The attached DRAFT document (provided here for historical purposes) has been superseded by the following publication:

Publication: **NIST Cybersecurity White Paper**

Title: **Best Practices for Privileged User PIV Authentication**

Publication Date: **4/21/2016**

- Final Publication: http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf.
- Related Information on CSRC: http://csrc.nist.gov/groups/SNS/piv/
- Information on other NIST cybersecurity publications and programs can be found at: http://csrc.nist.gov/

NIST National Institute of Standards and Technology • U.S. Department of Commerce

The following information was posted with the attached DRAFT document:

Feb. 5, 2016

Whitepaper

DRAFT Best Practices for Privileged User PIV Authentication

This draft white paper is a best practices guide. The paper is in response to the Cybersecurity Strategy and Implementation Plan (CSIP), published by the Office of Management and Budget (OMB) on October 30, 2015, requiring Federal agencies to use Personal Identity Verification (PIV) credentials for authenticating privileged users. The paper outlines the risks of password-based single-factor authentication, explains the need for multi-factor PIV-based user and provides best practices for agencies to implementing PIV authentication for privileged users.

The public comment period closes on: **March 4, 2016**.
Send comments to csip-pivforprivilege @nist.gov with "Comments on PIV Credential for privileged use" in the subject line.

NIST Computer Security Division and Applied Cybersecurity Division
csrc.nist.gov

Best Practices for Privileged User PIV Authentication

Computer Security Division
Information Technology Laboratory

Applied Cybersecurity Division
Information Technology Laboratory

DRAFT

February 5, 2016

National Institute of Standards and Technology
U.S. Department of Commerce

Abstract

The Cybersecurity Strategy and Implementation Plan (CSIP), published by the Office of Management and Budget (OMB) on October 30, 2015, requires that Federal agencies use Personal Identity Verification (PIV) credentials for authenticating privileged users. This will greatly reduce unauthorized access to privileged accounts by attackers impersonating system, network, security, and database administrators, as well as other information technology (IT) personnel with administrative privileges. This white paper further explains the need for multi-factor PIV-based user authentication to take the place of password-based single-factor authentication for privileged users. It also provides best practices for agencies implementing PIV authentication for privileged users.

Keywords

authentication; Cybersecurity Strategy and Implementation Plan (CSIP); Derived PIV Credential; identification; multi-factor authentication; Personal Identity Verification (PIV); PIV Card; privileged access; privileged user

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Additional Information

For additional information on NIST's Computer Security Division and Applied Cybersecurity Division programs, projects, and publications, visit the Computer Security Resource Center, csrc.nist.gov. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is available at www.nist.gov and www.nist.gov/itl.

NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems.

DRAFT

Table of Contents

List of Appendices

List of Figures

List of Tables

DRAFT

1 The Need to Strengthen Authentication for Privileged Users

Attackers impersonate system, network, security, and database administrators, as well as other information technology (IT) personnel with administrative privileges, to gain unauthorized access to Federal systems and the information they contain. Impersonation is usually accomplished by exploiting known weaknesses of password-based single-factor authentication. To greatly reduce the risk of privileged user impersonation to non-national security Federal systems, the Cybersecurity Strategy and Implementation Plan (CSIP) [1] published by the Office of Management and Budget (OMB) directs agencies to transition to multi-factor[1] Personal Identity Verification (PIV)-based authentication for all privileged users.

This white paper provides additional information regarding this requirement from the CSIP. The purpose of the white paper is to explain the requirement's importance from a security standpoint and to provide best practices for adopting a solution that meets the requirement.

1.1 Limitations of Password-Based Single-Factor Authentication

For many years, most organizations, including Federal agencies, have relied heavily on password-based single-factor user authentication. There are many types of threats against this form of authentication, including the following:

- **Capturing passwords:** an attacker acquiring a password from storage, transmission, or user knowledge and behavior. Examples of ways that attackers capture passwords include the following:
    - Infecting a system with malware that acts as a keylogger,[2] capturing the user's keystrokes
    - Conducting social engineering to trick a user into revealing a password via phishing emails and fraudulent imitation websites, social networks, phone calls, etc.
    - Gaining logical or physical access to a system and recovering stored passwords that are unencrypted or weakly encrypted
    - Monitoring network traffic and recovering passwords or password hashes that are not adequately protected (e.g., unencrypted, weakly encrypted, replayable)
    - Watching a user type a password (i.e., shoulder surfing)
    - Finding password that have been written down on paper, workstations, white boards, etc.
- **Guessing passwords:** an attacker repeatedly attempting to authenticate using default passwords, dictionary words, and other likely passwords.
- **Cracking passwords offline:** an attacker recovering cryptographic password hashes and using analysis methods to attempt to identify a character string that will produce one of these hashes.

[1] Multi-factor is a characteristic of an authentication system or a token that uses more than one authentication factor. The three types of authentication factors are something you know, something you have, and something you are.
[2] A hardware-based keylogger can also be placed on a computer if it uses a keyboard attached by a cable.

DRAFT

- **Resetting passwords:** an attacker resetting an existing password to an attacker-selected password. For example, an attacker could intercept and manipulate a user's legitimate attempt to reset a password.

