
Authentication, Authorization, and Audit Design Pattern: External User Authentication

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

Version 1.0

Date Issued: September 08, 2014



THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

APPROVAL COORDINATION

Mr. Tim McGrail
Deputy Director (Acting)
OI&T Architecture, Strategy, and Design (ASD)

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

REVISION HISTORY

Version Number	Date	Organization	Notes
0.1	06/04/14	ASD TS	Initial Draft
0.4	07/03/14	ASD TS	Draft for Review
0.5	07/15/14	ASD TS	Incorporated edits from IAM team
0.7	08/07/14	ASD TS	Incorporated edits from ESS Security, the Office of Cyber Security (OCS), Benefits Gateway Service (BGS), ASD Product Platform Management (PPM), IAM Business Program Management Office (BPMO), and external vendors: Oracle and RSA
1.0	08/17/14	ASD TS	Incorporated comments from the AA&A Public Forum held on August 14, 2014

REVISION HISTORY APPROVALS

Version	Date	Approver	Role
0.1	06/15/14	Dusty Jackson	AA&A Design Pattern Lead
0.5	07/15/14	Dusty Jackson	AA&A Design Pattern Lead
0.7	08/07/14	Dusty Jackson	AA&A Design Pattern Lead
1.0	09/08/14	Dusty Jackson	AA&A Design Pattern Lead

TABLE OF CONTENTS

1 Introduction 6

1.1 Background 6

1.2 Business Need 6

1.3 Scope 7

1.4 Document Development and Maintenance 7

2 Design Pattern Description 8

2.1 External User Identity Authentication 8

2.2 Authentication to VA Resources 8

2.3 Levels of Assurance (LOA) Framework 10

 LOA 2 12

 LOA 3 13

 LOA 4 13

 Other Security Controls 14

2.4 Enterprise Shared Services 14

2.5 Adaptive Authentication Requirements 15

3 Design Pattern Architecture 16

3.1 External User Identity Authentication to VA resources 17

3.2 Application Integration with SSOe 18

3.3 Support for Mobile Authentication 18

3.4 Identity Propagation 18

Appendix A. Acronyms 19

Appendix B. References/Applicable Standards 22

Appendix C. Level of Assurance (LOA) Requirements 24

TABLE OF FIGURES

Figure 1 - Current External User Identity Authentication 17

TABLE OF TABLES

Table 1 - Level of Assurance Overview 11

1 INTRODUCTION

1.1 Background

In order to deliver services and benefits to our nation's Veterans VA's maintains a number of resources that are available to users who are neither employee nor employed as consultants. These external users require access to VA resources for a variety of reasons and can be roughly categorized as belonging to three groups.

1. Other government agencies and their employees
2. External private sector partners including both commercial and non-profit and their employees
3. Citizens including Veterans, dependents, etc.

These external users gain access to VA resources through accessing or logging into a VA application. This design pattern will focus on the 'direct' external user authentication process. This Design Pattern is intended to outline enterprise guidelines for authenticating these external users through the use of a standardized enterprise approach and authentication service that complies with established VA security policies (VA 6500 Information Security Handbook) and NIST e-Authentication Guidelines (800-63-2). This authentication framework is also designed to be supportive of VA's current and future enterprise authorization and audit guidelines.

1.2 Business Need

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

Within VA, VA 6500 is the foundational security document that contains all requirements specific to VA's security and privacy programs. Office of Information Technology employees should view VA 6500 as the primary directive for information security.

For information systems to ensure compliance with the Federal Information Security Management Act (FISMA) of 2002 they must implement a foundational level of security controls outlined in the Federal Information Processing Standard (FIPS) 200 and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. FIPS 200 states that, "Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems."

VA has adopted NIST risk management framework, NIST 800-63-2: Electronic Authentication Guideline standards for rating application Levels of Assurance (LOA) and aligning appropriate authentication protocols to the level of risk posed by those applications.

It should be noted that the NIST 800-63-2 framework 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.

