Authentication, Authorization, and Audit

Design Pattern:

Internal User Identity Authentication

Office of Technology Strategies (TS)
Architecture, Strategy, and Design (ASD)
Office of Information and Technology (OIT)

Version 1.1

Date Issued: April 23, 2014

THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

APPROVAL COORDINATION

Date: MAY 6, 2014

Mr. Joe Paiva
Chief Technology Strategist
OIT Architecture, Strategy, and Design (ASD)

Date: 8 Jul 14

Dr. Paul Tibbits, M.D.
Deputy Chief Information Officer (DCIO)
OIT Architecture, Strategy, and Design (ASD)

REVISION HISTORY

Version Number	Date	Organization	Notes
0.6	02/21/14	ASD TS	Initial Draft
0.8	03/14/14	ASD TS	Edits incorporated from vendor engagement meetings, and feedback from ASD's Enterprise Shared Services Security Group
0.9	03/28/14	ASD TS	Edits incorporated from DISA and NIST engagement meetings, and feedback from ASD's Enterprise Share Services Security Group. Technical edit completed Major changes include: • Removal of duplicative language in an effort to shorten the document • Refocused the document around the 'Core Concepts' related to each area • Updated section 3 to reflect ESS Security recommendation to show which authentication protocol was the primary choice for VA and included exception criteria
1.0	04/07/14	ASD TS	Finalized edits to the design pattern for presentation at the 04/09/14 Public Forum
1.1	04/23/14	ASD TS	Incorporated Feedback from the Public Forum

REVISION HISTORY APPROVALS

Version	Date	Approver	Role
0.6	02/21/14	Dusty Jackson	ASD TS AA&A Design Pattern Lead
0.8	03/14/14	Dusty Jackson	ASD TS AA&A Design Pattern Lead
0.9	03/28/14	Dusty Jackson	ASD TS AA&A Design Pattern Lead
1.0	04/07/14	Dusty Jackson	ASD TS AA&A Design Pattern Lead
1.1	04/23/14	Dusty Jackson	ASD TS AA&A Design Pattern Lead

TABLE OF CONTENTS

1 Introduction 1
1.1 Background 1
1.2 Business Need 2
1.3 Scope 2
1.4 Document Development and Maintenance 3
2 Design Pattern Description 3
2.1 Internal User Identity Authentication 3
2.2 Authentication to VA Networks 4
2.3 User Credentials 4
2.4 Levels of Assurance (LOA) Framework 5
LOA 2 8
LOA 3 8
LOA 4 8
Other Security Controls 9
2.5 Enterprise Shared Services 9
2.6 Adaptive Authentication Requirements 11
3 Design Pattern Architecture 12
3.1 Deciding Which Authentication Protocol to Implement 14
3.2 Application of Design Pattern to Authentication Protocols 14
3.3 VA Authentication Protocol Teams 20
Appendix A. Acronyms 21
Appendix B. Use Cases 23
Appendix C. References/Applicable Standards 24
Appendix D. Level of Assurance (LOA) Requirements 26

TABLE OF FIGURES

Figure 1 - Current Internal User Identity Authentication 1
Figure 2 - Design Pattern for Internal User Identity Authentication 13
Figure 3 - Single Sign-On Internal 15
Figure 4 - Direct Client Authentication Using PKI over TLS 17
Figure 5 - Kerberos Authentication 18

TABLE OF TABLES

Table 1 - Level of Assurance Overview 7
Table 2 - Identity Credential Mapped to LOA 13
Table 3 - Authentication Protocol Mapped to LOA 14
Table 4 – Responsible Integration Teams for Internal User Authentication Protocols 20

1 INTRODUCTION

1.1 Background

Office of Management and Budget (OMB) M 11-11 mandates that agencies "require the use of PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems." The Department of Veterans Affairs (VA) currently allows the use of non-standardized processes to conduct internal VA user identity authentication to the network and to applications. VA has implemented policy that will require the use of Public Key Infrastructure (PKI) enabled Personal Identity Verification (PIV) cards to enable internal user identity authentication to Active Directory (AD) (the "Network"). However, VA currently allows internal user identity authentication via the user's AD username and password. Additionally, internal user identity authentication to the application layer is allowed via various non-standardized protocols. While all applications are currently required to comply with standardized security requirements established in VA 6500 and National Institute of Standards and Technology (NIST) 800-53, to date, VA has not standardized accepted authentication protocols.

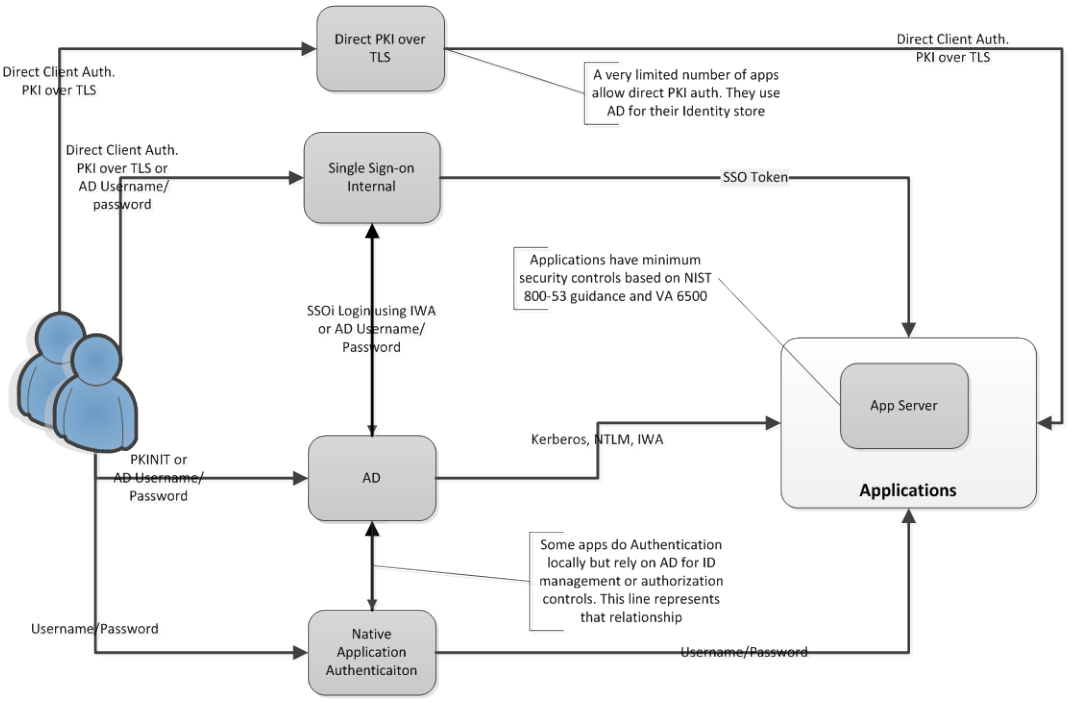

Figure 1 - Current Internal User Identity Authentication

Current user identity authentication protocols include:

- **Application Specific Authentication** – Some applications natively authenticate users, maintaining their own user store (e.g., user authentication to VistA is currently natively supported.)
- **Kerberos/NTLMV2** – Many VA applications currently leverage a Microsoft (MS)-based token system to allow user authentication. These MS processes leverage Active Directory.
- **PKI Authentication** – VA network authentication and a limited number of applications use PKI technology.

- **IAM Single Sign-On Internal (SSOi)** - Some applications have migrated to SSOi authentication services. SSOi can support PKI, AD username/password, and Kerberos. SSOi is only used by internal VA users.
- **IAM Single Sign-On External (SSOe)** – SSOe is used to authenticate external users to VA systems. This system is outside the scope of this document.

(This list is not intended to be exhaustive; other authentication protocols may be in use.)

1.2 Business Need

The purpose of the Authentication, Authorization & Audit Increment 1 Design Pattern is to provide standardized enterprise-level direction for internal VA user identity authentication. This design pattern is one part of a set of design patterns that will be produced for Authentication, Authorization & Audit.

To perform proper authentication, information system owners must use approved identity authentication procedures that consider the importance and sensitivity of the information in a system, recognize the threats and vulnerabilities to the system, consider the level of confidence in any user's asserted identity, and understand the risks that are posed to the enterprise by the potential loss or exposure of information contained in the system.

VA is adopting standardized enterprise design patterns to ensure appropriate security controls are maintained and standard designs are implemented throughout the Department. As VA moves towards implementing enterprise shared services (ESS), design patterns will guide application development and set boundaries to ensure solutions support VA's information technology (IT) model as outlined in:

- **VA Enterprise Shared Services (ESS) Strategy Draft Version v0.7**
- **Enterprise Application Architecture v 1.1**
- **VA SOA Technical Framework v 1.1**
- **Federal Enterprise Architecture Framework (FEAF) v 2.0**

To support the move to enterprise authentication services, VA is adopting a NIST risk management framework, NIST 800-63: Electronic Authentication Guideline. NIST 800-63 contains standards for rating applications at their required Level of Assurance (LOA) and aligning appropriate authentication protocols to the level of risk posed by those applications. Standardization of these authentication protocols and technologies used by these applications will simplify application design, increase network security, and allow for proper user management.

It should be noted that NIST 800-63 establishes the, "low bar," or minimum requirements for user identity authentication. Business owners, Application owners, and developers must meet these minimum requirements; however, they should fully understand that these are the minimal security requirements. Implementation of higher security requirements is encouraged wherever possible.

1.3 Scope

This design pattern describes the "to-be" state for VA internal user (PIV enabled VA employees, contractors, and volunteers) identity authentication. In addition to describing the "static" rules for authentication the design pattern describes "adaptive" authentication tools that will be implemented and the need for authentication protocols that can support attribute- and risk-based access controls.

- This pattern does not address further authentication processes that may occur after internal users are authenticated to applications, such as application to application data calls, nor does it address standards for passing user authentication data for the purposes of making authorization decisions, as in the Service-oriented Architecture (SOA) model.
- This pattern does not address user identity authentication for external users, defined as Veterans, Veteran Service Organizations (VSOs), other federal users, or other stakeholders who may require access to the VA network or VA systems on occasion.
- This pattern does not address requirements for authenticating devices (non-person entities).
- This document is not a technical implementation guide, but is intended to guide application design by setting appropriate boundaries for designers. Information on technical implementation of these authentication protocols can be obtained from the appropriate OIT teams outlined in table 4.
- While technologies (Token, Kerberos, Direct Client PKI) will be specified in this design document, it is vendor agnostic.