All of these threats can be exploited by an attacker obtaining the identity credential (the single-factor password) of a legitimate user to gain unauthorized access to an agency's systems and/or networks with that user's privileges. If a password is used across multiple systems, the compromise of this password enables unauthorized access to all the other systems. There are some controls available to counter these threats, but they have limited effectiveness, so the threats as a whole against password-based single-factor user authentication can only be slightly mitigated. Many attackers leverage the impersonation of a regular user into greater access to an agency's systems and networks by issuing subsequent attacks to escalate privileges and gain administrative-level access. This, in turn, can be used to move from system to system, surreptitiously traveling through the enterprise to eventually reach a High Value Asset.[3] Administrative-level access can also be used to tamper with system integrity by establishing backdoors into the system, such as creating additional privileged accounts or altering a service to permit unauthorized access to the system. An attacker can use these backdoors to gain persistent access to the system.

Most instances of user impersonation from password-based single-factor authentication can be prevented by multi-factor authentication. Multi-factor authentication makes it more difficult for an attacker to gain unauthorized access to a system. An attacker would have to compromise two factors – not just one – to gain access, such as something the user has (a smart card) and either something the user knows (a password or PIN to unlock the smart card) or something the user is (a biometric characteristic to unlock the smart card). NIST Special Publication (SP) 800-63 [2] and SP 800-53 [3] recognize these differences. In NIST SP 800-63, password-based single-factor authentication is at most Level of Assurance[4] 2 (LOA-2) while two-factor authentication reaches LOA-3 and LOA-4. In tandem, NIST SP 800-53 requires multi-factor authentication for all systems categorized as MODERATE or HIGH.

For more information on general threat models and mitigations for the identity management lifecycle, including identity proofing, registration, issuance, and revocation, see the latest revision of NIST SP 800-63 [2].

1.2 Multi-Factor Authentication Using PIV Credentials

Homeland Security Presidential Directive 12 (HSPD-12) [4] mandated the development and use of a Federal standard for identification and authentication of federal employees and contractors. HSPD-12's intent is to eliminate the "wide variations in the quality and security of identification used to gain access." The standard resulting from HSPD-12, Personal Identity Verification (PIV), is defined in Federal Information Processing Standards (FIPS) Publication 201 [5]. FIPS

3 From the CSIP [1]: "'High Value Assets' refer to those assets, systems, facilities, data and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions or data used in critical Federal operations, or house unique collections of data (by size or content) making them of particular interest to criminal, politically-motivated, or state-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the U.S. Government."

4 See Section 1.4 of this document for more information on LOA.

DRAFT

201 requires each federal employee and contractor to be issued a smart card (a PIV Card) that contains identity credentials. PIV Cards can provide multi-factor authentication by requiring each user to possess a valid card and enter the correct PIN or biometrics for that card. The card then executes secure cryptographic authentication exchanges with host computer systems to convey the user's identity with a high level of assurance.

The deployment of PIV Cards is an important part of the Federal government's effort to mitigate theft and subsequent reuse/replay of users' credentials. As reinforced by the CSIP, PIV Cards significantly reduce the risks from capturing, guessing, cracking, or resetting single-factor passwords (PINs) since an imposter must compromise two factors by gaining access to the PIV Card and obtaining the corresponding PIN[5] or biometric to unlock the card. The cryptographic key used for authentication is stored on the card and protected by active internal security mechanisms. As such, PIV Cards are difficult to compromise.

Revision 2 of FIPS 201 [5], published in 2013, introduced another PIV credential called the Derived PIV Credential,[6] which may be used with mobile devices,[7] where the use of the PIV Card is impractical. Similar to the PIV Authentication certificate on the PIV Card, the Derived PIV Credential on a mobile device is a public key infrastructure (PKI) based credential called the Derived PIV Authentication certificate that provides two-factor authentication. The Derived PIV Authentication certificate can be issued according to the requirements of either LOA-3 or LOA-4[8], depending on whether the private key corresponding to the credential is protected and used in a hardware or software cryptographic module, and also depending on how the credential was issued. Like the PIV Card and its PIV Authentication credential, the Derived PIV Credential also significantly reduces the risks from capturing, guessing, cracking, or resetting single-factor passwords.

1.3 The CSIP and PIV-Based Authentication for Privileged Users

On June 12, 2015, the Federal Chief Information Officer (FCIO) started an activity known as the Cybersecurity Sprint. Led by OMB, the Sprint Team, comprising over 100 members from Federal agencies, performed a 30-day review focused on improving cybersecurity for Federal information and information systems. The team's goal was "to identify and address critical cybersecurity gaps and emerging priorities, and make specific recommendations to address those gaps and priorities." [1]

This work resulted in the development of the CSIP [1]. A major gap identified by the CSIP is the delay in utilizing PIV credentials for logical access control and identity management on Federal information systems, with an especially high priority for strengthening authentication for

DRAFT

---

5 PIN-guessing attacks are seldom successful against PIV Cards because the card will lock after a small number of failed PIN entry attempts.

6 For more information on Derived PIV Credentials, see NIST SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials* [6].

7 A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable, or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smartphones, tablets, and e-readers. [6]

8 See Section 1.4 of this document for more information on LOA.

privileged users. Privileged users have network accounts with privileges that grant them greater access to IT resources than non-privileged users have. These privileges are typically allocated to system, network, security, and database administrators, as well as other IT administrators. Privileged accounts are exceptionally attractive targets for attackers of High Value Assets. A higher level of assurance than what is provided by single-factor authentication is therefore required for privileged users since unauthorized access to administrator capabilities can have catastrophic adverse effects on agency operations, assets, and/or individuals.