In addition to the use of a common framework VA is moving towards the implementation of enterprise shared security services through the Identity and Access Management (IAM) program. System owners must design applications to leverage these enterprise services where they are available. To perform proper authentication, information system owners, business and IT, must use identity authentication protocols that have been reviewed and approved by VA's Office of Information and Technology. To determine which protocols are required system owners must assess the importance and sensitivity of the information in a system, recognize the threats and vulnerabilities to the system, consider the required 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. Once a system owner has a firm understanding of the risks posed by their system they can use ASD's external and internal user authentication design patterns to determine which authentication protocol is appropriate for use with their system.

1.3 Scope

This design pattern describes the "to-be" state for the authentication of external users. Defined as users who access VA resources from outside of the VA 'network'. This includes users accessing information from any type of device, mobile or not. In addition to describing the "static" rules for authentication, the design pattern describes the response to the need for authentication protocols that can support attribute- and risk-based access controls.

- ❖ This pattern does not address standards for passing user authentication data for the purposes of making authorization decisions.
- ❖ This pattern does not address user identity authentication for internal users, defined as VA employees or Contractors or other stakeholders who access VA resources through machines on 'the VA network' or connected to it through Citrix Access Gateway (CAG), leveraging Active Directory, Single Sign-On Internal (SSOi), or Direct PKI. These standards are described in the Authentication, Authorization, and Audit Design Pattern Increment 1.
- ❖ 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.
- ❖ This document may refer to specific current technologies, but the design pattern itself is vendor-agnostic.

1.4 Document Development and Maintenance

This design pattern was developed collaboratively with stakeholders from the Enterprise Shared Services (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 user identity authentication processes and capabilities that VA will implement. It supports the Enterprise Technology Strategic Plan vision for the expanded use of shared services that support VA's goals of increasing security, decreasing total cost of ownership (TCO) and increasing information re-use/agility.

2.1 External User Authentication

User authentication to VA resources: applications, 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;
- provides non-repudiation of identity, integrity, and origin of data;
- provides availability of data for users;
- and provides auditability for the enterprise.

To perform proper authentication, information system owners must use authentication protocols that conform to the NIST 800-63-2 framework that requires the specific type(s) of identity credential used in an identity authentication process be 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. To conduct reliable external user authentication, information system owners shall comply with the established VA architecture for external user authentication provided by IAM through the Single Sign on External (SSOe) service.

2.2 Authentication to VA Resources

External User Credentials

Core Concepts:

1. **User identity assertions shall only be accepted from Credential Service Providers that are FICAM approved and that are integrated with the enterprise IAM SSOe.** Applications shall not require application specific credentials for login but shall leverage the IAM architecture.
2. **User credentials shall be appropriate for use in the requested environment:** Information system owners shall ensure that any credential employed for user authentication is appropriate for the system's environment and the sensitivity level of the information that it provide access to.
3. **IAM SSOe shall ensure that any credential employed for user authentication has been validated by a trusted and approved Credential Service Provider (CSP).**
4. **Approved CSPs shall verify that any identity credential employed for identity authentication is valid at the time of presentation:** Information systems must check that the user credential presented has not been revoked by the identity credential provider or otherwise declared invalid.
5. **Information systems shall only authorize users who present credentials, to approved CSPs, 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.

- 6. The IAM program for SSOe shall approve additional CSPs as needed to facilitate access to VA resources:** The IAM Business Program Management Office (BPMO) has developed requirements that manage the onboarding and integration of CSPs with SSOe. All CSPs are required to be FICAM compliant or submit to review and approval by IAM.

Types of User Credentials

Identity credentials available to External VA users for identity authentication include:

- **VA-issued PIV Cards:** PIV cards and PKI authentication are LOA 4 and below credentials.
- **Other Federally Issued PIV Cards and CAC Cards:** PIV cards and CAC cards combined with PKI authentication are LOA 4 credentials and below.
- **Other credentials supported by trusted external CSPs. Including:**
 - Username and passwords (LOA 2 and below)
 - Username and Passwords in addition to the use of One Time Passwords (OTPs) and/or Out of Band Tokens (LOA 3 and below)

VA CSP Approach

VA has adopted a federated approach that allows the use of many different credential types to access VA resources. This approach allows external users to authenticate to requested VA information resources using the credential that is most convenient for them (given that it meets, the proper LOA). The goal is to provide users with access to multiple VA resources without requiring separate authentication for each one. This approach achieves the goal of increasing access to VA resources while eliminating complexity for external users.