1.4 Document Development and Maintenance

This design pattern was developed collaboratively with stakeholders from the ESS Security Group and included participation from VA's Office of Information and Technology (OIT), Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). In addition, the Technology Strategies team engaged industry, external government agencies, and academic experts to review, provide input, and comment on the proposed pattern.

This document contains a revision history and revision approval logs to track all changes. Updates will be coordinated with the Office of Technology Strategies' lead for this document; they will facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

2 DESIGN PATTERN DESCRIPTION

This design pattern provides an overview of the user identity authentication processes and capabilities that VA will implement. It supports the Enterprise Technology Strategic Plan vision for the expanded use of ESS that support VA's goals of increasing security, decreasing total cost of ownership (TCO) and increasing information re-use/agility.

2.1 Internal User Identity Authentication

Identity authentication for information systems and networks within VA must be conducted in a manner that: provides confidentiality by preventing unauthorized access; provides integrity that protects against unintentional or malicious change; and provides availability of data for users. To perform proper authentication, information system owners must use identity authentication protocols that consider the importance and sensitivity of the information in a system, recognize the threats and vulnerabilities to the system, consider the level of confidence in any user's asserted identity, and the impairment or destruction that could be inflicted on the information system.

To conduct reliable internal user identity authentication, information system owners shall choose the specific type(s) of identity credential used in an identity authentication process based on the sensitivity of the information that can be accessed, the strength of the identity credential, and the environment where the identity credential is being presented.

2.2 Authentication to VA Networks

Core Concepts:

1. **Direct PKI shall be the default protocol used to access VA networks**: Authentication to VA networks shall be accomplished with direct client authentication using PKI over Transport Layer Security (TLS) sessions (*some exceptions to this model may exist, but they are extremely limited.)*
    - Where exceptions apply, controls must properly limit user access to the LOA of the user's primary authentication

VA policy has established PIV only Authentication (POA) to the VA network. VAIQ #7100147 states, "In accordance with Office of Management and Budget (OMB) Memorandum 11-11, *Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors,* dated February 3, 2011, the use of PIV credential is required as the common means of authentication for access to VA's facilities, networks and information systems."

Exceptions to PKI Authentication
VA policies governing temporary network or application access, in the case of forgotten, lost, or stolen PIV cards, must comply with LOA guidance and core concepts in section 2.3. Use of Active Directory username and password to access applications rated above LOA 2 is prohibited.

2.3 User Credentials

Core Concepts:

1. **User credentials shall be appropriate for use in the requested environment:** Information system or VA network shall ensure that any credential used for identity authentication is appropriate for the authenticating entity's environment and the sensitivity level of the information for which the information system facilitates access.
2. **Information system or VA network shall ensure that any credential used for identity authentication has been issued by an approved VA identity credential provider or an approved federal or industry partner identity credential provider.**
3. **Information system or VA network shall verify that any identity credential used for identity authentication has not been revoked:** Information systems or the VA network must check to ensure that the identity credential presented has not been revoked by the identity credential provider or otherwise declared invalid.
4. **Information system or VA network shall only permit authentication to users who present identity credentials at or above the required LOA for the requested resource**

All VA information systems and networks shall be capable of distinguishing and limiting user identity authentication to users who have presented identity credentials which meet the required LOA for the resource which they are attempting to access.

Information systems or networks must perform checks of the identity credential upon presentation for authentication to ensure that the credential:

- Was issued by a VA identity credential provider
- Has not been revoked by the identity credential provider or otherwise declared invalid

In situations where automated credential checking is not available, the information system or network shall perform credential revocation checking in accordance with applicable credential policy**.**

The information system shall validate during logon that the authenticator is bound to the identity credential used in the identity authentication process.

The information system or network shall implement rules-based processes for mapping an authenticated identity to a network or information system account or role.

Types of User Credentials
The primary identity credentials available to internal VA users for identity authentication are:

- **VA-issued PIV Cards:** PIV cards and PKI authentication are LOA 4 credentials and are acceptable for authentication to all four LOAs depending on the authentication protocol used by the application. ***The PIV card is the default authentication identity credential for all internal VA users.***
- **Active Directory Username and Password:** AD username and password are LOA 2 credentials and are only acceptable for temporary authentication to LOA 2 or lower rated applications.
- **Other Credentials:** VA may choose to implement other identity credentials for allowing temporary access to the VA network and applications. Any identity credential must be compliant with the NIST 800-63 LOA framework and guidelines, FICAM, FIPS, and VA 6500 security controls.

2.4 Levels of Assurance (LOA) Framework

Core Concepts:

1. **VA Applications shall be assessed and implement LOA requirements for authentication:** VA shall implement guidance in OMB 04-04 and NIST 800-63 to rate all existing applications to their appropriate LOA and enforce strict and appropriate security controls for user authentication to those applications.
2. **LOA for user authentication shall be determined by the weakest link in the authentication process**
3. **Application authentication protocols shall comply with all existing guidance established in VA 6500**

To determine the required LOA, application managers and developers will follow OMB guidance. OMB outlines a five-step process by which agencies should meet their authentication assurance requirements.

1. **Conduct a risk assessment of the application/system** – NIST SP 800-30 offers a general process of risk assessment and risk mitigation. VA's Office of Information Security shall provide additional guidance for conducting assurance risk assessments inside VA. Application developers in concert with the respective business owners will conduct this assessment and present the results to IAM and OIS.
2. **Map identified risks to the appropriate assurance level** – OMB M-04-04 provides guidance for this mapping.

3. **Select technology based on authentication technical guidance** – VA's default authentication protocol is the use of IAM single sign-on internal for all internal user identity authentications. Applications that meet exception criteria, outlined in section 3.1, may be required to use direct client authentication using PKI over TLS or may use Kerberos if approved.
4. **Validate the implemented system has met the required assurance level** – OIT OIS will use NIST SP 800-53A to conduct an assessment to determine if the application has meet the required LOA standards.
5. **Periodically reassess the information system to determine technology refresh requirements** – NIST 800-37 revision 1 provides guidelines for periodic reassessments. Agencies should also follow assessment guidelines established in NIST SP 800-53.

Application managers and developers shall apply appropriate controls to the authentication protocol selected to ensure it meets the determined LOA's requirements. Details on the LOAs and requirements for applying different controls to Kerberos and single sign-on are detailed below.

The OMB 04-04 describes four levels of identity authentication assurance levels, with Level 1 being the lowest level of assurance and Level 4 being the highest level of assurance. Each assurance level describes the degree of confidence that the user that presented a credential (e.g., a password) is in fact that user. It should be noted that the four LOAs are established for the use of civilian agencies and do not apply to systems that rate as National Security Systems or contain classified or highly sensitive information. Standards for those systems are set by the National Security Administration (NSA) and are not described in this document.

The level of assurance needed is based on the consequence of authentication errors and/or misuse of credentials. As the consequences of an authentication error increase, the level of assurance should increase. Informal or low value requests will require less stringent assurance. Higher value or legally significant requests (e.g., HIPAA, PII) will require more stringent assurance.

Identified risks for a particular application should be mapped to a minimum assurance level based on potential impact. Assignment of impact to these risks is based on the context and nature of the people or entities affected by an improper authentication. For example, if five categories of potential impact are for Level 1 and one category of potential impact is for Level 2, the application should require Level 2 assurance.

Table 1 - Level of Assurance Overview

LOA	Description	Technical Requirements: Identity Proofing	Technical Requirements: Token (Secret) Requirements	Technical Requirements: Authentication Protection Mechanisms Requirements	Example of credentials meeting requirements
1	Little or no confidence exists in the asserted identity; usually self-asserted; essentially a persistent identifier	Requires no identity proofing	Allows any type of token including a simple PIN	Little effort to protect session from offline attacks or eavesdropper is required.	
2	Confidence exists that the asserted identity is accurate; used frequently for self service applications	Requires some identity proofing	Allows single-factor authentication. Passwords are the norm at this level.	Online guessing, replay and eavesdropping attacks are prevented using FIPS 140-2 approved cryptographic techniques.	Username and password
3	High confidence in the asserted identity's accuracy; used to access restricted data	Requires stringent identity proofing	Multi-factor authentication, typically a password or biometric factor used in combination with a 1) software token, 2) hardware token, or 3) one-time password device token	Online guessing, replay, eavesdropper, impersonation and man-in-the-middle (MitM) attack are prevented. Cryptography must be validated at FIPS 140-2 Level 1 overall with Level 2 validation for physical security.	OTP devices or X.509 user certificates
4	Very high confidence in the asserted identity's accuracy; used to access highly restricted data.	Requires in-person registration	Multi-factor authentication with a hardware crypto token (Use of barer SSO is not permitted)	Online guessing, replay, eavesdropper, impersonation, MitM, and session hijacking attacks are prevented. Cryptography in the hardware token must be validated at FIPS 140-2 level 2 overall, with level 3 validation for physical security	X.509 user certificates on a hardware token that is FIPS 140-2 compliant

(Detailed requirements for authentication at different LOAs are available in Appendix D)

LOA 1

LOA 1 applications are required to comply with security standards set forth by VA 6500, NIST 800-53, and NIST 800-63. There are no special internal user identity authentication requirements for LOA 1.

LOA 2

LOA 2 allows Direct PKI, SSOi, or Kerberos authentication technologies to be employed and permits the use of any of the token methods of Levels 2, 3 and 4. Successful authentication requires that the claimant shall prove, through a secure authentication protocol, that he or she controls the token. Session hijacking (when required based on the FIPS 199 security category), replay, and online guessing attacks shall be resisted. Approved cryptography is required to resist eavesdropping to capture authentication data. Protocols used at Level 2 and above shall be at least MitM resistant.

Session data transmitted between the claimant and the relying party following a successful Level 2 authentication shall be protected as described in the NIST FISMA guidelines. Specifically, all session data exchanged between information systems that are categorized as FIPS 199 "Moderate" or "High" for confidentiality and integrity, shall be protected in accordance with NIST SP 800-53 Control SC-8 (which requires transmission confidentiality) and SC-9 (which requires transmission integrity).

A wide variety of technologies can meet the requirements of Level 2. For example, a verifier might authenticate a claimant who provides a password through a secure (encrypted) TLS protocol session (tunneling).