As stated in the CSIP, "The Cybersecurity Sprint directed agencies to immediately implement PIV for […] 100% of privileged users." [1] The reason for this directive is that "Although there is no single method by which all cyber incidents can be prevented, improving the access management of user accounts on Federal information systems could drastically reduce current vulnerabilities. Privileged user accounts are a known target for malicious actors but can be protected by an existing, strong authentication solution: Personal Identity Verification (PIV) credentials. Implementing strong authentication PIV credentials, as directed in *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD-12)* and *Federal Information Processing Standard (FIPS) 201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors*, is a cost-effective and immediate action that agencies should take to drastically reduce their risk profiles. PIV credentials […] reduce the risk of identity fraud, tampering, counterfeiting, and exploitation." [1]

1.4 PIV-Based Authentication and Assurance Levels

Agencies are required to perform a risk assessment to determine the level of assurance requirements of their systems according to OMB Memorandum 04-04 (M-04-04), *E-Authentication Guidelines for Federal Agencies* [7] (see Section 2.3). To achieve the requirements of a given level of assurance, agencies must implement the safeguards specified in NIST SP 800-63 [2] for the following elements:

- Identity proofing (Chapter 5)[9]
- Tokens (Chapter 6)
- Token and credential management (Chapter 7)
- Authentication process (Chapter 8)
- Assertions, where applicable (Chapter 9)

The PIV Authentication certificates on PIV Cards are issued in a manner that satisfies the requirements for level of assurance 4 (LOA-4) for identity proofing, token, and token and credential management in NIST SP 800-63 [2]. Derived PIV Authentication certificates are also

DRAFT

[9] Issuance of a Derived PIV Credential avoids duplicating identity proofing processes. Instead of identity proofing, the Derived PIV Credential is issued based on proof of possession and control of a previously issued credential (i.e., the PIV Card).

issued in a manner that satisfies the identity proofing, token, and token and credential management requirements of NIST SP 800-63 [2]; however, NIST SP 800-157 allows Derived PIV Authentication certificates to satisfy these requirements at either LOA-3 or LOA-4, with the certificate identifying the level of assurance that was met. Systems that accept PIV credentials must implement the authentication process requirements in NIST SP 800-63 [2], and will also need to implement the assertions requirements in NIST SP 800-63 [2] if they make use of assertions (see Section 2.4.1).

PIV Authentication certificates and Derived PIV Authentication certificates may be used in various PKI-based protocols including Transport Layer Security (TLS) certificate-based client authentication and initial authentication for Kerberos (PKINIT) [19]. Authentication using one of the PIV authentication certificates requires that a digital signature operation be performed with the private key associated with the certificate and that the system performing the authentication verify the signature while also validating the certificate itself. As further discussed in Section 2.3 of this document, not all protocols achieve the overall LOA-4 authentication level that the certificate being used is capable of providing. This is especially true if the authentication protocol involves a third party (a Verifier) that simply conveys to the system that needs to know the individual's identity (the Relying Party) that successful PIV-based authentication has occurred.

DRAFT

2 Best Practices for PIV-Based Privileged User Authentication

An agency is said to have *PIV enabled* a system for privileged users if its users must successfully authenticate using the PIV Authentication certificates on their PIV Cards or Derived PIV Authentication certificates on their mobile devices in order to gain access to privileged accounts on the system. This section of the white paper recommends the following best practices for PIV-enabling Federal information systems to prevent the impersonation of privileged users:

- Inventory all privileged users and accounts, then eliminate all unnecessary privileged access (Section 2.1).
- Issue dedicated, highly secured endpoint devices for all privileged use (Section 2.2).
- Use a risk-based approach to select the appropriate level of assurance for each system (Section 2.3) based on the criticality of each type of privileged access to the system. For access to privileged accounts, the appropriate level of assurance is either LOA-4 or LOA-3.
- Select the appropriate PIV authentication architecture (Section 2.4). The selection of the architecture for each system should be based on the determined level of assurance, the feasibility and impact to the system's functionality, and the system's capabilities to support the PIV authentication architecture.
    - For those systems that do not support a PIV authentication architecture that provides the appropriate level of assurance, implement the necessary compensating controls found in NIST SP 800-53 [3]. Table 1 in this document lists the controls most likely to be needed to complement PIV authentication.
    - For those systems that either do not support PIV authentication at all or do not support it at the appropriate level of assurance, establish a plan of action and milestones (POA&M) to transition from the system's technology and resolve the issue within an acceptable time period determined by the agency.
- To minimize the potential impact of a compromised privileged account, agencies should automate monitoring of privileged access and implement continuous monitoring of all privileged access.[10] Frequent or continuous monitoring is particularly important for legacy systems that do not support PIV authentication for privileged users at the appropriate level of assurance.

Note that these best practices do not need to be performed sequentially. For example, an agency may issue dedicated, highly secured endpoint devices for privileged use at the same time that it inventories privileged access and uses a risk-based approach for selecting the appropriate level of assurance for each system. Applying the best practices documented in this section will allow

[10] For more information on continuous monitoring, see NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* [8].

DRAFT

agencies to take advantage of the security and usability of PIV credentials not only for privileged access but also across systems for all other users at various assurance levels. The benefit of determining an assurance level for each system is that it provides agencies the information necessary to select the most appropriate PIV authentication architecture (see section 2.4).

2.1 Minimize Privileged Access

By adhering to the NIST Risk Management Framework (RMF) (as described in Section 2.3), the FIPS 199 [9] categorization selected for each system, and the FIPS 200 [10] security baseline (which is further specified in NIST SP 800-53 [3]), an agency has an excellent basis for identifying its high-risk privileged users and accounts. Starting with the highest risk or most critical systems (for example, any system with an overall FIPS 199 categorization of High or identified High Value Assets), agencies should inventory all privileged users, the privileged accounts those users have access to, the permissions granted to each privileged account, and the authentication technology or combination of technologies required to use each privileged account.

