

Characteristics of a FICAM PACS

According to [The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard](#) and NIST [SP 800-116, Revision 1](#), a FICAM-compliant PACS system has the following characteristics:

- Uses high-assurance credentials for electronic authentication of employees and contractors
- Uses non-deprecated authentication mechanisms
- Validates the status and authenticity of credentials
- Interoperates with PIV credentials issued by other agencies
- Uses components listed on the General Services Administrations (GSA) FIPS 201 Approved Products List (APL)

Approved FICAM PACS Topologies

Currently, there are two approved FICAM PACS topologies.

- [13.01 Topology](#): end-to-end systems which integrate components from three categories (PACS Infrastructure; Validation System; and PIV Reader) together through software (SDK or API)
- [13.02 Topology](#): end-to-end systems which integrate the first two components (PACS Infrastructure; Validation System) into a "PACS Validation Infrastructure," which is then integrated with the third component category (PIV Reader)

Currently, there are several 13.01 and 13.02 topology options that meet the strict GSA APL. The solutions available require a wide range of technical abilities to properly configure.

- The 13.01 configurations can be more complex and expensive to procure and budget for lifecycle management because there are multiple PACS and software manufacturers involved in the submission.
- The 13.02 configurations are less complicated because the approach is an all-in-one submission with a single PACS manufacturer.

Challenges to FICAM Compliance

Despite the fact that FICAM was passed more than a decade ago, many systems (both inside and outside of the federal government) are obsolete and do not meet the requirements. When it comes to complying, these organizations face a range of challenges.

In some cases, the cost associated with ripping out an existing physical access control system is exorbitant. For others, already substantial investment in technology means the organization is wary of proprietary solutions. However, non-compliance could result in forgoing prospective government contracts.

Conventionally, the options for replacing a non-compliant system or securing a new site were limited. FICAM-approved PACS

options were often proprietary in nature. This constrained an organization's ability to take advantage of progressing innovation and tied it to a single provider.

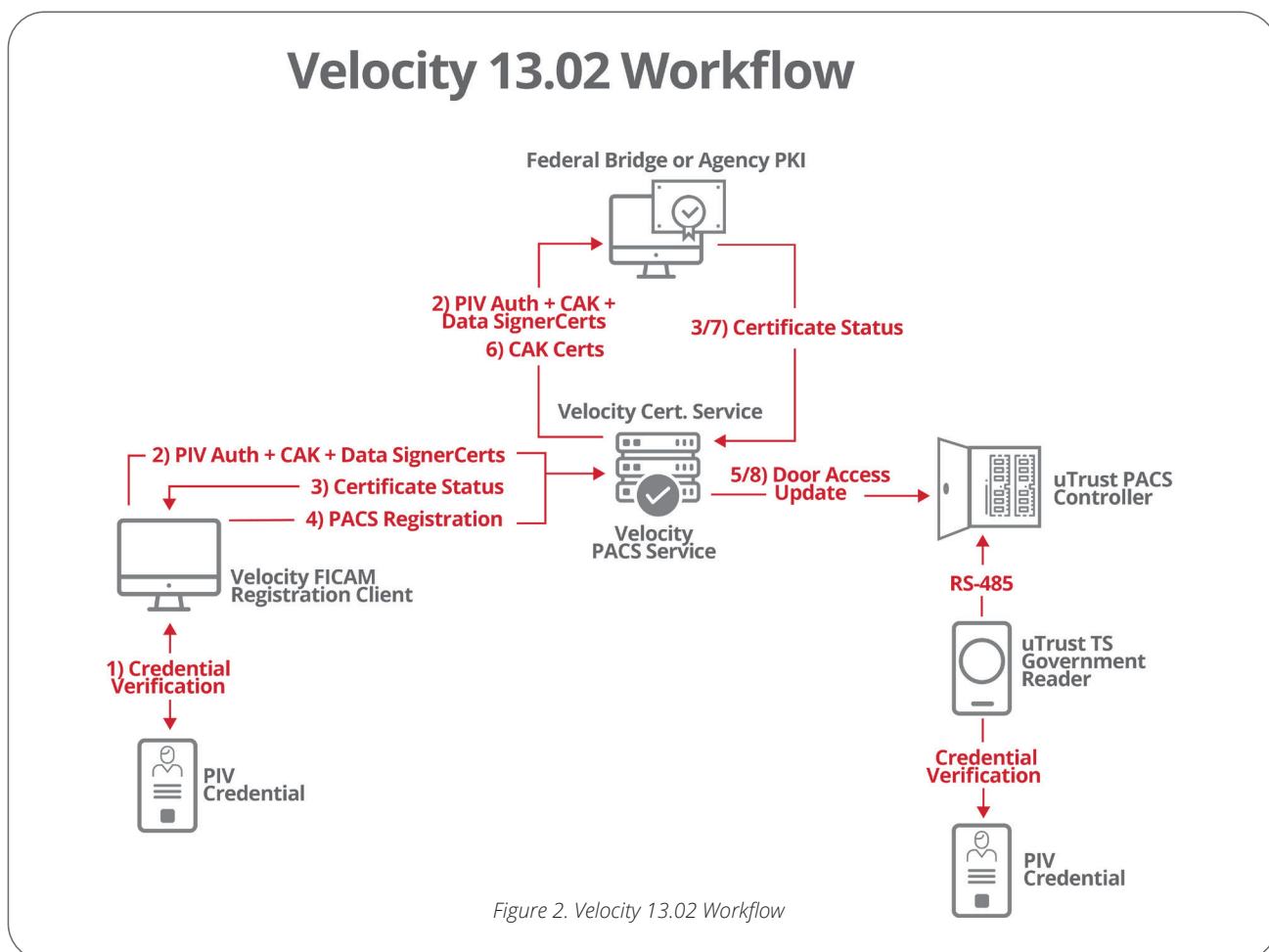
Today, as organizations look to modernize their systems, they can explore Identiv for a certified solution.