LOA 3

Level 3 provides multi-factor network authentication. At least two authentication factors are required. LOA 3 is based on proof of possession of the allowed types of tokens through a cryptographic protocol. Level 3 also permits any of the token methods of Level 4. Refer to NIST 800-63 Section 6 for requirements for single tokens and token combinations that can achieve Level 3 authentication assurance. Additionally, at Level 3, strong cryptographic mechanisms shall be used to protect token secret(s) and authenticator(s). Long-term shared authentication secrets, if used, shall never be revealed to any party except the claimant and credential service provider (CSP); however, session (temporary) shared secrets may be provided to verifiers by the CSP, possibly via the claimant. Approved cryptographic techniques shall be used for all operations including the transfer of session data.

Level 3 assurance may be satisfied by client authenticated TLS (implemented in all modern browsers), with claimants who have public key certificates. Other protocols with similar properties may also be used.

Level 3 may also be met by tunneling the output of a multi-factor (MF) one-time password (OTP) token, or the output of a single factor (SF) OTP token in combination with a Level 2 personal password, through a TLS session.

LOA 4

Level 4 is intended to provide the highest practical network authentication assurance.

Level 4 requires strong cryptographic authentication of all parties, and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. The token secret shall be protected from compromise through the malicious code. Long-term shared authentication secrets, if used, shall never be revealed to any party except the claimant and CSP; however session (temporary) shared secrets may be provided to verifiers or Relying Party RPs by the CSP. Strong, approved cryptographic techniques shall be used for all operations including the transfer of session data. All

sensitive data transfers shall be cryptographically authenticated using keys that are derived from the authentication process in such a way that MitM attacks are strongly resisted.

Level 4 assurance may be satisfied by client authenticated TLS (implemented in all modern browsers), with claimants who have public key MF hardware cryptographic tokens. Other protocols with similar properties can also be used. It should be noted that, in multi-token schemes, the token used to provide strong MitM[1] resistance need not be a hardware token. For example, if a software cryptographic token is used to open a client-authenticated TLS session, and the output of a multifactor OTP device is sent by the claimant in that session, then the resultant protocol will still provide Level 4 assurance.

LOA Determined by "Weakest Link"

All elements of the user's authentication to an application factor into the LOA rating of the authentication: the user's identity credential; the in-direct client authenticator; the secondary authentication token; and, the application. The lowest LOA for any of these credentials, systems, tokens, or applications shall be the LOA for the entire process. For example, if an internal VA user authenticates to a VA active directory domain controller using direct PKI over TLS, a PIV card (LOA 4), the user then requests access to an application integrated with AD. AD authenticates the user to the application using the Kerberos protocol (LOA 2), and the application is rated at LOA 2. The LOA for this entire process would be LOA 2. Had the user attempted to access an application rated at LOA 3, the application or in-direct client authenticator should have prompted the user to re-authenticate at a higher LOA.

Other Security Controls

The LOA requirements outlined in NIST 800-63 are not the only requirements governing user authentication. All federal information systems must meet the minimum security requirements defined in FIPS 200. These requirements direct organizations to select/apply appropriate security controls as described in NIST 800-53. From this standard, VA's baseline security controls are contained and detailed in the VA 6500 Handbook. The combination of FIPS 200, NIST 800-53, and VA 6500 sets the foundational level of security for all information and information systems within VA. All foundational requirements in these documents that pertain to user authentication are required to be applied to the applications, systems, and authentication protocols within the authentication framework established by this document.

2.5 Enterprise Shared Services

Core Concepts:

1. **Enterprise Shared Services shall be used to support authentication, authorization, and auditing**
    - VA has begun implementing ESS through IAM's Access Services (IAM AcS) program which provides an enterprise provisioning service and user store, role based and attributed based access controls, authentication, and audit services.

[1] Man-in- the-Middle (MitM) Attack: is a form of active eavesdropping where an attacker inserts itself between victims (e.g. an AD Domain Controller and an application) and relays messages between them. In a MitM attack the affected parties believe they are talking directly to each other, but the conversation is controlled by the attacker. This allows the attacker to intercept messages, inject new messages, or redirect messages.

2. **Create enterprise identity and attribute management stores:** VA shall adopt the Master Veteran Index (MVI) as the central identity and attribute management structure. VA has identified the MVI as the appropriate enterprise identity store for VA (VAIQ #7011145). IAM Access Services (AcS) Provisioning Service provides an enterprise user store which contains internal and external users and is integrated with MVI. It is understood that the IAM AcS Provisioning Service will not be the only identity and attribute management store, but will be the central identity and attribute repository. The enterprise will implement a structure that allows federation of user identities and attributes across existing user stores.
3. **Applications shall rely on VA's central identity and attribute stores to conduct user authentication**
4. **Authentication protocols must support VA's Service Oriented Architecture (SOA) environment:** As VA moves to a SOA environment all authentication protocols must be implemented in a way that can support standards set by the SOA design pattern
5. **Applications shall support authentication protocols that support the implementation of enterprise wide role and attributed based access controls**

The VA Enterprise Shared Services (ESS) Security Model outlines the Department's goals for enterprise security services. "The VA Enterprise Application Architecture (EAA) specifies the use of SOA services as the basis for the development of VA systems and specifies the use of ESS to the degree feasible."[2] To support the adoption of this SOA based model, VA is currently developing enterprise security services that "…will provide confidentiality, integrity, and availability services for the VA's platform. Security services are implemented as protection services, such as authentication and authorization, detection services, such as monitoring and auditing, and response services, such as incident response and forensics."[3]

To fully leverage a SOA design in VA's future architecture, a centralized user identity and attribute management store must be created for internal VA users. VA has established the MVI as the unique user identity and attribute store. In its current state, MVI is used as the unique repository for Veteran and stakeholder identities. To complete the transition of MVI to VA's enterprise user identity store, IAM AcS Provisioning, which is integrated with MVI, is building connections to:

- VA's HR system (Personnel and Accounting Integrated Data (PAID)' s replacement, HR Smart)
- VA's current enterprise identity store, Active Directory
- MVI has also requested access to the VA's PIV card system

The "to-be" MVI will support unique identification of organizational users for authentication purposes.

Pro-path process (PRI-7) "Complete Identity Access Management Requirements" requires all projects evaluate their need for the use of ESS managed by the IAM team upon initiation.

Authentication and Authorization

[2&3] Department of Veteran Affairs, Enterprise Shared Services Security Model V0.6, p. 7-8

All authentication protocols shall be designed and implemented in such a way that they are capable of supporting the implementation of enterprise user authorization controls. Industry best practices for information security include the use of appropriate enterprise role-, attribute-, and risk-based access controls. The implementation of authorization controls relies on the use of supportive authentication protocols. Authentication protocols that can support transmission of user attributes can help facilitate the design and implementation of these advanced authorization controls.

2.6 Adaptive Authentication Requirements

Core Concepts:

1. **Implement LOA step up functionality and policy:** VA authentication protocols and applications must be able to trigger an LOA step up functionality that will require users who have accessed the network at a lower LOA to re-authenticate at a higher LOA when they attempt to access resources that are rated higher than their initial authentication would allow.
2. **Authentication protocols must support future role based and attribute based access control:** All approved authentication protocols must be implemented in a way that will support the enterprise in instituting role based and/or attribute based access control policies at the enterprise level.
3. **Implementation of functionality and policy to allow re-authentication challenges:** VA shall implement functionality and policies that allow re-authentication challenges to be issued to users based upon the future need for risk based access control.

Step-Up Authentication

Authentication protocols must have functionality in place to allow a user to re-authenticate to an appropriate LOA in order to access requested resources to which they have appropriate access rights. This "step-up" functionality allows the issuance of a new authentication challenge at any point in a user session during which an increase LOA authentication is necessary. The implementation of this functionality will allow VA to continue to properly secure applications and resources while providing a better user experience. An example of how this process might work is:

1. Internal VA user accesses the VA AD with a LOA 2 credential (MS username/password)
2. User requests access to an SSOi integrated application rated at LOA 3
3. SSOi, or the application, determines that the user's current LOA is not sufficient to access the requested resource
4. User redirected to SSOi login page and prompted to re-authenticate with LOA 3 or higher credential

Adaptive Authentication

VA Authentication protocols must be designed to allow the network to issue occasional re-authentication challenges to users per established policy. This functionality will allow VA to re-authenticate users at their current or higher LOA based on perceived or established risks associated with a user's session, behavior, or other established policy.

NIST 800-53 control IA-10: *Adaptive Identification and Authentication* allows organizations to employ these adaptive authentication controls requiring users to provide additional authentication information

based on assessed risks. Control IA-10 is also related to controls AU-6: *Audit Review, Analysis and Reporting,* and SI-4: *Information System Monitoring*.

3 DESIGN PATTERN ARCHITECTURE

The Internal User Authentication Design Pattern is intended to guide the use of enterprise user authentication protocols during development and provisioning of applications and services. Policies are already in place directing applications to leverage enterprise authentication services. The implementation of this design pattern will support adherence to those policies by all applications currently in use or under development within the VA.

Core Concepts:

1. **Information systems shall only conduct internal user identity authentication using approved authentication protocols.**
    - **Institute IAM single sign-on internal as the default authentication protocol:** SSOi shall become the default authentication protocol within VA. Exception criteria will direct the use of direct PKI or Kerberos as required.
    - **Where required, VA shall enable use of PIV cards for authentication at the application layer:** LOA 4 applications shall be required to fully leverage the PIV credential using direct PKI over TLS.

    a. **Use of application-specific authentication protocols is prohibited:** all VA applications shall rely on enterprise authentication services and enterprise identity management services for user authentication. ***Legacy systems that rely on native authentication processes will be evaluated and migrated to use an appropriate enterprise authentication protocol and enterprise identity management services***
2. **Federal security standards governing user authentication including NIST SP800-53 and VA Handbook 6500 shall be respected**
3. **Implement sufficient security controls within active directory and Kerberos:** VA shall ensure that its implementation of active directory and Kerberos within the department meets best practices for information security and is able to support NIST 800-63 requirements for authentication.