The agency should compare the inventory to what is necessary to meet the organization's mission, and then remove all unnecessary privileged accounts, unnecessary permissions for privileged accounts, conflicting permissions for privileged accounts[11], unnecessary user access to privileged accounts in accordance with the principle of least privilege and perform automated reviews of privileged user access. This should include, at a minimum, the following actions:

1. Remove all privileged account access from users who no longer require access to perform their assigned duties (e.g., system, network, or database administration).
2. Remove or disable all privileged accounts, including default and built-in accounts, that are no longer required.
3. Remove excessive access to privileged accounts from privileged users in accordance with the principles of least privilege and separation of duties. Access should be evaluated in the context of enterprise risk, not just application risk. For example, granting a privileged user access to both portions of a sensitive personally identifiable information (PII) data set divided between two systems may create excessive risk to the organization.
4. Remove all unnecessary permissions from privileged accounts. This includes restricting which commands, functions, or other elements can be performed through privileged accounts. It may also include additional restrictions to more strongly limit the use of privileged accounts via remote access (in other words, allow certain actions to be performed only from dedicated, highly secured endpoint devices).
5. Enforce a maximum single session length for use of each privileged account. The maximum length specified for each account may depend on the criticality of the functions available through that account.
6. Require re-authentication to a privileged account after a prolonged period of inactivity.
7. Establish and use a mechanism to rate privileged user access risk so that the agency knows which privileged accounts are the riskiest (to include those not protected with PIV

DRAFT

[11] In some cases, a single privileged user may have access to one or more privileged accounts that offer excessive privileges to that user—for example, violating the principle of separation of duties.

authentication), which privileged users have the riskiest access, and what operations can be performed with the privileged access.

8. Log and monitor all use of privileged accounts, and alert when abnormal or questionable activities are observed.
9. Conduct automated reviews (for example, every 30 days) of privileged user access in accordance with law, regulation, policy, and NIST guidelines. This review should ensure compliance with the principle of least privilege, and the privileged user and account inventory should be updated as part of the review process.

2.2 Issue Dedicated Endpoint Devices for Privileged Use

An attacker able to gain control of a privileged user's device may be able to hijack privileged-access sessions and impersonate that user on critical systems. The risk of compromise on these devices increases if they are used for general computing activities, such as web browsing or e-mail.

To mitigate that risk, agencies should consider providing privileged users with dedicated endpoint devices (laptops, desktops, mobile devices, etc.) for privileged use only. These devices should be hardened and secured as strongly as possible to reduce the risk of compromise. Systems should ensure that privileged access is only possible from these dedicated endpoint devices. For example, systems could authenticate not only the user via the PIV credential but also authenticate the device itself. With strong device authentication, access from non-dedicated devices could be deterred at the device level.

As an alternative to device authentication, some agencies are considering issuing two credentials to users with privileged access, one dedicated to accessing privileged user accounts that is only to be used from dedicated endpoint devices and one for accessing unprivileged user accounts. However, this alternative relies on the user to never accidentally or intentionally use the credential for privileged access in a non-dedicated or untrusted device. Using device credentials, or other credentials tightly bound to devices dedicated for privileged access, in combination with PIV credentials for user authentication, can mitigate this risk at a technical level.

Privileged access from a device also used for non-privileged access should be based on the agency's risk assessment for a given system. To the extent possible, single devices should include controls to block malware targeting impersonation of the privileged user from a non-privileged session. Approaches may include sandboxing technologies, jump servers and virtual dedicated machines. Dedicated devices represent a stronger security posture than using a single device for both privileged and unprivileged access. Agencies need to consider and manage the risk when selecting the single device approach.

2.3 Integrate LOA-3 and 4 Privileged Authentication Requirements into an Overall Risk-Based Approach

The NIST Risk Management Framework (RMF) [12] specifies the security risk management activities that an agency should perform throughout the system development lifecycle. The RMF references the associated standards and guidelines necessary to categorize system risk, select and implement security controls, and assess, monitor, and enhance their efficacy over time.

DRAFT

Authenticating privileged and non-privileged users through PIV credentials is a best practice and supports requirements from OMB Memorandum 05-24 [14], OMB Memorandum 11-11 [15], and the CSIP [1] to use PIV credentials for employees and contractors accessing Federal systems. This document provides concrete technical options agencies can select from to enable PIV for LOA-4 use cases and can be applied to users and systems in lesser assurance use cases. This document recommends LOA-4 or LOA-3 PIV authentication for privileged authentication.

For those systems that do not support PIV authentication at all or do not support it at the appropriate level of assurance (LOA-3 or LOA-4 for privileged accounts), establish a plan of action and milestones (POA&M) to transition from the system's technology to a technology that supports PIV authentication at the appropriate level of assurance. The POA&M will allow the agency to resolve the issue within an acceptable time period. Until the issue is resolved, the agency should consider more frequent monitoring and access reviews (for example, every week) for the affected privileged users and accounts.