VA has approved a number of external CSPs in order to support a variety of credentials and LOAs. VA will continue the process of approving CSPs as needed. It is envisioned that the creation of the Federal Cloud Credential Exchange (FCCX) may reduce or eliminate the need for VA to separately approve CSPs on a case-by-case basis, and instead, would allow VA to leverage CSPs through the FCCX.

Information concerning currently on-boarded CSPs can be obtained from the IAM office.

External CSPs and User Attributes

The IAM Business Program Management Office (BPMO) has established a formal process for evaluating and approving CSPs to provide user credentials to the enterprise. VA's future authentication and authorization environment will require that a 'rich' user profile (one that contains required user attributes) be provided to allow for proper implementation of access control services. VA's current mandatory set of user attributes is defined by MVI. The IAM BPMO is working with the FCCX to ensure that all Federally approved CSPs implement and pass required attributes. This will allow the enterprise to securely authenticate and authorize users as needed.

In addition, the ESS Security group has defined a common attribute set for the IAM SAML broker token. This standard is maintained and published by the ESS Security group in conjunction with the ESS governance bodies to provide application developers with a understanding of available user attributes.

Federal Cloud Credential Exchange (FCCX)

FCCX is a cross-agency cloud service that would provide an “easy button” for federal agencies to use a wide range of Federal Identity, Credential, and Access Management (FICAM)-approved credentials, while allowing citizens to use private sector-issued credentials across multiple agencies and applications. By setting up a government-wide cloud service that handles the heavy lifting, each agency would only need to connect once to FCCX to take advantage of the increasing number of FICAM-approved third party credentials in the Identity Ecosystem.

The FCCX adheres to the National Strategy for Trusted Identities in Cyberspace (NSTIC) Guiding Principles by developing a secure, privacy-enhancing, and easy-to-use solution for streamlining digital authentication. Further, FCCX will reduce costs for government agencies, improve the customer experience, and facilitate maturation of the Identity Ecosystem.

FCCX is a White House led initiative being implemented with support from the U.S. Postal Service, the General Services Administration, and the NIST’s NSTIC National Program Office.

2.3 Levels of Assurance (LOA) Framework

Core Concepts:

- 1. VA Applications shall implement LOA requirements for authentication:** VA shall use guidance from OMB 04-04 and NIST SP 800-63-2 to rate all existing applications to their appropriate LOA and implement appropriate security controls for user authentication to those applications.
- 2. LOA for a user’s authentication shall be determined by the weakest link in the authentication process**
- 3. Application authentication protocols shall comply with all existing policy 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, Revision 1 Guide for Conducting Risk Assessment, 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. Additionally, GSA provides an electronic risk and requirements assessment (e-RA) tool and activity guide to assist in conducting assessments and mappings, which is posted at: <http://www.idmanagement.gov/resource/electronic-risk-and-requirements-assessment-e-ra-tool>
- 3. Conducted integration with IAM SSOe based on authentication technical guidance** – VA’s default authentication protocol is the use of IAM single sign-on external (SSOe) for all external user identity authentications.
- 4. Validate that the implemented system has met the required assurance level** – In conjunction with OIT OIS will use NIST SP 800-53A to conduct an assessment to determine if the application has met 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 were 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 for an application/service is based on the consequences 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			Example of credentials meeting requirements
		Identity Proofing Requirements	Token (Secret) Requirements	Authentication Protection Mechanisms 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 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) ¹ 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 stringent and in-person registration	Multi-factor authentication with a hardware crypto token (Use of barer tokens 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 C)

LOA 1

All applications are required to comply with minimum security standards set forth by VA 6500, FIPS 200, NIST 800-53, and NIST 800-63-2. At LOA 1 there are no special user identity authentication requirements.

