Authentication and security solutions you can trust.™

FOUR PILLARS FOR A SUCCESSFUL PIV ECOSYSTEM

Continued HSPD-12 Implementation under OMB M-11-11

Four Pillars that HSPD-12 Programs must consider for a secure, efficient, interoperable PIV enterprise deployment.

About XTec Incorporated

XTec Incorporated, a Small Business, has provided government and commercial users viable, sustainable security solutions for over two decades. We are a key technology management provider and leading developer of Homeland Security Presidential Directive-12 (HSPD-12) solutions.

An acknowledged thought leader in the security and authentication field, XTec provides unparalleled expertise. A testament to our knowledge base, to date XTec has more Certified Smart Card Industry Professionals/Government (CSCIP/G) than any other company. More importantly, we leverage this expertise to create a forward-thinking vision to meet our customers' needs. Our customized solutions implement industry-leading technology to address today's requirements and anticipate future mandates.

XTec has dedicated the past 15 years to authentication and identification solutions in support of large-scale identity management deployments. These include, but are not limited to, experiences with Department of Homeland Security (DHS), Department of State (DOS), and Department of Defense (DOD). Many XTec customers achieved card issuance in a fraction of the implementation time and "cost per cardholder" of other Agencies, all while managing cardholder identities in a secure, interoperable, and high-performance identity management system (IDMS). XTec has issued more than 500,000 PIV/FAC cards for the Federal Government and supports more than 70 Federal Agencies with card usage.

Authentication and security solutions you can trust.™

11180 Sunrise Valley Drive
Suite 310
Reston, Virginia 20191

Telephone (703) 547-3524
Fax (703) 547-3533

Table of Contents

OMB M-11-11
February 3, 2011

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

February 3, 2011

M-11-11

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Jacob J. Lew
Director

SUBJECT: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors

Effective FY2012, existing physical and logical access control systems must be upgraded to use PIV credentials, in accordance with National Institute of Standards and Technology (NIST) guidelines, prior to the Agency's using development and technology refresh funds to complete other activities.

The Government-wide architecture and completion of Agency transition plans must align with the Federal CIO Council's "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance."

Introduction

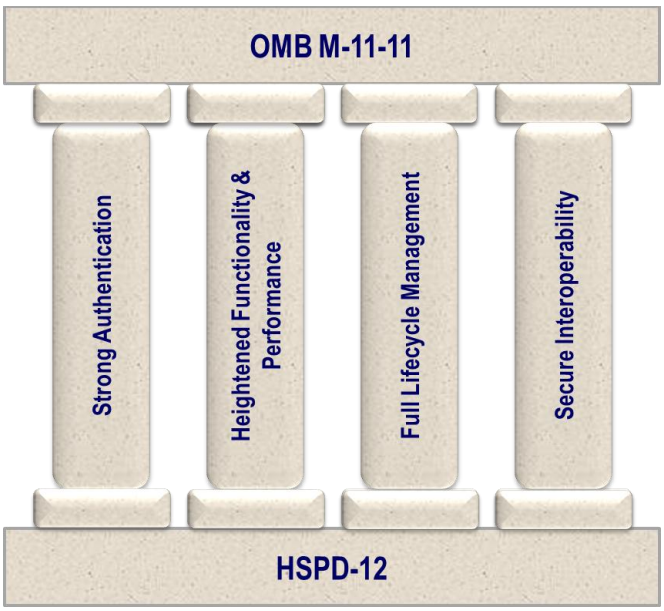
Homeland Security Presidential Directive-12[1] (HSPD-12), issued in 2004, requires Federal Government identity verification that:

a) Is issued based on sound criteria for verifying an individual employee's identity
b) Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
c) Can be rapidly authenticated electronically
d) Is issued only by providers whose reliability has been established by an official accreditation process.

In March 2011 the Office of Management and Budget (OMB) reported[2] that 84% of Federal employees and contractors had been issued a personal identity verification (PIV) card. This statistic indicates widespread deployment, but use of the card and its electronic capabilities has yet to be fully leveraged.