As mentioned in Section 1.4, multiple levels of assurance are possible using PIV credentials. Section 6.1.1 of FIPS 201 [5] specifies that: "In the context of the PIV Card, owners of logical resources shall apply the methodology defined in [OMB0404] to identify the level of identity authentication assurance required for their electronic transaction." Therefore, agencies should supplement their risk management processes with guidance from OMB M-04-04 [7], which takes into account the potential impact of a failed authentication transaction or fraudulent identity gaining unauthorized access to Federal systems. This assessment should apply in the context of enterprise risk of authentication vulnerabilities throughout its technical architecture, such as databases, webservers, and network devices, for both regular users that access the system via client software, and privileged users that may have access to portions of the system. Analyzing risks according to this process will allow agencies to determine the most appropriate level of assurance for the system. This helps the agency determine the best approach for PIV enabling the system not only for privileged users but also for typical system users.[12]

As Section 2.4.1 indicates, a direct[13] or LOA-4 indirect PIV architecture is required for any system that has been assessed at LOA-4. This white paper details best practices to meet LOA-4 requirements; however, it also lists PIV approaches for systems assessed at LOA-3 and provides guidelines for systems that can only implement lower levels of assurance that need to transition to LOA-4 or LOA-3 architectures.

The approaches also promote continued and consistent use of PIV credentials as intended by HSPD-12. These approaches should meet NIST SP 800-63 LOA-3 requirements for mitigating vulnerabilities associated with authentication assertions.

DRAFT

---

[12] For additional recommendations on applying the e-Authentication risk assessment from M-04-04 to determine the impact of failed authentication for privileged users, agencies may also use the toolkit provided by Federal Identity, Credential, and Access Management (FICAM). [13]

[13] The direct approach will only achieve LOA-3 if the user authenticates with a Derived PIV Credential and the corresponding private key is implemented in software and/or if the credential is issued in accordance with LOA-3 issuance requirements.

2.4 Select the Appropriate PIV Authentication Architecture

There are three high-level architectures for PIV-enabled systems. While PIV Authentication certificates and some Derived PIV Authentication certificates are capable of providing level of assurance 4, some architectures will result in the PIV-enabled system receiving a lower level of assurance. For each system to be PIV enabled, agencies should implement the architecture that provides the highest level of assurance possible, given the system's capabilities. Should the system's technical capability fall short with respect to the determined level of assurance, compensating security controls should be implemented as described in Section 3.2 of NIST SP 800-53 Revision 4 [3]. Additional information on the security controls from NIST SP 800-53 most closely related to PIV-based privileged user authentication is available in Section 2.5 of this white paper.

2.4.1 Direct and Indirect Verification Architectures

Figure 1 shows two high-level architectures for PIV-enabled systems.

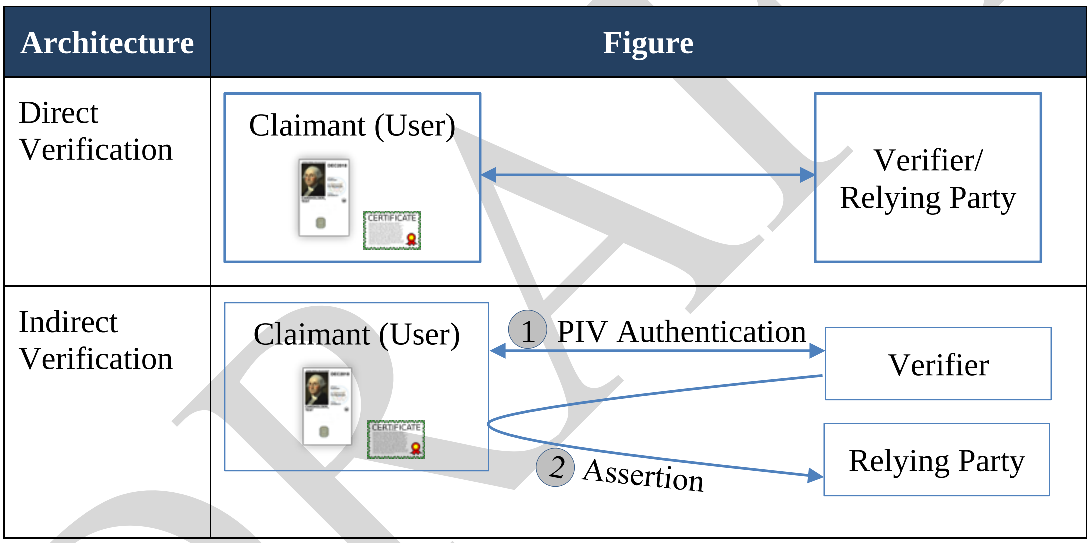


Figure 1: High-Level Architectures for PIV-Enabled Systems

Figure 1 and the corresponding architecture discussions in this section and Section 2.4.2 use terminology from NIST SP 800-63 [2]. The user trying to gain access to the privileged account is the *Claimant*, the system that hosts the privileged account is the *Relying Party*, and the system that performs PIV authentication in order to authenticate the user's identity is the *Verifier*. In all cases, the Verifier authenticates the Claimant using PKI-based authentication, which involves validating the Claimant's PIV Authentication certificate or Derived PIV Authentication certificate, and using the public key in the certificate to verify the signature on a data object signed using the corresponding private key.[14]

Direct Verification. In the direct verification architecture, the Relying Party is also the Verifier. Because this minimizes the number of components, and having more components generally

[14] See Section 6.2.3.1 of FIPS 201-2 [5] for an example of PKI-based authentication using the PIV Authentication certificate.

creates additional attack vectors, direct verification is the preferred architecture. The direct verification architecture provides the Relying Party with LOA-4 authentication if PIV Authentication is used. The direct architecture can also provide LOA-4 for a Derived PIV Authentication certificate issued in accordance with the requirements of LOA-4, but also LOA-3 authentication when issued in accordance with the requirements of LOA-3. An example of the direct verification architecture is when accounts are accessed through a web browser, TLS is used to protect communication between the client and the server, and certificate-based client authentication is used. With certificate-based client authentication, the client needs to send a certificate (the PIV Authentication certificate or Derived PIV Authentication certificate) to the server and use the corresponding private key to sign transaction data in order for the TLS session to be established. The server also checks that the client's certificate is valid prior to establishing the TLS session.