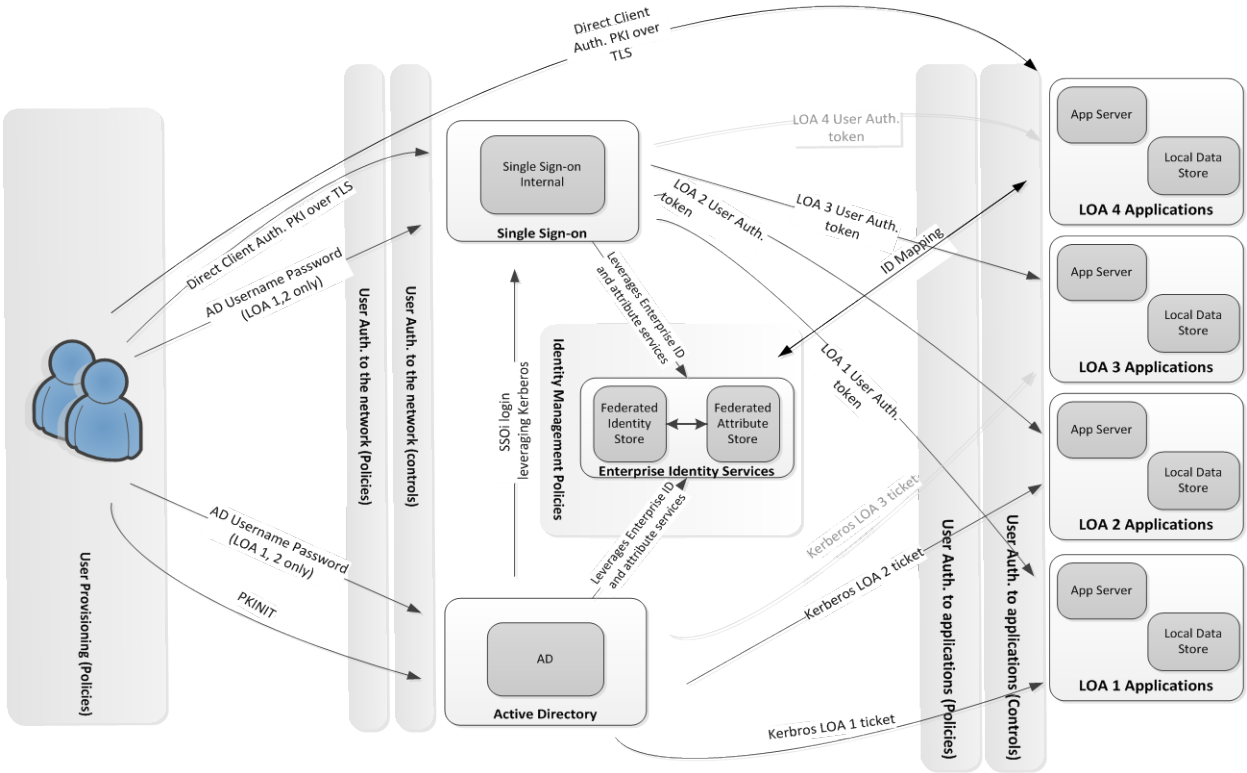

Figure 2 - Design Pattern for Internal User Identity Authentication

The Enterprise Design Pattern for Internal User Identity Authentication, Figure 2 (above), reflects the complex nature of the VA environment. Users will continue to have the ability to authenticate to VA networks or applications through the use of two primary identity credentials. The VA issued PIV card will be the default identity credential and the only means of obtaining access to applications and networks rated at all four of the LOAs. The use of AD username and password will be maintained for use by users on a temporary basis, but will be restricted to authentication to applications rated at LOA 2 or lower. VA may choose to implement additional identity credentials to allow temporary access to applications and networks at a LOA equal to the identity credential selected.

The table below shows how VA identity credentials for internal VA users map to their respective LOAs.

Table 2 - Identity Credential Mapped to LOA

	LOA 1	LOA 2	LOA 3	LOA 4
Direct PKI over TLS (PIV Card)	X	X	X	X
Active Directory Username and Password	X	X		

The Enterprise Design Pattern for Authentication reflects the authentication protocols which will continue to be available for application designers. Within VA, three (3) approved authentication protocols will exist:

- Direct client authentication using:
    1. PKI over TLS
- Indirect client authentication using:
    2. Single sign-on internal (SSOi)
    3. Kerberos (within active directory)

The need to use three protocols is reflective of the complex and diverse nature of the VA environment and it is important to understand when and how each of these protocols should be implemented. The following table, Table 3, provides a mapping of each authentication protocol to the LOAs defined by NIST and is meant to aid in selecting the appropriate protocol authentication of users to applications based upon level of risk.

Table 3 - Authentication Protocol Mapped to LOA

	LOA 1	LOA 2	LOA 3	LOA 4
Direct PKI over TLS	**X**	**X**	**X**	**X**
Single Sign-On Internal	**X**	**X**	**X**	(Not approved until holder of key technology is released and approved for use at LOA 4)
Kerberos	**X**	**X**	(Not approved under current AD and Kerberos implementation)	

3.1 Deciding Which Authentication Protocol to Implement

1. Applications are rated to their LOA using NIST SP 800-30 or other VA guidance issued by VA Office of Information Security (OIS)
2. Application owners access their ability to implement ***VA's default authentication protocol, SSOi***
    a. Applications that meet exception criteria (listed in section 3.2) should still be reviewed by the IAM team
3. Application owners work with the appropriate authentication protocol team and OIS to ensure that all necessary security standards are implemented
4. OIS conducts an assessment to ensure the application meets required security standards.

3.2 Application of Design Pattern to Authentication Protocols

Single Sign-On Internal (SSOi)

As depicted in Figure 3, below, SSOi is the default authentication protocol for all applications rated LOA 1-3. SSOi fully leverages the envisioned ESS for user authentication. Additionally the token technology used by SSOi is capable of fully support the envisioned SOA environment that VA is implementing under the VistA modernization program. Finally, SSOi can fully support the implementation of future enterprise role-, attribute-, and risk-based authorization controls that will further secure the VA environment.

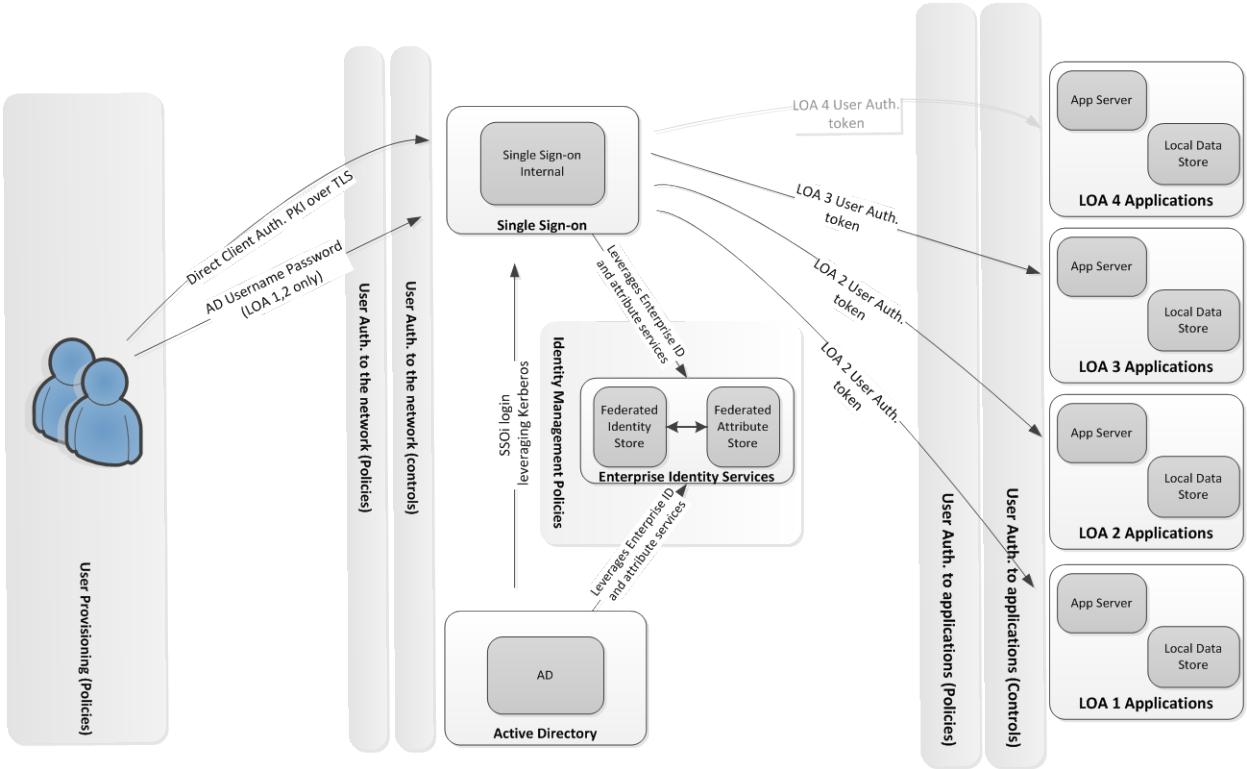

Figure 3 - Single Sign-On Internal

All applications are required by existing VA policy to assess the feasibility of implementing SSOi to support internal user authentication

SSOi directly supports VA's move to enterprise authentication, identity and attribute management services. In addition, IAM provides a range of provisioning and authorization services that can be leveraged for use by application owners. The token based design of the SSOi protocol also directly supports OIT's move to SOA by providing a suite of services and capabilities that will allow SOA to function within the enterprise.

All applications are required by default to implement SSOi for authentication services

The IAM team can provide application developers with integration patterns to help them understand how SSOi and IAM enterprise services can be implemented to ensure their applications' compliance with the design pattern. Only those applications that meet exception criteria are required to implement other authentication protocols.

SSOi Exception Criteria

- *LOA 4 applications are required to use Direct PKI over TLS*

- *LOA 3 or lower applications that, given special consideration by the application owner and the IAM team, feel that a higher LOA authentication protocol is needed, should implement Direct PKI over TLS*
- *LOA 2 or lower rated application that is Microsoft productivity software (e.g., MS Office or MS Email). Special consideration should be given to SharePoint. Some SharePoint sites may contain information that may require a more secure, LOA 3 or LOA 4, authentication protocol.*
- *LOA 2 or lower rated applications that natively support Kerberos and cannot support token based authentication (only applies to legacy applications)*
- *LOA 2 or lower rated MS application that is cost prohibitive to integrate with SSOi*
- *Legacy application which uses Kerberos, does not meet any other exception criteria, and is being replaced with a SSOi or Direct PKI over TLS compliant system currently under design or development*
- *Application has been reviewed by ASD and IAM and it has been determined it will not be integrated with SSOi*

SSOi and LOA 4

In order for SSOi to be used to authenticate users at LOA 4 they must implement 'holder-of-key-assertions'. The Holder-of Key assertion allows client public key and authorization information to be passed via a signed SAML token with integrity and confidentiality protection using mutual certificates. The current VA SSOi capability has not yet implemented holder of key assertions at LOA 4 and is therefore not approved for use at LOA 4 until it is demonstrated that the technology can sufficiently meet NIST 800-63 requirements at this LOA.