OMB's recent Memorandum 11-11[3] encourages Federal Agencies to "aggressively step up their efforts to use the electronic capabilities" of the PIV card. The memorandum calls for enterprise PIV use by FY2012. Implementing a comprehensive identity and access management program with the PIV card as the authentication token is a significant, and often expensive, undertaking. Federal Agencies tasked with implementation can successfully meet OMB M-11-11 mandates and continue HSPD-12 implementation by achieving four major goals:

- **Strong Authentication**
- **Heightened Functionality & Performance**
- **Full Lifecycle Management**
- **Secure Interoperability**



This white paper explores the four pillars needed for a successful identity and access management solution under the direction of HSPD-12. While additional implementation techniques and guidelines are addressed in Federal guidance such as the Federal Identity, Credential and Access Management (FICAM), this paper focuses on main points Agencies should consider when designing and implementing their PIV-based access control systems and support infrastructure. The insight and recommendations provided herein are based on "best practices" implementation of smart card technology derived from years of experience.

I. Strong Authentication

Authentication is the process of establishing confidence in user identities. Strong PIV card authentication ensures that the credential is, as required by HSPD-12, *"strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation."* Authentication can mean a username-password pair and matching the credentials presented with entries in a database but *strong* authentication must include cryptographic functions.

Two major types of cryptographic functions, symmetric and asymmetric, exist with respect to PIV card authentication. Asymmetric cryptography is the use of two related keys, a public and a private, to perform complementary operations. Symmetric cryptography is the use of a secret cryptographic key to perform both the cryptographic operation and its inverse. Both symmetric and asymmetric methods allow for strong authentication, as both methods meet

the highest level of assurance defined by National Institute of Standards and Technology (NIST) Special Publication (SP) *800-63 Electronic Authentication Guideline*[4]. While both offer the same level of assurance, each requires different steps and is suited for different situations.

While asymmetric cryptography is necessary for authenticating X.509 digital certificates, Agencies can use symmetric authentication in some instances to increase efficiency without compromising assurance and security. For example, symmetric cryptography is ideal when most cardholders entering a building at the perimeter have been vetted and issued personalized cards at that particular Agency. The Agency maintains and manages the credential being presented and is the primary party for notification of compromise, replacement, renewal, expiration, and status.

Symmetric cryptography works best when the PACS or LACS system operator and owner (Agency) know the individual presenting the credential. In these cases, Agencies that employ symmetric cryptography will decrease the time required to complete a transaction, allow the card to "readily authenticate," and increase user experience by preventing burdensome lines. Note: It is assumed that any implementation will not be deployed without diversified symmetric keys.

Asymmetric cryptography is widely accepted as an interoperable means of authenticating a PIV card. To perform strong authentication, access control systems must complete four major steps.

1. Verify Genuine Card Identity. Verify that the unique ID on the card was not altered. Check unique ID (CHUID/FASCN) to ensure it is signed and matches unique ID on the digital certificates.

2. Ensure Certificate is Linked to Card. Perform challenge-response exchange to ensure the certificate belongs to that specific card. Challenge is issued using public key, to which the card responds with the corresponding private key.

3. Validate Trusted Origin. Ensure that no root or intermediate key certificate has been revoked. Perform path validation. Review the chain of issuers to determine that all are legitimate and trusted.

4. Check Status. With the legitimacy of the certificate and card confirmed, now ensure that the certificate is active and has not been revoked. Check status of digital certificate using Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) Responder.

Cryptography

The discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity.