Indirect Verification. In many cases, the Relying Party is not able to perform PKI-based authentication, so an alternative means for authenticating the Claimant needs to be used. In the indirect verification architecture, the user authenticates to a Verifier that is not the Relying Party, after which the Verifier provides the Relying Party with an assertion that the user's identity has been verified. As described in Section 9 of NIST SP 800-63 [2], which provides detailed requirements for use of assertions, some assertion mechanisms can provide e-authentication level 4 assurance to the Relying Party (e.g., Kerberos), and such mechanisms are preferred and should be employed whenever possible, if the indirect verification architecture is used.[15]

The Kerberos Network Authentication Protocol [16] is commonly used to implement indirect verification, and it can be implemented in such a way that it provides e-authentication level 4 assurance to the Relying Party. The assertions created by the Verifier in Kerberos are called Kerberos tickets, and they include symmetric session keys that allow the Relying Party to perform a strong cryptographic authentication of the Claimant. The overall authentication process must ensure that the Claimant uses a PIV credential to authenticate to the Verifier before access is granted by the Relying Party. This requirement is satisfied if the Verifier is configured to only accept PIV authentication, and this is the recommended approach.

Security Assertion Markup Language (SAML) bearer assertions [17] are also commonly used to implement indirect verification. Unlike Kerberos, with bearer assertions SAML assertions are typically bearer assertions; the Claimant authenticates to the Relying Party by simply providing a copy of the assertion that it got from the Verifier. So, unlike Kerberos, an attacker could defeat the authentication mechanism by obtaining a copy of the assertion.[16] For this reason, bearer assertions provide a lower level of assurance to the Relying Party (at most LOA-3), and should not be used to enable privileged access if stronger mechanisms can be implemented.

DRAFT

[15] Note that if the Claimant authenticates to the Verifier using a certificate that was issued at LOA-3 (i.e., a Derived PIV Authentication Certificate), then the level of assurance provided to the Relying Party will be at most LOA-3, regardless of the verification architecture used.

[16] SAML also supports holder-of-key assertions, which require the Claimant to prove possession of a key to the Relying Party. Holder-of-key assertions can be implemented in a way that provides up to LOA-4 to the Relying Party.

Some indirect verification architectures may use assertions that only provide LOA-2 authentication (e.g., unsigned bearer assertions). Agencies using such an architecture should establish a POA&M to transition to a technology that supports PIV using the direct or indirect verification architecture at LOA-3 or LOA-4.

2.4.2 Transitional Proxy Architecture

The direct and indirect verification architectures require Relying Party systems that can either perform PKI-based authentication or accept identity assertions. Some systems, however, cannot do either. For example, an appliance firewall may only support password authentication for administrative access. In cases such as this, the use of a Proxy architecture is the only option. The proxy architecture is a less secure approach than the direct or the indirect architecture, but it does strengthen the overall security of the username/password-only system and allows for a grace period until transitioning to products that support direct or indirect verification architectures at LOA-3 or LOA-4 is possible.

Figure 2 shows a high-level depiction of the Proxy architecture. The Proxy is placed between the user (Claimant) and the Relying Party, so that it is only possible to gain privileged access to the Relying Party after successfully authenticating to the Proxy. The Proxy needs to be PIV enabled, and it may be PIV enabled either by acting as the Verifier itself (direct verification) or by accepting identity assertions from a separate PIV-enabled Verifier (indirect verification).

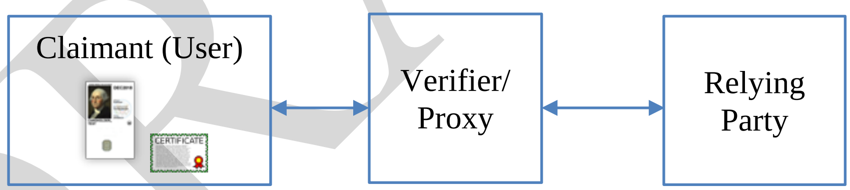
Architecture	Figure
Transitional Proxy	

Figure 2: High-Level Transitional Proxy Architecture

Proxy architectures will typically provide at most LOA-2 authentication, as these architectures are limited by the strength of the identity assertions made by the Verifier to the Relying Party. As such, transition away from the Proxy architecture is needed. Agencies should establish a POA&M to help with the transition to a technology that supports PIV using the direct or indirect verification architecture at the appropriate level of assurance (see the Section 2 introduction and Section 2.3).

Implementers of the Proxy architecture should ensure that they:

- Isolate the Relying Party system from all untrusted systems. This includes designing and configuring network architectures so that all privileged access to the Relying Party system flows through the Proxy.

DRAFT

- Segment internal networks to restrict the ability for a compromise of the Proxy to spread to other systems.
- Authenticate and encrypt all communications between users (Claimants) and the Proxy.
- Log and regularly review all activities occurring within the Proxy host to identify abnormal and questionable activities, and generate alerts as appropriate.
- Harden the Proxy's host using industry and government recommended security practices.[17] This includes:
    - Keeping the operating system and applications fully patched and up to date[18]
    - Ensuring that the host cannot initiate outbound traffic to the Internet
    - Allowing the Proxy to execute only the authorized applications that are necessary for the Proxy to perform its duties[19]
- Implement automated monitoring and access reviews (for example, every other week) for privileged users and accounts on systems that utilize the Proxy architecture.