LOA 2

LOA 2 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 that is protected through the use of a secure (encrypted) TLS protocol session (tunneling).

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.

LOA 3

Level 3 provides multi-factor 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 800-63-2 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 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 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 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 must be factored 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: An external VA user requests access to a VA application, integrated with IAM SSOe and rated at LOA 2; that application redirects the user to an approved CSP for user authentication; the user authenticates using an LOA 2 credential (username and password); and is granted access to the SSOe integrated application. The LOA for this entire process

would be LOA 2. Had the user attempted, during the same session, to access an additional application or perform a function within the current application that rated at LOA 3, the application or SSOe should have prompted the user to re-authenticate at a higher LOA.

Other Security Controls

The LOA requirements outlined in NIST 800-63-2 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.

2.4 Enterprise Shared Services

Core Concepts:

- 1. Enterprise Shared Services shall be used to facilitate authentication, authorization, and auditing:** VA shared services include the delivery of some security services as enterprise shared services. Through the implementation of the IAM program individual applications shall leverage enterprise security services. The use of enterprise security services increases security through the application of common, consistent, and centrally managed security services and policies. Through the use of enterprise security services application developers can reduce time spend developing redundant application level security services.
- 2. Leverage enterprise identity and attribute management stores:** VA has adopted the Master Veteran Index (MVI) as the central identity and attributes management structure. VA has identified the MVI as the appropriate enterprise identity store (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 IAM AcS Provisioning Service will not be the only identity and attribute management store, but is the central identity and attribute repository. VA will implement a structure that allows federation of user identities and attributes across existing user stores.
- 3. Authentication protocols shall 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, auditability, and availability services for the VA's platform.

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

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

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

Authentication and Authorization

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 support the transmission of user attributes can help facilitate the design and implementation of these advanced authorization controls.

2.5 Adaptive Authentication Requirements

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*.

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 VA 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.
- 4. Implement capability to control and log-out user sessions:** VA authentication services must be able to monitor user sessions and ensure or force user log-out (single Log-out) across all applications as needed.

Step-Up Authentication

Authentication protocols must have functionality in place to allow a user to re-authenticate to a higher 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 during a user’s session at a point where an increase LOA authentication is necessary. This functionality is required to enable a true SSO session where a user may request to access different resources which may or may not match the LOA of the credential with which the user was authenticated.

Additionally the implementation of step-up authentication can offer application designers the ability to expose different services within their application at different LOAs depending on the ratings of those services. For instance, viewing information might require a LOA2, but updating that information may require an LOA3. This enterprise step-up authentication service can be leveraged by application designers to enable these different authentication controls, given that the proper security controls are present within the application.

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 a current or higher LOA based on the risks levels associated with a user’s session, or a change in the threat environment. Additionally VA should design a risk-based component of the adaptive authentication system that can take in account additional information provided by trusted external identity intelligence provides. Vetted indicators of fraud and abuse, such as known hostile IP addresses, should be evaluated in real-time along with behavioral elements in determining when to issue re-authentication challenges.

Single Log-Out

The implementation of the capability to monitor and manage the single log out of all of a user’s sessions across all applications that are integrated with IAM is important. This will ensure that user sessions within some applications do not continue past the validity of the token issued by IAM or are not inadvertently left logged in when the use terminates their session with IAM.

3 DESIGN PATTERN ARCHITECTURE

Core Concepts:

- 1. Information systems shall only conduct external user identity authentication using VA’s approved framework.** The VA implementation of the SSOe (VAAF1) service allows applications to rely on enterprise services to perform many of the trust, policy verification, and authentication actions required to secure the application. The SSO implementation is consistent with an approach based on Service Oriented Architecture (SOA) and is a key component of ESS.
- 2. Established security policies and guidelines: NIST 800-53, NIST 800-63-2, and VA 6500 shall be respected.** Applications must meet established security standards contained in the VA6500 and other security controls as appropriately identified by their VA Information Security Officer (ISO). The ISO will work with teams to ensure that all applicable standards are implemented as required.