Direct Client Authentication using PKI over TLS

As depicted in Figure 4, below, direct client authentication to applications is the most secure method of conducting authentication. When a user is directly authenticated to an application using a strong authentication protocol such as direct client authenticated PKI over TLS most of the techniques used to eavesdrop, hijack, impersonate or redirect authentication are presented. All applications rated at LOA 4 are required to use direct client authenticated PKI. Other applications, considered on a case by case basis, that want to implement strong authentication can also implemented direct client authenticated PKI upon evaluation with the IAM and ASD teams.

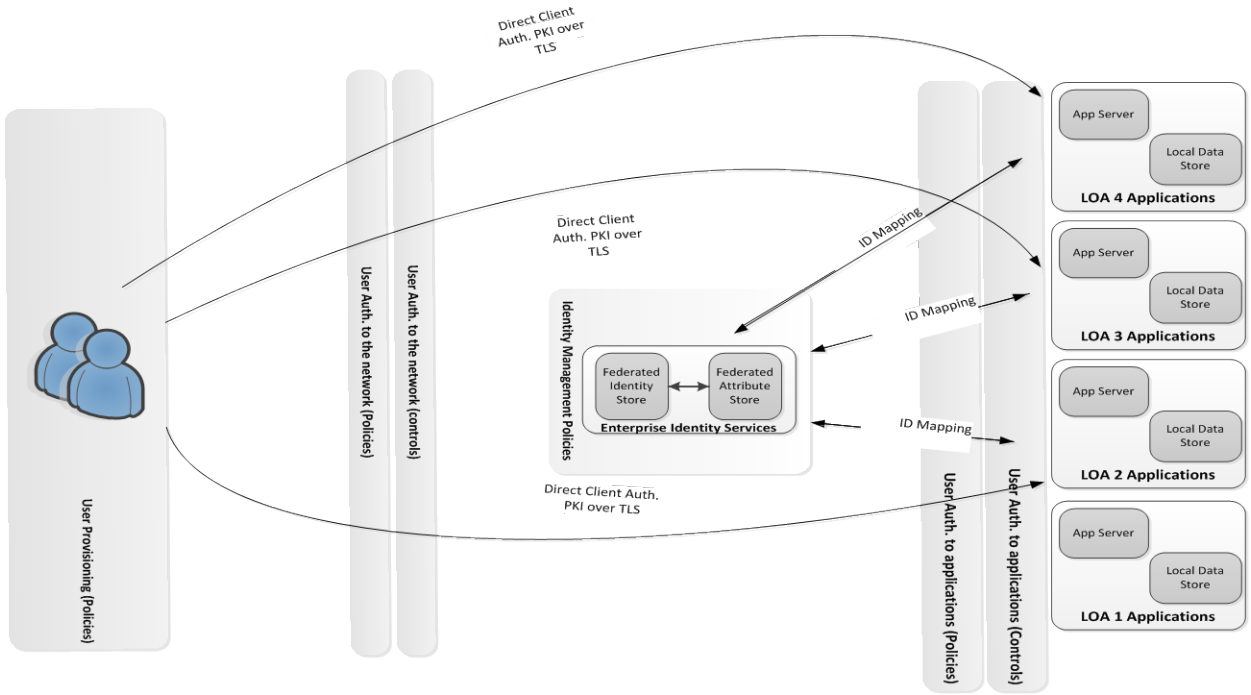

Figure 4 - Direct Client Authentication Using PKI over TLS

The implementation of Direct PKI over TLS at the application layer requires the application to facilitate the process of validating the presented certificates. Additionally, these applications must also rely on enterprise IAM services to provide identity and attribute management to the application for authorization purposes. Because the PKI authentication is only capable of presenting authentication credentials, applications will be required to make additional data calls to IAM services such as MVI to map user identities and to obtain attributes for authorization decisions.

The implementation of direct PKI over TLS is more complex and difficult to manage at the enterprise level than SSOi. Additionally, direct PKI presents some challenges in usability, in that end users, depending on the architecture, may be required to re-authenticate to each new application. Re-authentication would require end users to re-enter their personal identity number (PIN) each time a new application is accessed. Careful management and implementation, where appropriate, will help VA implement this strong authentication protocol where necessary.

Any VA systems rated at LOA 4 shall implement direct PKI over TLS to ensure users are properly authenticated directly to the application.

Application of direct PKI over TLS will be considered on a case-by-case basis and implemented where necessary to protect VA's most sensitive information.

Kerberos, NTLMv2, and Active Directory

A review of the current VA Kerberos, NTLMv2, and active directory infrastructure and management practices is needed to identify necessary changes in technology or policy that must be implemented to align with assurance standards. It is understood that VA's "as-is" implementation and management of AD is only rated as an LOA 2 authentication protocol and will not allow for the use of Kerberos to satisfy requirements at LOA 3 or higher.

Upgrades that are available as parts of Microsoft Windows Server 2008r2 significantly improve the Kerberos by allowing claims based authentication and leverage the use of SAML tokens that allow the exchange of user attributes within the authentication process. Absent these upgrades, distinguishing between Kerberos tickets generated for an LOA 2 or LOA 4 user's request to access an application requires burdensome custom alterations to the Kerberos tickets and changes at the application level. These issues are compounded with VA's current policy of continuing to allow AD authentication with LOA 2 credentials (username/password) in addition to the more secure LOA 4 PIV card authentication.

As depicted in Figure 5, below, because of the issues surrounding current VA policies and the existing implementation of AD, it is recommend to limit Kerberos and NTLMv2 based authentication to LOA 1 and 2 applications, until such a time that necessary changes can be implemented to allow for secure access to LOA 3 applications.

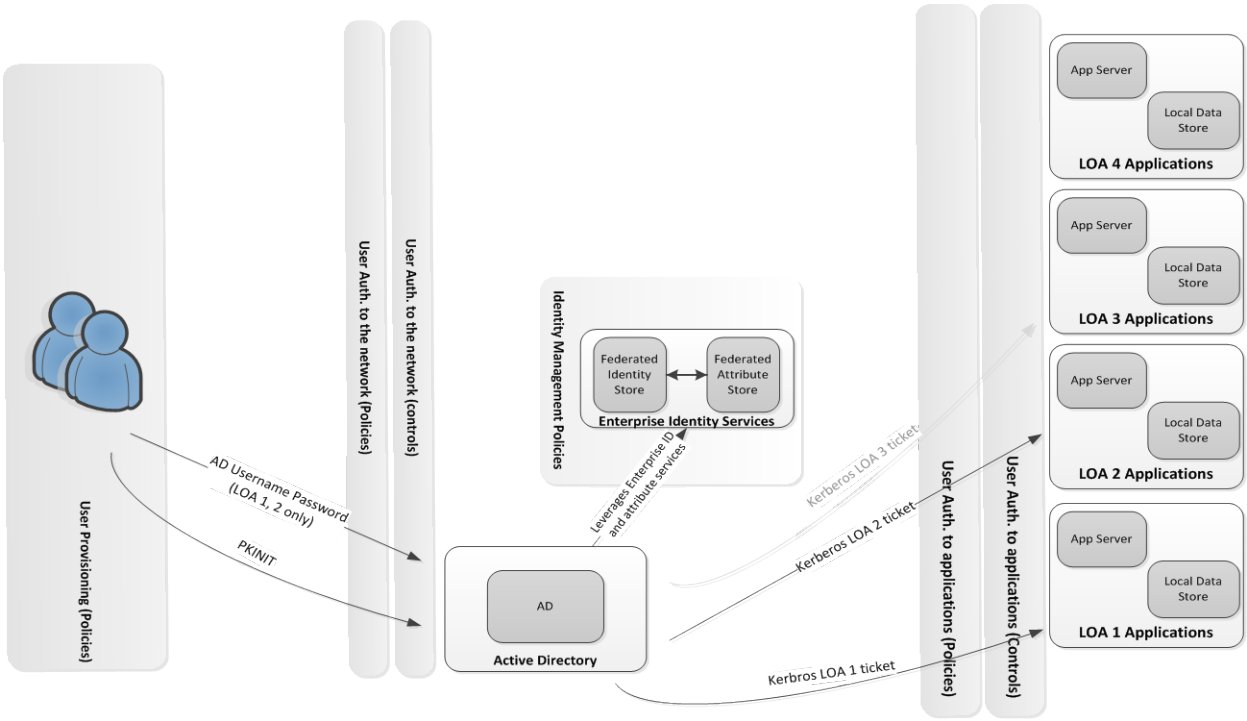

Figure 5 - Kerberos Authentication

Due to the integral nature of AD within VA authentication systems, the review of the current protocol and implementation of the following requirements is considered a high priority.

Requirements that must be met and verified to bring these systems into compliance include:

- ***Kerberos tickets are not acceptable for use as assertions at LOA 4***

- ***Kerberos tickets are acceptable for use as assertions at LOA 3 if:***
  - ***All verifiers (Kerberos Authentication Servers and Ticket Granting Servers) are under the control of a single management authority that ensure the correct operation of the Kerberos protocol***
  - ***The subscriber authenticates to the verifier using a Level 3 or higher token (PIV card)***
  - ***All LOA 3 requirements related to non-repudiation are satisfied***

Kerberos Exception Criteria:

Kerberos can continue to be used for:

- Legacy applications that cannot support token based authentication
- Integrated MS products that do not require higher than LOA 2 (e.g., MS productivity software)
- Legacy applications that are currently being or will soon be replaced with SSOi or direct PKI over TLS compatible designs
- Other applications that are determined on a case by case basis by the ASD and IAM teams

NTLMv2

NTLMv2 is a Microsoft authentication protocol introduced in Windows NT 4.0 and intended to harden the original NTLM standard. Both NTLM and NTLMv2 have published security compromises that make them susceptible to credentials forwarding attacks, commonly referred to as 'Pass the Hash'. From Microsoft: "Implementers should be aware that NTLM does not support any recent cryptographic methods, such as AES or SHA-256. It uses cyclic redundancy check (CRC) or message digest algorithms (RFC1321) for integrity, and it uses RC4 for encryption. Deriving a key from a password as is specified in RFC1320 and FIPSS46-2. Therefore, applications are generally advised not to use NTLM."[4]

Because a wide variety of applications still leverage NTLMv2 for user authentication the cost for completely eliminating it from use on the network is seen as prohibitive. However, no new applications built or acquired by VA should use NTLMv2 for user authentication. Legacy applications that rely on NTLMv2 should be seen as having a high potential for compromise and should have a high priority for migration to a new authentication protocol if the application rates above LOA2 and contains sensitive information.