2.5 Select and Implement Other Necessary Security Controls

Although this section focuses on best practices for PIV-enabling Federal information systems to strengthen privileged user authentication, these best practices assume that other security controls related to privileged user authentication and access are already in place. Agencies should follow standard risk management processes, which are defined by the NIST RMF [12], to identify all risk associated with privileged user authentication. Agencies are then responsible for mitigating their risk to an acceptable level through selection, implementation, and ongoing management of the necessary security controls.

Controls in the NIST SP 800-53 [3] catalog that may be particularly helpful for supporting PIV-based privileged user authentication are listed in Table 1. Other security controls are also relevant, and it is outside the scope of this white paper to identify which security controls are applicable for any given organization, environment, or system affected by the implementation of PIV-based privileged user authentication.

DRAFT

---

[17] NIST hosts the National Checklist Program for IT Products, which provides a repository of industry and government-created security checklists. For more information, visit the checklist repository at http://checklists.nist.gov or see the latest revision of NIST SP 800-70 at http://csrc.nist.gov/publications/PubsSPs.html.

[18] For more information on patch management, see NIST SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies* (http://dx.doi.org/10.6028/NIST.SP.800-40r3).

[19] One way of achieving this is through a combination of operating system access control lists to restrict application installation and application whitelisting technologies to restrict application execution. For more information on application whitelisting, see NIST SP 800-167, *Guide to Application Whitelisting* (http://dx.doi.org/10.6028/NIST.SP.800-167).

Table 1: Mapping PIV-Based Privileged User Authentication to Selected NIST SP 800-53 Controls

NIST SP 800-53 Control Number and Name	Applicability to Privileged User Authentication
AC-1, Access Control Policy and Procedures	Establish and maintain policy and procedures for roles, responsibilities, and other aspects of enabling access through privileged accounts
AC-2, Account Management	Perform all duties associated with privileged account management, including creating, enabling, modifying, disabling, and removing privileged accounts, as well as specifying each account's privileges. Monitor all privileged account use. Ensure that all requests for access to existing privileged accounts or for creation of new privileged accounts are authorized. Also AC-2 control enhancements of particular interest include (3), (4), and (11).
AC-3, Access Enforcement	Enforce logical access processes related to privileged account management. Also, AC-3 control enhancements of particular interest include (2).
AC-5, Separation of Duties	Assign privileges so that no single privileged user has excessive privileges to avoid violating the separation of duties principle.
AC-6, Least Privilege	See the guidelines in Section 2.2 for details on achieving the principle of least privilege for privileged accounts. Also, AC-6 control enhancements of particular interest include (1), (2), (3), (5), (6), (7), (9), and (10).
AC-7, Unsuccessful Logon Attempts	Limit consecutive authentication failures for privileged accounts.
AC-11, Session Lock	Lock a privileged user's privileged session after a period of inactivity or upon user request.
AC-12, Session Termination	Terminate a privileged user's privileged session after a period of inactivity or upon user request.
AC-17, Remote Access	Restrict which systems can be accessed remotely by privileged users and what actions those users can perform on each system via remote access. Also see AC-17 control enhancement (4).
AU-3, Content of Audit Record	Determine if the information system generates audit records.
AU-2, Audited Events	Ensure that the system logs the appropriate events related to privileged account use.
AU-6, Audit Review, Analysis, and Reporting	Review audit records for privileged accounts to identify inappropriate or unusual activity. Report all such activity to the appropriate personnel. Also see AU-6 control enhancement (8).
AU-12, Audit Generation	Generate one or more audit records for every action taken using a privileged account.
CA-7, Continuous Monitoring	Ensure that all usage of privileged accounts is continuously monitored to provide rapid identification of threats.
CM-5, Access Restrictions for Change	Limit the ability to make approved changes to systems to qualified and authorized privileged users.
IA-1, Identification and Authentication Policy and Procedures	Establish and maintain policy and procedures related to identifying and authenticating privileged users.
IA-2, Identification and Authentication (Organizational Users)	Uniquely identify and authenticate each privileged user. Also, see IA-2 control enhancements (1), (3), (6), (8), (11), and (12).
IA-4, Identifier Management	Manage information system identifiers for all privileged users.
IA-5, Authenticator Management	Manage information system authenticators for all privileged users. IA-5 control enhancements of particular interest include (1), (2), and (11).

NIST SP 800-53 Control Number and Name	Applicability to Privileged User Authentication
IA-8, Identification and Authentication (Non-Organizational Users)	Uniquely identify and authenticate each privileged user. Also, see IA-8 control enhancements (1) and (5).
SC-8, Transmission Confidentiality and Integrity	Protect the confidentiality and integrity of all communications related to privileged user authentication and privileged sessions.
SC-10, Network Disconnect	Terminate network connections from privileged accounts after a defined period of inactivity.
SI-2, Flaw Remediation	Apply patches and other updates to correct vulnerabilities in protocols, services, etc. used for privileged user authentication.
SI-4, Information System Monitoring	Perform ongoing monitoring of all privileged account usage. SI-4 control enhancements of particular interest include (20).

Similarly, major security features of PIV-based privileged user authentication map to subcategories from the NIST Cybersecurity Framework [18] as shown in Table 2.