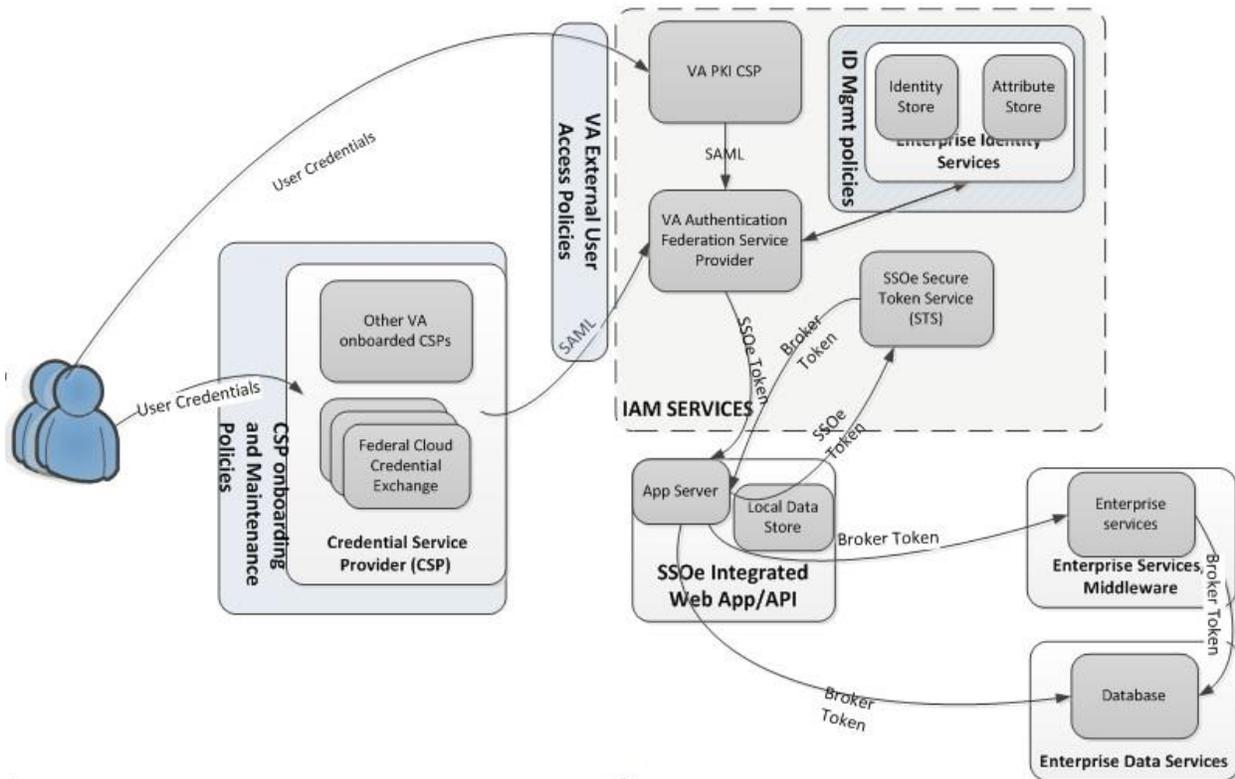


Figure 1 - To-Be External User Authentication Design Pattern

3.1 External User Identity Authentication to VA resources

The Enterprise Design pattern for External User Identity Authentication, (Figure 1), reflects the consolidated Single Sign-on approach that VA is implementing. This approach allows application designers to perform a single integration with IAM SSOe, which avoids the need to integrate with many different CSPs. This architecture also allows external users to authenticate once to VA and gain access to many different resources.

In this architecture the IAM SSOe platform is integrated with a number of CSPs, which are either externally or internally managed. The CSPs provide identity assertions in the form of SAML tokens to the VA Authentication Federation Service Provider within the SSOe infrastructure. Once received by the Federation Service Provider, the token is validated and the service provider brokers the connection from the user to the application. In the brokered connection, user information is passed to SSOe integrated applications in HTTP headers, called SSOe Tokens in the diagram above.