[4] "Security Considerations for Implementers", *NT LAN Manager (NTLM) Authentication Protocol Specification* (Microsoft)

3.3 VA Authentication Protocol Teams

For more information detailing how to implement the required authentication protocols in adherence with applicable standards and policies, application developers should contact the team(s) responsible for their implementation (See Table 4, below).

Table 4 – Responsible Integration Teams for Internal User Authentication Protocols

User Authentication Protocol	Responsible Integration Team
Single Sign-On	Identity & Access Management
Direct Client Authentication using PKI over TLS	PIV Only Authentication Team, Service Delivery & Engineering
Kerberos	Service Delivery & Engineering

Appendix A. ACRONYMS

Acronym	Description
AD	Active Directory
CSP	Credential Service Provider
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HSPD-12	Homeland Security Presidential Directive 12
LOA	Level of Assurance
MitM Attack	Man-in-the-Middle Attack
MVI	Master Veteran Index
NIST	National Institute of Standards and Technology
NSS	Network Security Services
NTLM	NT LAN Manager
NTLMv2	NT LAN Manager version 2
OIT	Office of Information and Technology
OIS	Office of Information Security
OMB	Office of Management and Budget
RA	Registration Authority
RP	Relying Party
PE	Person Entity
PKI	Public Key Infrastructure
PIV Card	Personal Identity Verification Card
RBAC	Role Based Access Control
REST	Representational State Transfer

Acronym	Description
SAML	Secure Assertion Markup Language
SSL	Secure Socket Layer
SSOe	Single Sign-On External
SSOi	Single Sign-On Internal
TLS	Transport Layer Security
VistA	Veterans Health Information Systems and Technology Architecture

Appendix B. USE CASES

Click Here	Click Here	Click Here
Direct Client Auth via PKI over TLS Use Cas	Kerberos Use Case Document 20140401.	IAM SSOi Use Case Document 20140401.

<u>Use Case 1:</u> Internal VA User Direct Client Authentication to Applications via PKI over TLS (LOA 1-4)

Purpose
This use case is meant to provide the high-level process steps for granting an internal VA user logical access to applications within the VA network through direct client authentication via PKI over TLS.

Scope
This use case applies to internal VA users attempting to gain logical access to VA applications using government furnished equipment (GFE) through PIV card-enabled direct client authentication via PKI over TLS. This method of authentication provides high level security. Network access to applications by users in any way other than the use of a VA issued PIV card, VA issued GFE, and direct connection to the VA network are out of scope for this use case.

<u>Use Case 2:</u> Internal VA User Authentication to Applications using Microsoft Kerberos Tickets (LOA 1-2)

Purpose
This use case provides a high level overview of the Microsoft Kerberos authentication protocol and how it could be used to support internal VA user authentication to LOA 1 and LOA 2 VA applications if the prerequisite conditions (ref. page 11, Section 3) were met. This document is not intended to provide detailed technical information, but policy and strategic guidance.

Scope
This use case applies to the use of Kerberos to support LOA 1 and LOA 2 authentication. Kerberos is currently only approved as a method to accomplish authentication at LOA 1 and LOA 2.

<u>Use Case 3:</u> Internal VA user authentication to VA applications using Identity and Access Management Single Sign-on Internal (LOA 1-3)

Purpose
This use case provides a high level overview of the IAM, SSOi authentication protocol and how it can be used to support internal VA user authentication to Level of Assurance (LOA) 1 through LOA 3 applications. This document is not intended to provide detailed technical information, but policy and strategic guidance.

Scope
This use case applies to the use of the IAM SSOi tool to support LOA 1 – LOA 3. SSOi is not the only approved method to accomplish authentication at these LOAs. SSOi is one option that is available to project managers to comply with VA standards for authentication.

Appendix C. REFERENCES/APPLICABLE STANDARDS

This Design Pattern includes information and references that were gathered and reviewed from:

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	VA	VA 6500 Handbook	• Directive information security program. • Defining overall security framework for VA.
2	VA	VA 6300 Directive	• Directive records and information management. • Defines information management framework for VA access services.
3	NIST	SP 800-53-4	• Special Publication — recommended security controls for federal information systems and organizations. • Defines the required security controls for IT systems under the Federal Information Security Management Act .
4	NIST	SP 800-63-2	• Special Publication — electronic authentication guideline. • Defines levels of assurance in user identities presented to IT systems over open networks. • Defines the data and procedural requirements for VA access services.
5	NIST	FIPS-201-2	• Federal Information Processing Standards Publication — PIV of federal employees and contractors. • Provides identity proofing, credentialing and chain of trust requirements and processes. • Defines the method for secure administrative interaction and control.
6	NIST	FIPS-140-2	• Federal Information Processing Standards Publication — security requirements for cryptographic modules. • Defines the cryptographic standards and requirements.
7	NIST	SP 800-122	• Guide to protecting the confidentiality of personally identifiable information (PII). • Provides technical procedures for protecting PII in information systems. • Defines the information that can be used to distinguish or trace an individual's identity.
8	OMB	M-04-04	• Memorandum to the heads of all departments and agencies – e-authentication guidance for federal agencies. • Defines the e-authentication requirement.
9	GSA	FICAM	• Federal Identity, Credentialing and Access Management roadmap and implementation guidance. • Provides the common segment architecture and implementation guidance for federal ICAM programs.
10	White House	NSTIC	• National Strategy for Trusted Identities in Cyberspace – Provides guidance for identity trust in cyberspace.
11	US Congress	FISMA	• FISMA of 2002, Public Law 107-347
12	US Congress	E-Government Act of 2002	• Federal management and promotion of electronic government services. • Defines the requirements for electronic services.
13	US Congress	The Privacy Act of 1974	• § 552a. Records maintained on individuals. • Defines VA access services privacy assessment and control requirements.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
14	National Archives and Records Administration (NARA)	Federal Records Act	• Establishes the framework for records management programs in federal agencies.
15	VA	VA D 0735	• Homeland Security Presidential Directive 12 (HSPD-12) Program. • Defines department-wide policy, roles, and responsibilities for the creation and maintenance of systems and processes to implement VA's HSPD-12 Program necessary to implement HSPD-12 program.
16	OMB	M-05-24	• Implementation of HSPD 12 – policy for a common identification.

Appendix D. LEVEL OF ASSURANCE (LOA) REQUIREMENTS

General Requirements LOA 4-2
Registration • Records of registration shall be maintained by either the Registration Authority (RA) or by the CSP. • Either the RA or the CSP shall maintain a record of each individual whose identity has been verified and the steps taken to verify their identity. • The CSP shall have the capability to provide ID proofing records to Relying Parties (RP). • If the RA and the CSP are remotely located and communicate over a network the registration transaction between RA and CSP shall occur over a mutually authentication protected session. • This transaction may consist of time-stamped or sequenced messages signed by their sources and encrypted for their recipient; in both cases approved cryptography is required. • The CSP shall be able to uniquely identify each subscriber and the associated tokens and credentials issued to that subscriber. • The CSP shall be capable of conveying unique IDs and associated tokens to verifiers. • At all levels, PII collected as part of the registration process shall be protected. • The applicant must supply full legal name, address of record, date of birth, and may be subject to policies established by the RA or CSP, and also supply other PII. **Tokens** • Two factors for authentication are sufficient to achieve the highest LOA. • Memorized secret tokens are only appropriate for LOA 2 and 1. • Pre-registered knowledge tokens are only appropriate for LOA 2 and 1. • Look-up secret tokens are only appropriate for LOA 2 and 1. • Out of band tokens are only appropriate for LOA 2 and 1. • Single-factor one-time password devices are only appropriate for LOA 2 and 1. • Single-factor cryptographic devices are only appropriate for LOA 2 and 1. • Multi-factor software cryptographic tokens are appropriate for LOA 3, 2, and 1. • Multi-factor one time password hardware tokens are appropriate for all LOAs. • Multi-factor hardware cryptographic tokens are appropriate for all LOAs. • Combinations of tokens can be used to achieve higher LOAs (e.g. two Level 2 tokens can be used to achieve LOA 3); details provided in NIST 800-63.
LOA 4
General LOA 4 Requirements • Level 4 requires strong cryptographic authentication of all parties, and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. • The token secret shall be protected from compromise through the malicious code threat. • Long-term shared authentication secrets, if used, shall never be revealed to any party except the claimant and CSP; however session (temporary) shared secrets may be provided to verifiers or RPs by the CSP. Strong, approved cryptographic techniques shall be used for all operations including the transfer of session data. • All sensitive data transfers shall be cryptographically authenticated using keys that are derived from the authentication process in such a way that MitM attacks are strongly resisted. • Level 4 assurance may be satisfied by client authenticated TLS (implemented in all modern browsers), with claimants who have public key MF hardware cryptographic tokens. Other protocols with similar properties can also be used. • At LOA 4, only verified names may be specified in credentials and assertions. • The token (or combination of tokens) used shall have assurance level of 4 or higher. • The binding between the identity proofing and the token(s), if proofing is done separately from token issuance, shall be established at level 4.

- The authentication protocols used shall have Level 4 assurance level or higher.
- The token and credential management process shall use a Level 4 assurance level or higher.
- Authentication assertions (if used) shall have a Level 4 assurance or higher.

Registration Requirements Specific to LOA 4

- At LOA 4 the name associated with the subscriber shall be verified.
- AT LOA 4 only in person registration is permitted.
- For physical registration:
    - The applicant shall identify himself in each new transaction through the use of a biometric that was recorded during a prior encounter.
    - If the CSP issues permanent secrets, they must be loaded locally onto a physical device that is issued in person.

Token Requirements Specific to LOA 4

- Cryptographic module shall be FIPS 140-2 validated, Level 2 or higher, with physical security at FIPS 140-2 Level 3 or higher.
- For one time password hardware tokens:
    - The one-time password shall be generated by using an approved block cipher or hash function to combine a symmetric key stored on a personal hardware device with a nonce to generate a one-time password.
        - The nonce may be a date and time, a counter generated on the device.
    - Each authentication shall require entry of a password or other activation data through an integrated input mechanism.
- For hardware cryptographic tokens:
    - shall require entry of a password, PIN, or biometric to active the authentication key.
    - shall not allow export of authentication keys.