Table 2: Mapping PIV-Based Privileged User Authentication to Selected NIST Cybersecurity Framework Subcategories

NIST Cybersecurity Framework Subcategory	Applicability to Privileged User Authentication
PR.AC-1: Identities and credentials are managed for authorized devices and users	Manage information system identifiers and authenticators for all privileged users.
PR.AC-3: Remote access is managed	Restrict remote access to systems by privileged users.
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.	See the guidelines in Section 2.2 for details on achieving the principles of least privilege and separation of duties for privileged accounts.
PR.AT-2: Privileged users understand roles & responsibilities	Educate all privileged users on best practices for safeguarding their privileged access to systems.
PR.DS-2: Data-in-transit is protected	Protect the confidentiality and integrity of all communications related to privileged user authentication and privileged sessions.
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Generate one or more audit records for every action taken using a privileged account. Review audit records for privileged accounts to identify inappropriate or unusual activity. Report all such activity to the appropriate personnel.
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	Specify the system access and privileges authorized for each privileged account.

DRAFT

3 Summary and Future Collaborative Work

Authentication of users for access to privileged accounts requires a high level of assurance in the user's identity (LOA-4 or LOA-3, depending on the criticality of the privileged access to the system). PIV-enabling systems for privileged user access can provide this high level of authentication assurance. Using the authentication architectures described in this white paper, agencies have the tools to map their systems to the assurance levels they require and implement additional controls, should a system's existing controls fall short of the level of assurance deemed appropriate. In addition to implementing additional controls, agencies are advised to only use PIV-enabling architectures that provide less than LOA-3 authentication (e.g., proxy architectures, indirect verification using unsigned bearer assertions) on a temporary basis, while implementing a POA&M to transition to systems that support stronger PIV authentication architectures.[20]

As an aid to departments and agencies, during the Sprint Federal agencies reported on the successes and challenges with PIV-enabling privileged account access. Reported successes were collected at MAX.gov[21] to share with agencies. The content of MAX.gov will be converted to Federal Identity, Credential, and Access Management (FICAM) playbooks, as appropriate by FICAM. NIST will contribute to the playbooks as it continues to engage with the vendor/industry community in the future.

DRAFT

[20] The Proxy architecture provides less than LOA-3 authentication and so do some types of assertions that would be used in an indirect verification architecture.

[21] https://community.max.gov/display/Egov/CIO+Council+Knowledge+Portal

Appendix A—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

CSIP	Cybersecurity Strategy and Implementation Plan
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
HSPD	Homeland Security Presidential Directive
IT	Information Technology
ITL	Information Technology Laboratory
KDC	Key Distribution Center
LOA	Level of Assurance
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OMB	Office of Management and Budget
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
RFC	Request for Comments
RMF	Risk Management Framework
SAML	Security Assertion Markup Language
SP	Special Publication
TLS	Transport Layer Security

DRAFT

Appendix B—References

[1] Office of Management and Budget (OMB), OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, October 30, 2015. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf [accessed 11/12/2015]

[2] W. Burr, D. Dodson, E. Newton, R. Perlner, W. Polk, S. Gupta, and E. Nabbus, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-2, *Electronic Authentication Guideline*, August 2013. http://dx.doi.org/10.6028/NIST.SP.800-63-2

[3] Joint Task Force Transformation Initiative, National Institute of Standards and Technology (NIST) SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4

[4] Department of Homeland Security (DHS), *Homeland Security Presidential Directive 12 (HSPD-12): Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004. http://www.dhs.gov/homeland-security-presidential-directive-12 [accessed 11/12/2015]

[5] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf [accessed 11/12/2015]

[6] H. Ferraiolo, D. Cooper, S. Francomacaro, A. Regenscheid, J. Mohler, S. Gupta, and W. Burr, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, December 2014. http://dx.doi.org/10.6028/NIST.SP.800-157

[7] Office of Management and Budget (OMB), OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf [accessed 11/12/2015]

[8] K. Dempsey, N. Chawla, A. Johnson, R. Johnston, A. Jones, A. Orebaugh, M. Scholl, and K. Stine, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011. http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf [accessed 11/24/2015]

[9] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf [accessed 11/12/2015]

DRAFT

[10] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf [accessed 11/16/2015]

[11] D. Cooper, H. Ferraiolo, K. Mehta, S. Francomacaro, R. Chandramouli, and J. Mohler, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-73-4, *Interfaces for Personal Identity Verification – Part 1: PIV Card Application Namespace, Data Model and Representation*, May 2015. http://dx.doi.org/10.6028/NIST.SP.800-73-4

[12] Joint Task Force Transformation Initiative, National Institute of Standards and Technology (NIST), Special Publication (SP) 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010. http://dx.doi.org/10.6028/NIST.SP.800-37r1

[13] Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions, *Determination of Identity Assurance Level Requirement for Agency Applications Accepting FICAM TFS Approved Third Party Credentials*, Version 1.0.0. http://www.idmanagement.gov/sites/default/files/documents/FICAM_TFS_Determine_Required_LOA.pdf [accessed 11/12/2015]

[14] Office of Management and Budget (OMB), OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, August 5, 2005. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf [accessed 11/12/2015]

[15] Office of Management and Budget (OMB), OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors*, February 3, 2011. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf [accessed 11/23/2015]

[16] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 4120, *The Kerberos Network Authentication Service (V5)*, July 2005. http://www.ietf.org/rfc/rfc4120.txt [accessed 11/12/2015]

[17] Organization for the Advancement of Structured Information Standards (OASIS), *Security Assertion Markup Language (SAML) v2.0*, March 2005. http://www.oasis-open.org/standards#samlv2.0 [accessed 11/12/2015]

[18] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014. http://www.nist.gov/cyberframework/index.cfm [accessed 11/18/2015]

DRAFT

[19] L. Zhu and B. Tung, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 4556, *Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)*, June 2006. https://www.ietf.org/rfc/rfc4556.txt [accessed 11/25/2015]

DRAFT