It is important to note that the high level architecture above does not include all the details concerning the implementation of SSOe inside VA. Detailed architecture for SSOe infrastructure is provided in the *Identity and Access Management VA Authentication Federation Infrastructure (VAAFI) System Design Document*.

The SSOe implementation is designed to support a number of authentication flows due to the complexity of possible authentication paths. These include: unprotected resources, authentication from AccessVA website, authentication from a CSP, authentication from an integrated application.

3.2 Application Integration with SSOe

As mentioned above, the design of the SSOe Infrastructure only requires application owners to integrate once with the SSOe to enable the full suite of authentication services that it provides. This architecture simplifies application design, while allowing applications to take advantage of the SSOe capabilities. In addition, by allowing SSOe to manage the authentication process, application security is assured through the adoption of a common enterprise approved authentication standard. Finally, the use of SSOe Services by applications allows external users to obtain VA services with a variety of existing credentials and credential service providers. This reduces the need for VA to maintain a diverse set of user stores that support individual applications.

In order to facilitate integration with applications the IAM team has created a series of integration patterns for VA's Access Services. These include patterns for application owners to use to integrate with Single Sign-On External, Single Sign-On Internal, Credential Service Providers, Electronic Signature services, Identity Proofing, User Provisioning, Specialized Access Control, and Compliance Audit and Reporting Services. Integration patterns are included in the *IAM Access Service Integration Patterns* Document available on the Access Services TSPR site (<http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1653&Type=Active>).

3.3 Support for Mobile Authentication

Mobile applications should be designed to leverage the SSOe authentication framework. This framework will allow these applications to use FICAM compliant CSPs that have already been approved by VA. SSOe has solutions that support both native client and HTML. IAM solutions are designed to work in environments using both SOAP and REST based architecture and can work with project teams to identify and provide solutions that work best for their user base.

Furthermore, IAM will provide support for mobile authorization through an implementation of OAuth.

3.4 Identity Propagation

Because applications frequently need to call on middleware and other enterprise services to fulfill their functions the SSOe Infrastructure contains a Secure Token Service (STS). The STS allows integrated applications to exchange SSOe tokens for brokered tokens in order to assert the authenticated user's identities to enterprise middleware and enterprise data services. This assertion of the user's identity is important as service calls traverse system boundaries. These secure assertions allow consuming systems to have some level of confidence that the calling application is interacting with an approved user. Additionally the passing of tokens between systems can allow for additional user attributes to be passed that can be used to make authorization decisions and to enable audit functions.

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. 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	<ul style="list-style-type: none"> • Directive information security program. • Defining overall security framework for VA.
2	VA	VA 6300 Directive	<ul style="list-style-type: none"> • Directive records and information management. • Defines information management framework for VA access services.
3	NIST	SP 800-53-4	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Federal Information Processing Standards Publication — security requirements for cryptographic modules. • Defines the cryptographic standards and requirements.
7	NIST	SP 800-122	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Memorandum to the heads of all departments and agencies – e-authentication guidance for federal agencies. • Defines the e-authentication requirement.
9	GSA	FICAM	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • National Strategy for Trusted Identities in Cyberspace – Provides guidance for identity trust in cyberspace.
11	US Congress	FISMA	<ul style="list-style-type: none"> • FISMA of 2002, Public Law 107-347
12	US Congress	E-Government Act of 2002	<ul style="list-style-type: none"> • Federal management and promotion of electronic government services. • Defines the requirements for electronic services.
13	US Congress	The Privacy Act of 1974	<ul style="list-style-type: none"> • § 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	<ul style="list-style-type: none"> Establishes the framework for records management programs in federal agencies.
15	VA	VA D 0735	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Implementation of HSPD 12 – policy for a common identification.

Appendix C. 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 800-63-2.

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 800-63-2.
 - 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, they 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 authenticate 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 of 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 shared 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.