Token and Credential Management Requirements Specific to LOA 3

- No additional stipulations to LOA 3 credential storage requirements.
- No additional stipulations to LOA 3 token and credential verification service requirements.
- Sensitive data transfers shall be cryptographically authenticated using keys bound to the authentication process.
- All temporary or short-term keys derived during the original authentication operation shall expire and re-authentication shall be required after not more than 24 hours from the initial authentication.
- CSP shall have a procedure to revoke credentials within 24 hours.
- Verifiers or RPs shall ensure that the credentials they rely upon are either freshly issued (within 24 hours) or are still valid.
- All stipulations from LOA 2 and LOA 3 apply to records retention at LOA 4.
- The minimum record retention period for LOA 4 credential data is 10 years and six months beyond the expiration of revocation of the credential.
- The CSP must employ appropriately tailored security controls from the moderate baseline of security controls defined in NIST 800-53 and must ensure that the minimum assurance requirements associated with the moderate baseline are satisfied.

Authentication Process requirements Specific to LOA 4

- LOA 4 must maintain threat resistance against: online guessing, replay, session hijacking, eavesdropping, phishing/pharming (verifier impersonation), MitM-strong, and denial of service/flooding.
- LOA 4 requires strong cryptographic authentication of all parties, and all sensitive data transfers between the parties.
- Either public key or symmetric key technology may be used.
- The token secret shall be protected from compromise through the malicious code threat.
- Long-term shared authentication code secrets, if used, shall never be revealed to any party except the claimant and the CSP.
- Session (temporary) shared secrets may be provided to the verifiers or RPs by the CSP.
- Strong, approved cryptographic techniques shall be used for all operations including the transfer of session data.
- All session data transfers shall be cryptographically authenticated using keys that are derived from the authentication process in a way that strongly resists MitM attacks.
- LOA 4 may be satisfied by client authenticated TLS with claimants who have public key MF hardware cryptographic

tokens. Other protocols with similar properties can also be used.

- For multi-token schemes, the token used to provide strong resistance to MitM attacks is not required to be a hardware token.

Assertion Requirements Specific to LOA 4

- Bearer assertions (including cookies) shall not be used to establish the identity of the claimant to the RP.
- Assertions made by the verifier may be used to bind keys or other attributes to an identity.
- Holder-of-key assertions may be used, if:
  - the claimant authenticates to the verifier using a LOA 4 token in a LOA 4 authentication protocol;
  - the verifier generates a holder-of-key assertion that references a key that is part of the LOA 4 chain of trust; and,
  - the RP verifies that the subscriber possess the key that is references in the holder-of-key assertion using a LOA 4 protocol.
- The RP shall maintain records of the assertions it receives, allowing the RP to detect any attempt by the verifier to impersonate the subscriber using fraudulent assertions.
- Kerberos tickets are acceptable for use as assertions at LOA 4, if:
  - all verifiers (Kerberos authentication servers and ticket granting servers) are under the control of a single management authority that ensure the correct operation of the Kerberos protocol;
  - the subscriber authenticates to the verifier using a Level 4 token;
  - all LOA 4 requirements related to non-repudiation are satisfied.
- All LOA 1-3 requirements regarding protection of assertion data remain in force at LOA 4.

LOA 3

General LOA 3 Requirements

- LOA 3 provides multi-factor remote network authentication. At least two authentication factors are required. At this level, proofing procedures require verification of identifying materials and information. LOA 3 authentication is based on proof of possession of the allowed types of tokens through a cryptographic protocol.
- Multi-factor software cryptographic tokens are allowed at LOA 3.
- LOA 3 permits any of the token methods of LOA 4.
- LOA 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token against compromise by threats specified for LOA in NIST 800-63.
- At LOA 3, only verified names may be specified in credentials and assertions.
- The registration and identity proofing process shall, at a minimum, use Level 3 processes.
- The token (or combination of tokens) used shall have an assurance Level of 3 or higher.
- The binding between the identity proofing and the token(s), if proofing is done separately from token issuance, shall be established at Level 3.
- The authentication protocols used shall have a Level 3 assurance level or higher.
- The token and credential management process shall use a Level 3 assurance level or higher.
- Authentication assertions (if used) shall have a Level 3 assurance or higher.

Registration Requirements Specific to LOA 3

- The names associated with the subscriber shall be verified.
- Both in person and remote registration is permitted.
- Confirmation of a financial or utility account number is required.
- For remote registration:
  - The applicant shall identify himself in each new electronic transaction by presenting a temporary secret established during a prior transaction or encounter, or sent to the applicant's phone number, email, or physical address of record.
- For physical registration:
  - The applicant shall identify himself either by using the temporary secret described above or through use of a previously recorded biometric. Temporary secrets shall not be reused.
  - If the CSP issues permanent secrets, the must be loaded locally onto a physical device that is issued in person.

Token Requirements Specific to LOA 3

- Shall accept LOA 4 tokens.
- For multi-factor software cryptographic tokens:
  - The cryptographic module shall be validated at FIPS 140-2 Level 1 or higher.
  - Each authentication shall require the entry of the password or other activation data and the unencrypted copy of the authentication key shall be erased after each authentication.

Token and Credential Management Requirements Specific to LOA 3

- Files of long-term shared secrets used by CSPs or Verifiers at LOA 3 shall be protected by access controls that limit access to administrators and only those applications that require access.
- Shared secret files shall be encrypted so that:
  - the encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 Level 3 or 4 cryptographic module and decrypted only as immediately required for an authentication operation.
  - shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and is not exported in plaintext from the module.
- CSPs shall provide a secure mechanism to allow verifiers or RPs to ensure that the credentials are valid.
  - Mechanisms may include on-line validation servers or the involvement of CSP servers that have access to status records in authentication transactions
- Temporary session authentication keys may be generated from long-term shared secret keys by CSPs and distributed to third party verifiers as part of the verification services offered by the CSP, but long-term secrets shall not be shared with any third parties, including third party verifiers.
- Token and credential verification services categorized as FIPS 199 “moderate” or “high” for availability shall be protected in accordance with the contingency planning controls specified in NIST SP 800-53.
- Renewal and re-issuance shall only occur prior to expiration of the current credential.
- Claimants shall authentication to the CSP using the existing token and credential in order to renew or re-issue the credential. All interactions to do so shall occur over a protected session such as SSL/TLS.
- CSPs shall have a procedure to revoke credentials and tokens within 24 hours.
- Verifiers shall ensure that the tokens they rely upon are either freshly issued (within 24 hours) or still valid.
- All stipulations from LOA 2 regarding records retention apply.
- The CSP must employ appropriately tailored security controls from the moderate baseline of security controls defined in NIST 800-53 and must ensure that the minimum assurance requirements associated with the moderate baseline are satisfied.

Authentication Process Requirements Specific to LOA 3

- LOA 3 must maintain threat resistance against: online guessing, replay, session hijacking, eavesdropping, phishing/pharming (verifier impersonation), MitM–weak, and denial of service/flooding.
- At LOA 3 at least two authentication factors are required.
- LOA permits any of the token methods of LOA 4.
- Strong cryptographic mechanisms shall be used to protect token secret(s) and authenticator(s).
- Long-term shared authentication secrets shall never be revealed to any party except the claimant and the CSP.
- Session (temporary) shared secrets may be provided to verifiers by the CSP, possibly via the claimant.
- Approved cryptographic techniques shall be used for all operations including the transfer of session data
- LOA 3 may be satisfied by client authentications TLS, with claimants who have public key certificates. Other protocols with similar properties may also be used.
- LOA 3 may also be met by tunneling the output of a MF OTP token, or the output of SF OTP Token in combination with a Level 2 personal password through a TLS session.

Assertion Requirements Specific to LOA 3

- Shall meet all LOA 2 requirements.
- Assertions shall be protected against repudiation by the verifier.
- All assertions shall be signed.

- Shall specify verified names and not pseudonyms.
- Kerberos tickets are acceptable for use as assertions at LOA 3.
    - Can only be used at LOA 3 if all verifiers (Kerberos authentication servers and ticket granting servers) are under the control of a single management authority that ensure the correct operation of the Kerberos protocol.
    - The subscriber authenticates to the verifier using a Level 3 token.
    - All LOA 3 requirements related to non-repudiation are satisfied.
- All single-domain assertions (web cookies) if used shall expire after 30 minutes if not used.
- Cross-domain assertions shall expire after five minutes if not used.
- Verifier may re-authenticate the subscriber prior to delivering assertions to the new RPs using a combination of long and short term assertions if:
    - the subscriber has successfully authentication to the verifier within the last 12 hours;
    - the subscriber can demonstrate that they were the party that authenticated to the verifier;
    - the verifier can determine if the subscriber has been in active communication with an RP since the last assertion was delivered by the Verifier, meaning that the subscriber has been actively using the services of the RP and has not been idle for more than 30 minutes.

LOA 2

General Requirements

- Shall permit any of the token methods of LOAs 3 and 4.
- Identification requirements requiring presentation of identifying materials or information are required for registration.
- Single factor authentication is allowed, including:
    - memorized secret tokens, pre-registered knowledge tokens, look-up secret tokens, out of band tokens, and single factor one-time password devices.
- LOA 2 authentication requires that the claimant prove through a secure authentication protocol that he control an approved token.
- At LOA 2, online guessing, replay, session hijacking, and eavesdropping attacks shall be resisted, protocols are also required to at least weakly resist MitM attacks.
- At LOA 2, long-term shared authentication secrets, if used, are never revealed to any party, except verifiers operated by the CSP.
- Session (temporary) secrets may be provided to independent verifiers by the CSP.
- At LOA 2 all LOA 1 assertion requirements shall be met, in addition LOA 2 assertions shall be resistant to disclosure, redirection, capture and substitution attacks.
- Approved cryptographic techniques are required for all LOA 2 assertion protocols.
- The registration and identity proofing process shall, at a minimum, use Level 2 Processes or higher.
- The token (or combination of tokens) used shall have assurance Level of 2 or higher.
- The binding between the identity proofing and the token(s), if proofing is done separately from token issuance, shall be established at Level 2.
- The authentication protocols used shall have Level 2 assurance level or higher.
- The token and credential management process shall use a Level 2 assurance level or higher.
- Authentication assertions (if used) shall have a Level 2 assurance or higher.