-NIST SP 800-21-1 Guideline for Implementing Cryptography In the Federal Government

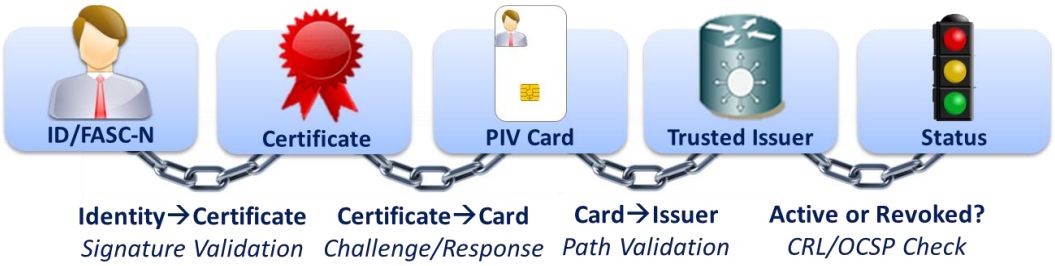


Figure 1- PIV Authentication

Failure to confirm all four links results in vulnerabilities. In addition to the steps for strong authentication, an Agency should be prepared to conduct asymmetric cryptography for physical and logical access as practically and efficiently as possible. Methods for asymmetric cryptography will be addressed in the next section.

Realizing both forms of strong authentication requires Federal Agencies to guarantee that their physical and logical access control systems can perform both symmetric and asymmetric cryptography. Given the progress of HSPD-12, Agencies with established access controls systems would be wise to determine if a vendor can upgrade legacy access control systems to perform strong authentication.

Recommendation: *Always use cryptographic mechanisms to perform strong authentication. To fully leverage the PIV card capabilities and increase security, avoid minimal, basic authentication (CHUID check, "free read"). Implement access control that can perform both (and seamlessly switch between) symmetric and asymmetric cryptography.*

II. Heightened Functionality & Performance

In conjunction with strong authentication, Agencies must consider the ability of their access control systems to operate efficiently. To add value to end users and maintain security, access control systems should perform authentication reliably. The design of the access control system architecture should be used as the primary tool to improve functionality, performance and availability. Agencies should consider two methods that result in increased functionality, the deployment of trusted edge devices and the use of cloud technology.

To increase performance and availability, Agencies should deploy authentication devices geographically close to access points. Much like a network router, an Online Certificate Status Protocol (OCSP) responder placed near an entry point or access decision point will decrease the time required to perform cryptographic functions and will ensure the appropriate decision

point is reached. Decreasing the load of requests on a single server or OCSP is a significant benefit with the deployment of enterprise access control. The number of users that possess a PIV card can be significant at any single Agency; deploying edge devices can be done strategically in areas of high concentration or in any area where several transactions take place. An edge device works to bring functionality to a specified location and prevents the procurement of multiple servers that operate identically. It is important to note that an edge device must be deployed in a trusted environment with two-way communication. For example, if the edge device is communicating with a card reader the card reader must be able to authenticate to the edge device, and vice versa. All critical devices should be capable of two-way communication to safeguard the infrastructure from fraudulent devices and communications.

In addition to increasing efficiency, trusted edge devices allow an access control system to be easily deployed, modified, or upgraded across multiple areas. As a result of placing trusted edge devices at or near access points and high-population areas, sub-agencies and various building locations can possess a certain level of autonomy to enforce entity policies. Local monitoring and configuration can be supported when an access control system is designed with trusted edge devices. For example, an access control point that requires multi-factor authentication and is strictly monitored can benefit from a dedicated OCSP responder edge device.

In addition to the deployment of edge devices, utilizing a "Software as a Service" (SaaS) or cloud computing model can improve services. As noted in the *Federal Cloud Computing Strategy,*[5] cloud computing can "maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost." The ability to improve IT flexibility, responsiveness and reduce costs leaves room for Agencies to focus on mission critical items. Particularly applicable to access control systems and the missions of HSPD-12, as well as to FICAM, is the fact that "cloud computing can help to mitigate the fragmented data, application, and infrastructure silo issues." Cloud technology, in combination with the deployment of edge devices that securely communicate through the cloud, will ultimately heighten the functionality of the access control system by:

- Increasing Performance
- Increasing Availability
- Increasing End User Experience
- Readily Performing Electronic Authentication
- Decreasing Cost

Recommendation: *Deploy authentication devices such as OCSP responders geographically close to access points to increase availability and performance. Consider combining cloud technology with edge devices to reduce costs and increase flexibility.*

III. Full Card Lifecycle Management

ID badges were traditionally static; the information they contained rarely changed. They were low maintenance and presented few problems. In the few cases where change was necessary, it was simple to issue a new one. Likewise, lifecycle management was effectively a non-issue.