The Identiv Solution: Hirsch Velocity Software 13.02

In today's physical access world, existing FICAM solutions are expensive, slow, and increasingly difficult to set up. Identiv's approach to FICAM and the FIPS 201 Topology Categories addresses current PACS infrastructure, validation systems, and PIV readers.

Identiv's award-winning U.S. federal government [FICAM Solution \(13.02\)](#) provides customers with a low-cost, simple to deploy, and secure solution for FICAM compliance.

The Identiv 13.02 solution is scalable to include thousands of access control points and millions of PIV credentials. The table below highlights the components that comprise the Identiv 13.02 solution.



Identiv's [Hirsch Mx Controller with onboard SNIB3 powered by RS-485 Reader Expansion Board \(RREB\) kit](#) is foundational for the critical U.S. federal government security standard known as FICAM. The Mx Controller is the core of Identiv's PACS and is designed for use with Identiv's Hirsch Velocity Software security management system, uTrust TS Readers, Hirsch ScramblePad®, ScrambleProx®, ScrambleSmartProx®, and secure keypads.

The high-quality, multi-door Hirsch Mx Controllers provide a wide range of features for enterprise-scale solutions encompassing large buildings, campuses, and multi-campus facilities. The modular design and scalable architecture enable an installation to start small and grow large, from a single controller system to a larger, multi-site enterprise. These FICAM-ready kits ship with the SNIB3 module built onto the main board,

and is powered by the included RREB, allowing an additional expansion module. SNIB3 is a leading-edge communication device that provides IPv6, Gigabit Ethernet, and FIPS 140-2 certified cryptography, including TLS v1.2.

Conclusion

Identiv is a one-stop shop manufacturing and building end-to-end security solutions for physical access control, including software, hardware, readers, and credentials. All products are TAA compliant. Over the years, Identiv has served numerous federal clients with enterprise deployments, including the U.S. Marshals Service (USMS), Transportation Security Administration (TSA), Federal Bureau of Investigation (FBI), U.S. Secret Service (USSS), and more.