Registration Requirements specific to LOA 2

- Records of registration shall be maintained by either the RA or by the CSP.
- Either the RA or the CSP shall maintain a record of each individual whose identity has been verified and the steps taken to verify his identity.
- The CSP shall have the capability to provide ID proofing records to RPs.
- If the RA and the CSP are remotely located and communicate over a network, the registration transaction between RA and CSP shall occur over a mutually authentication protected session.
- This transaction may consist of time-stamped or sequenced messages signed by their sources and encrypted for their recipient. In both cases, approved cryptography is required.
- The CSP shall be able to uniquely identify each subscriber and the associated tokens and credentials issued to that

subscriber.

- The CSP shall be capable of conveying unique IDs and associated tokens to verifiers.
- At all levels, PII collected as part of the registration process shall be protected.
- The applicant must supply full legal name, address of record, date of birth, and may subject to policies established by the RA or CSP, and also supply other PII.
- At LOA 2, the identifier associated with the subscriber may be pseudonymous, but the RA and CSP shall retain the actual identity of the subscriber.
- Pseudonymous LOA 2 credentials shall be distinguishable from LOA 2 credentials that contain verified names.
- For electronic transactions:
    - The applicant shall identify himself in any new transaction beyond the first transaction or encounter by presenting a temporary secret which was established during a prior transaction or encounter or sent to the applicant's phone number, email address, or physical address of record.
- For in person transactions:
    - The applicant shall identify himself in person by either using a secret obtained in the same way as for electronic transactions or by biometric verification.

Token Requirements Specific to LOA 2

- For memorized secret tokens:
    - Memorized secret shall be a randomly generated PIN consisting of 6 or more digits, a user generated string consisting of 8 or more characters chosen from an alphabet of 90 or more characters, or a secret with equivalent entropy.
    - CSP shall implement dictionary or composition rules to constrain user-generated secrets.
    - Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts to 100 or fewer in 30 days.
- For look-up secret tokens:
    - Token authentication has 64 bits of entropy.
    - Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts to 100 or fewer in 30 days.
- For out of band tokens:
    - Token is uniquely addressable and support communication over a channel that is separate from the primary channel for e-authentication.
    - Verifier generated secret shall have at least 64 bits of entropy.
    - Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts to 100 or fewer in 30 days.
- For single-factor one-time password device:
    - Shall use approved block cipher or hash function to combine a symmetric key stored on device with a nonce to generate a one-time password.
    - Password shall have a limited lifetime, less than 30 minutes.
    - Cryptographic module performing the verifier function shall be validated at FIPS 140-2 Level 1 or higher.
- For single-factor cryptographic device:
    - Cryptographic module shall be validated at FIPS 140-2 Level 1 or higher.
    - Verifier generated token input has at least 64 bits of entropy.

Token and Credential Management Requirements Specific to LOA 2

- Files of shared secrets used by the CSP at LOA 2 shall be protected by access controls that limit access to administrators and only to those applications that require access.
- Files of shared secrets shall not contain plaintext passwords or secrets.
- Shared secrets must be protected:
    - Passwords may be concatenated to a variable salt and then hashed with an approved algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are not useful to attack other similar password files. Hashed passwords shall be stored in the password file. The variable salt may be

composed using a global salt and the username or some other techniques to ensure the uniqueness of the salt within the group of passwords.
    - Or, shared secrets may be encrypted and stored using approved encryption algorithms and modes, and the needed secret decrypted only when immediately required for authentication.
    - Any method used to protect secrets at LOA 3 and 4 may be used at LOA 2.
- Long-term shared authentication secrets, if used, shall never be revealed to any other party except verifiers operated by the CSP.
- Session (temporary) shared secrets may be provided by the CSP to independent verifiers.
- Cryptographic protections are required for all messages between the CSP and verifier which contain private credentials or assert the validity of weakly bound or potentially revoked credentials.
- Private credentials shall only be sent through a protected session to an authenticated party.
- CSP shall establish suitable policies for renewal and re-issuance of tokens and credentials.
- Proof-of-possession of the unexpired current token shall be demonstrated by the claimant prior to the CSP allowing renewal and re-issuance.
- Passwords shall not be renewed; they shall be re-issued.
- After expiration of current token and any grace period, renewal and re-issuance shall not be allowed.
- Upon re-issuance, token secrets shall not be set to a default or reused in any manner.
- All interactions shall occur over a protected session such as SSL/TLS.
- CSPs shall revoke or destroy credentials and tokens within 72 hours after being notified that a credential is no longer valid or a token is compromised.
- If the issued credentials expire automatically after 72 hours then the CSP is not required to provide an explicit mechanism to revoke the credentials.
- CSPs that register passwords shall ensure that the revocation or de-registration of the password can be accomplished in no more than 72 hours.
- A record of the registration, history, and status or each token and credential (including revocation) shall be maintained by the CSP or its representative.
- Record retention period shall be seven years and six months beyond the expiration or revocation (whichever is later) of the credential.
- CSPs operated by or on behalf of an executive branch agency shall follow either the general records schedule established by the national archives or an agency-specific schedule as applicable.
- CSPs must employ appropriately tailored security controls from the low baseline of security controls defined in NIST 800-53 and must ensure that the minimum assurance requirements associated with the low baseline are satisfied.

Authentication Requirements Specific to LOA 2

- Shall permit the use of token methods used at LOAs 3 and 4.
- LOA 2 authentication requires the Claimant to prove through a secure authentication protocol that they control the token
- Session hijacking, replay, and online guessing attacks shall be resisted
- Shall be at least weakly Man-in-the-Middle resistant
- Session data transmitted between the Claimant and the RP following a LOA 2 authentication shall be protected as described in the NIST FISMA guidance
    - All session data exchanged between information systems that are categorized as FIPS 199 “moderate” or “high” for confidentiality and integrity, shall be protected in accordance with NIST 800-53 control SC-8

Assertion Requirements Specific to LOA 2

- If the subscriber name is a pseudonym, this information must be conveyed in the assertion.
- LOA 2 assertions shall be protected against manufacture/modification, capture, redirect and reuse.
- Assertion references shall be protected against manufacture, capture, and reuse.
- Each assertion shall be targeted for a single RP.
- RP shall validate that it is the intended recipient of the incoming assertion.
- All LOA 1 assertion requirements apply.
- Assertions, assertion references and any session cookies used by the verifier or RP for authentication purposes shall be

transmitted to the subscriber through a protected session linked to the primary authentication process in such a way that session hijacking attacks are resisted.

- Assertions, assertion references and session cookies shall not be subsequently transmitted over an unprotected session or to an unauthenticated party while they remain valid.
- Any session cookies used for authentication purposes shall be flagged as secure.
- Redirects used to forward secondary authenticators from the subscriber to the RP shall specify a secure protocol such as HTTPS.
- Assertions sent from the Verifier to the RP, either directly or through the subscriber's device, shall either be sent via a mutually authenticated protected session between the verifier and RP or equivalently shall be signed by the verifier and encrypted for the RP.
- All assertion protocols used at LOA 2 require use of approved cryptographic techniques.
- Kerberos keys generated from user generated passwords are not approved above LOA 2.

LOA 1

General Requirements

- Shall permit any of the token methods of LOAs 2, 3, and 4.
- LOA 1 authentication requires that the claimant prove through a secure authentication protocol that he possesses and controls an approved token.
- Plaintext passwords or secrets shall not be transmitted across a network.
- Simple password challenge-response protocols are allowed.
- At LOA 1, long-term share authentication secrets may be revealed to verifiers.
- At LOA 1, assertions and assertion references shall be protected from manufacture/modification and reuse attacks.
- The registration and identity proofing process shall, at a minimum, use Level 1 processes or higher.
- The token (or combination of tokens) used shall have assurance level of 1 or higher
- The binding between the identity proofing and the token(s), if proofing is done separately from token issuance, shall be established at Level 1.
- The authentication protocols used shall have level 1 assurance level or higher.
- The token and credential management process shall use a Level 1 assurance or higher.
- Authentication assertions (if used) shall have a Level 1 assurance or higher.
- At LOA 1, the name associated with the subscriber is provided by the applicant and accepted without verification.

Registration Requirements Specific to LOA 1

- Shall recognize the use of pseudonymous credentials

Token Requirements Specific to LOA 1

- For memorized secret tokens
    - Shall contain 6 or more characters chosen from an alphabet of 90 or more characters, a randomly generated PIN consisting of 4 or more digits, or a secret with equivalent entropy
    - Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts to 100 or fewer in 30 days
- For Pre-Registered Knowledge Tokens
    - Shall provide at least 14 bits of entropy
    - The entropy in the secret cannot be directly calculated (e.g. user chosen or personal knowledge questions)
    - Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts to 100 or fewer in 30 days
    - Verifier shall verify the answer provided for at least three questions

Token and Credential Management Requirements Specific to LOA 1

- Files of shared secrets used by verifiers at LOA shall be protected by access controls that limit access to administrators and only to those applications that require access.
- Files that contain shared secrets shall not contain plaintext passwords.
- Any method used for long term protection of long-term shared secrets at LOA 2 and above may be used.
- Long term token secrets should not be shared with other parties unless absolutely necessary.

Authentication Requirements Specific to LOA 1

- Shall permit the use of any token methods of LOA 2, 3, and 4.
- LOA 1 authentication requires that the Claimant prove, through a secure authentication protocol, that he or she possess and controls the token
- Plaintext passwords or secrets shall not be transmitted across the network
- At LOA 1 long-term shared authentication secrets may be revealed to Verifiers

Assertion Requirements Specific to LOA 1

- At LOA 1 it must be impractical for an attacker to manufacture an assertion or assertion reference that can be used to impersonate the subscriber.
- In a direct assertion model, the assertion which is used shall be signed by the verifier or integrity protected using a secret key shared by the verifier and RP.
- In an indirect assertion model, the assertion reference shall have a minimum of 64 bits of entropy.
- Bearer assertions shall be specific to a single transaction.
- If assertion references are used, they shall be freshly generated whenever a new assertion is created by the verifier (bearer assertions and assertion references are for one-time use).
- All assertions sent from the verifier to the RP shall either be signed by the verifier or transmitted from an authenticated verifier via a protected session.
- A strong mechanism must be in place to allow the RP to establish a binding between the assertion reference and its corresponding assertion based on integrity protected communications with the authenticated verifier.
- Assertions that are consumed by an RP which is not part of the same internet domain as the verifier shall expire if not used within five minutes.