PIV technology is a game changer. Security migrated to a secure portable FIPS 140-2 device. The card's integrated circuit contains information that is likely to change over time. It also requires a PIN code that must be remembered and entered to activate the card. So when a data item changes or a PIN is forgotten, Agencies have only one recourse, electrically updating the PIV. (Issuing a brand new PIV is economically prohibitive.)

Electrical updates bring Agencies into the realm of significant card lifecycle management. If they don't prepare carefully, Agencies will find that the lifecycle management becomes a high maintenance activity. Therefore, Agencies should take practical steps to ensure that PIV lifecycle management remains low maintenance.

Let's consider three PIV maintenance activities that are current or seemingly imminent.

1. **PIN Reset.** A cardholder forgets the PIN or remembers it too late, locking the card after too many unsuccessful attempts. To be usable, the card must be unlocked and the PIN reset.

2. **UPN Update (or equivalent).** The PIV authentication digital certificate contains information needed for enabling single sign-on to networks and applications. For Agencies using Microsoft's Active Directory (AD), the needed data element is the user principal Name (UPN). The UPN might change for a number of reasons. For example, a large Federal Department redesigns its AD forest structure and wants to modify UPNs to reflect the new structure. Another reason is that a cardholder might transfer to an organization based in a different AD forest. Depending on the AD

forest structure, the cardholder's UPN may change. In these and other cases, an Agency must update the PIV Card with the new UPN.

3. **Key Recovery.** Agencies are required to protect information – including transmitted documents and emails – with encryption. The PIV card and the PIV Key Encryption Key (KEK) each play a role in providing that protection. But encryption keys don't last forever, even though access to the protected information should. For example, an encrypted email may be needed many years after it was originally sent, even if the encryption key is expired or revoked.

   Key Recovery is a mechanism for retrieving one or more previous encryption keys for this purpose. As Agencies fully implement encrypted protection, they will need the ability to perform key recovery for legacy cardholders PIV Cards who are not enabled with information about escrowed encryption keys.

These are three PIV lifecycle management requirements envisioned today; others will undoubtedly arise over time. The challenge Agencies face is supporting these and forthcoming PIV lifecycle management activities securely using an efficient, low maintenance mechanism.

Requiring the cardholder to return to a location where PIV cards are issued is secure, but it is neither low maintenance nor low cost. Far better is to empower cardholders to perform these operations from their desktops. The trick is to extend the reach of the PIV management infrastructure to the user's desktop so that it not only enables the lifecycle management functionality but also does so securely, guaranteeing the integrity of the PIV Card during and after the update.

Recommendation: *Expand the reach of the PIV management infrastructure down to the cardholder desktop. Use edge devices and software to provide security, efficiency, and scalability.*

IV. Secure Interoperability

An Agency's ability to accept PIV credentials in a Government-wide scenario, as described in OMB M-11-11, is critical to the success of any PIV

FICAM Value Proposition

Enhanced customer service, both within agencies and with their business partners and constituents. Facilitating secure, streamlined, and user-friendly transactions – including information sharing – translates directly into improved customer service scores, lower help desk costs, and increased consumer confidence in Agency services.

-Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance V1.0

environment. Interoperability can be interpreted as accepting cards based on visual inspection, reading a CHUID value, or purchasing approved products. Unfortunately, these methods can be insecure and may cause Agencies to invest in solutions that do not foster secure interoperability. Therefore, Agencies should take advantage of the electronic capabilities of the PIV card specification to implement secure electronic interoperability.

Secure electronic interoperability with respect to the PIV card means leveraging the Federal trust network or the Federal public key infrastructure (PKI). Asymmetric cryptography, previously discussed in Section I, is the most common facet of interoperability. A core HSPD-12 requirement is that the PIV credential is "issued only by providers whose reliability has been established by an official accreditation process." The Federal PKI provides trust based on a set of common policies, processes, and supporting technical infrastructure. Furthermore, the Federal PKI has the sole ability with respect to HSPD-12 to issue, maintain and revoke public key certificates. The established policies and processes for maintaining a credential must be followed to ensure interoperable trust across the Government.