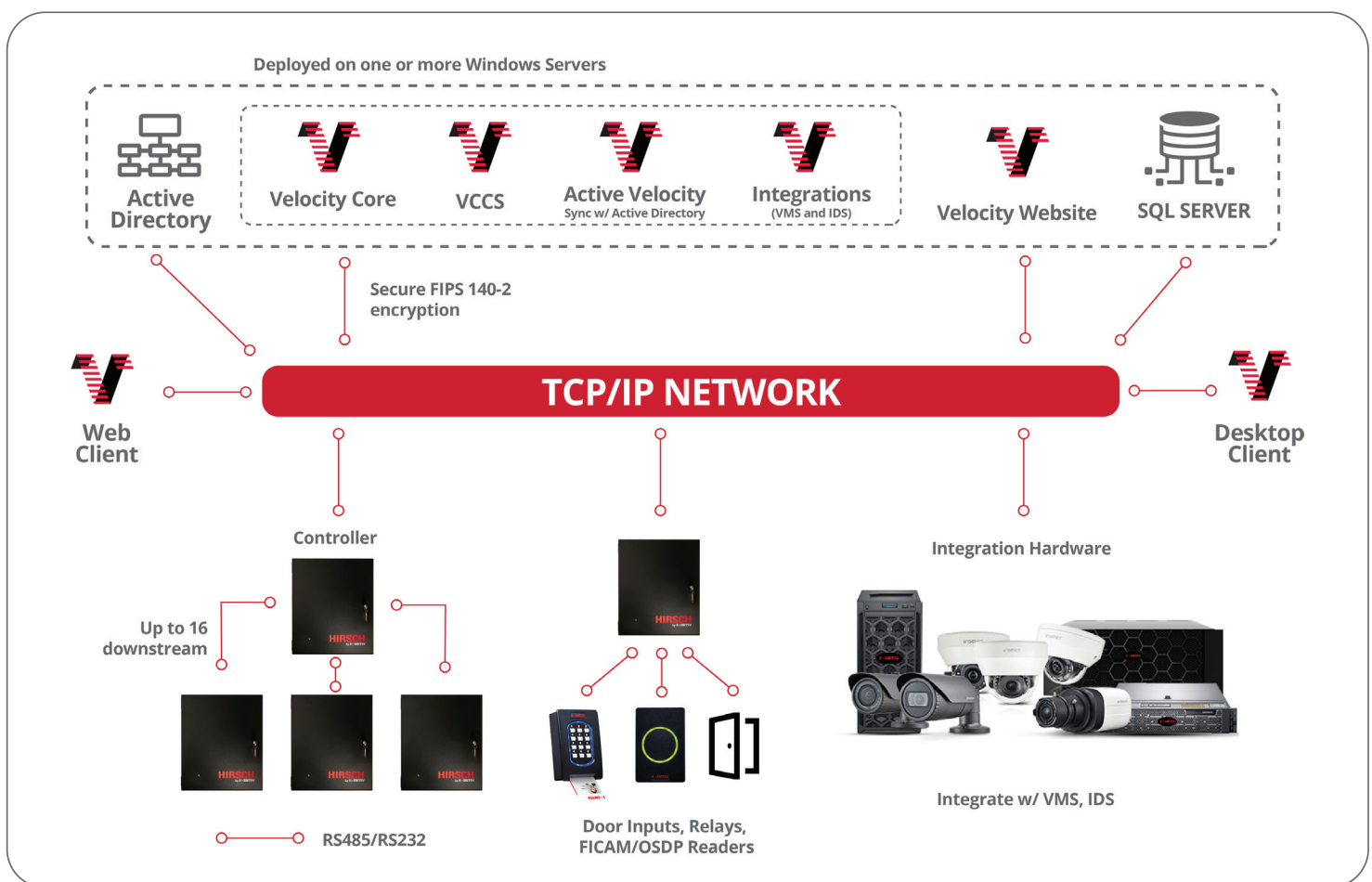


Figure 3. Velocity System Architecture

Examples of integration hardware:




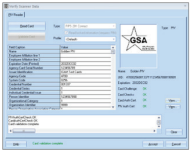


With Hirsch Velocity Software, any of the thousands of access points in the government space can be easily upgraded to FICAM compliance. Identiv leverages virtually the entire existing Hirsch system infrastructure, including Hirsch Mx-Series Controllers, uTrust TS Government Readers, SNIB3, and RREB. Even if replacing non-compliant systems is required, the Identiv solution is extremely cost-effective and quick to deploy. The time required to upgrade existing Hirsch PACS is significantly less than competitors' solutions and is available at a fraction of the cost.

Identiv works through a highly trained and certified reseller channel, maintaining a robust local DC office in Arlington, Virginia with full Pre-Sales Engineering and Training Support teams. All of Identiv's FICAM solutions can be found on the [GSA's Approved Products List](#).

References

- <https://playbooks.idmanagement.gov/arch/>
- <https://playbooks.idmanagement.gov/pm/>
- <https://playbooks.idmanagement.gov/pacs/>
- <https://playbooks.idmanagement.gov/piv/>
- <https://www.securetechalliance.org/publications-piv-corporate-enterprise/>
- <https://www.securetechalliance.org/publications-a-comparison-of-piv-piv-i-and-civ-credentials/>
- <https://www.securetechalliance.org/publications-industry-recommendations-for-implementing-piv-credentials-with-physical-access-control-systems-a-quick-guide-to-implementing-essential-nist-sp-800-116-r1-requirem/>
- <https://www.securetechalliance.org/identity-on-a-mobile-device-access-control-use-cases/>

The Identiv 13.02 solution is scalable to include thousands of access control points and millions of PIV credentials. The table below highlights the components that comprise the Identiv 13.02 solution.

PRODUCT NUMBER	PRODUCT DESCRIPTION	PRODUCT IMAGE
VELFED100	Velocity Security Management System - Base license includes 64 door modules, 10 thick clients, Velocity Web Services Console and the first year SSA	
VEL-VCCS	Velocity Certificate Checking Server	
Mx-1	Single Door Controller or GSA APL approved for wireless CAK readers (20.01) - Also available in a metal enclosure	
Mx-2-S3OB	Two-Door Controller - Expandable to 8 doors	

Mx-4-S30B	Four-Door Controller - Expandable to 8 doors	
Mx-8-S30B	Eight-Door Controller	
8002ABTF000	Mullion CAK Reader	
8102ABTF000	Wall Mount CAK Reader	
8202ABTF000	Wall Mount CAK Reader with Keypad	
8332ABTF000	ScramblePad CAK Reader with Keypad	
8336ABTF000	ScramblePad PAK Reader with Keypad	
8106ABTF000	Wall Mount CAK Reader with Contact Smart Card	
8206ABTF000	Wall Mount PAK Reader with Contact Smart Card and Keypad	
SPR332v2	USB Desktop Reader with Pinpad	