Secure interoperability, in addition to using the Federal PKI and strong authentication, will allow Agencies to reduce PIV lifecycle costs. The ability to accept and trust a different Agency's PIV card alleviates the cost of issuing multiple credentials for an individual who works at several Agencies, such as a contractor or an employee on assignment at a different Agency. Vendors today can provide software that is not only capable of performing strong authentication but also able to introduce that credential in their identity and credential management systems. This is particularly relevant for multi-tenant facilities, where more than one Agency is present at a location, but can be beneficial in other areas such as Agencies with independently operated facilities or branches.

Implementing access control systems that utilize cryptography is a timely investment for the future as well. New standards and infrastructure supporting Federal PKI cross-certified credentials, such as the PIV-Interoperable (PIV-I) credential, are currently being deployed. Federal CIO Council guidance *Personal Identity Verification Interoperability for Non-Federal Issuers*[6] is one such standard that will guide this practice; it is expected that NIST and additional CIO Council guidance will follow. Agencies can reduce future costs and prevent the use of technology refresh funds by ensuring their access control solutions support PIV-I or third party trusted credentials now.

FICAM Value Proposition

Improved interoperability, specifically between agencies using their PIV credentials along with other partners carrying PIV-interoperable or third party credentials that meet the requirements of the federal trust framework. Additional benefits include minimizing the number of credentials requiring lifecycle management.

-Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance V1.0

Recommendation: *Implement access control systems that use cryptographic authentication mechanisms and are capable of supporting future interoperability enhancements, such as PIV-I. Invest in products that can incorporate differing Agency credentials into the identity and credential management system on a regular or as-needed basis.*

Conclusion

It is not enough to simply procure approved products; Agencies must consider the ability of those products to provide true security, yet also be efficient and scalable. By addressing the four pillars described in this white paper, Federal Agencies can achieve a secure, efficient, interoperable enterprise PIV environment.

Strong authentication will ensure that physical and logical resources are protected from intrusion and fraud.

Heightened Functionality & Performance, specifically self-service and cloud or edge technology will make the PIV enterprise more efficient.

Full Lifecycle Management will be addressed by expanding the reach of the PIV management infrastructure down to the cardholder desktop and using edge devices and software to provide security, efficiency, and scalability.

Secure Interoperability, the ability to accept and trust differing Agency credentials while preparing for the acceptance of third party credentials, will prevent costly, time-consuming upgrades.

Recommendations:

Always use cryptographic mechanisms to perform strong authentication. To fully leverage the PIV card capabilities and increase security, avoid minimal, basic authentication (CHUID check, “free read”). Implement access control that can perform both (and seamlessly switch between) symmetric and asymmetric cryptography.

Deploy authentication devices such as OCSP responders geographically close to access points to increase availability and performance. Consider combining cloud technology with edge devices to reduce costs and increase flexibility.

Expand the reach of the PIV management infrastructure down to the cardholder desktop. Use edge devices and software to provide security, efficiency, and scalability.

Implement access control systems that use cryptographic authentication mechanisms and are capable of supporting future interoperability enhancements, such as PIV-I. Invest in products that can incorporate differing Agency credentials into the identity and credential management system on a regular or as-needed basis.

References

[1] Homeland Security Presidential Directive 12 HSPD-12 August 22, 2004
http://www.idmanagement.gov/documents/HSPD-12.htm
[2] HSPD-12 Status Report March 2011 http://idmanagement.gov/presentations/HSPD12_Current_Status.pdf
[3] OMB M11-11 Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf
[4] NIST SP 800-63 Electronic Authentication Guideline, April 2006 http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
[5] Federal Cloud Computing Strategy February 2011 http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf
[6] Personal Identity Verification Interoperability for Non-Federal Issuers, Federal CIO Council July 2010
http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers.pdf