Guidelines and Design Patterns for Single Sign-On (SSO) in VA

1. Strategic Guidelines

Here are the key **strategy elements** and **implementation guidelines** for Single Sign-On (SSO) in VA IT systems:

🎯 Strategic Principles

- **Enterprise Integration**
  Centralized authentication via VA's internal (Entra ID) and external (Okta) SSO services ensures all VA services integrate with SSO when technically feasible [1]. Governed by OMB M-11-11, FIPS 200, NIST SP 800-63/53, and FICAM [1].
- **Identity Assurance & Trust**
  Align authentication events, session security, and assurance levels (AALs) with NIST 800-63 Guidance, ensuring that session persistence, AALs, and token lifetimes correspond to applicable risk levels [1].

🛠 Technical Guidelines

1. Session Management & Binding

- Sessions must maintain an assurance level no higher than the authentication event.
- Secrets must be cryptographically random (min. 64 bits entropy, SP 800-90Ar1) [1].
- Secret must be securely stored, tied to HTTPS, invalidated on logout, and not available via local storage [1].

2. Session Tokens

- Cookies flagged as Secure, HttpOnly, bound to relevant domains, with explicit expiry aligned to session lifetime [1].
- URLs/POST content containing session identifiers must be validated by the relying party to prevent replay and tampering [1].

3. Federation & Token Handling

- OAuth tokens for authorization but not authentication [1].

- In federation, RPs must enforce max authentication age; IdPs must provide timestamp; use forceAuthn (SAML) or prompt=login (OIDC) [1].

4. Adaptive and Step-Up Authentication

- Implement adaptive MFA per NIST SP 800-53 IA-10, requiring step-up to higher AALs for richer resources [1].
- Sessions may trigger reauthentication based on risk or policy deviations [1].

5. Reauthentication Policy

- Enforce reauthentication thresholds per NIST SP 800-63B:
  - AAL1: 30 days
  - AAL2: 12 hours or 30 min inactivity
  - AAL3: 12 hours or 15 min inactivity [1].

6. Rate Limiting & Anti-brute Force

- Lockout threshold after no more than 100 failed attempts
- Use CAPTCHAs, delays, IP whitelisting, and anomaly detection [1].

🚧 **Exception Handling**

- **Legacy App Exemptions**
  If direct SSO integration is infeasible, a compliant proxy may be used, but must reside inside a **Device Isolation Architecture (DIA)** [1].
- **NTLMv2 / Smart Card Weakness**
  Use DIA for NTLM-based SSO to mitigate credential replay/self-hash risks [1].

📄 **Governance, Compliance, Auditing**

- Align SSO usage with VA Handbook 6500 and Directive 6500 on information security [2][3].
- Comply with VA Handbook/Directive 6510 on Identity, Credential & Access Management (ICAM), including PIV, credential levels, assurance levels, lifecycle, and audit logs [4][5].
- Maintain all authentication/audit logs per VA retention policy [1].

📦 Technology & Tooling

- VA Technical Reference Model recommends supported SSO tools (e.g., Citrix Workspace for SSO) operate under VA security standards (FIPS, Section 508, VA Handbooks 6102/6500, VA Directives 6004/6513/6517) [2][6].

✅ Summary Checklist

Domain	Key Controls & Policies
Session Security	Secure cookies, encrypted tokens, proper expirations, HTTPS
Federation Compliance	Force reauth via SAML forceAuthn / OIDC prompt=login
Reauthentication	Enforce AAL-based timeouts & inactivity thresholds
MFA & Adaptive Auth	NIST SP 800-63/SP 800-53 compliance, step-up flows
Logging & Auditing	Full retention, audit trails per VA policy
Exceptions Management	Use DIA proxies for legacy apps or NTLMv2

This framework ensures that VA SSO is secure, compliant, user-friendly, and aligned with federal and VA-specific cybersecurity mandates.

References

[1] Identity and Access Management (IAM) Enterprise Design Pattern

[2] Single Sign-on (SSO) - DigitalVA

[3] ACCESS MANAGEMENT - Department of Veteran Affairs VA ... - 1Library

[4] Department of Veterans Affairs VA HANDBOOK 6510 Washington, DC 20420 ...

[5] Department of Veterans Affairs VA DIRECTIVE 6510 Washington, DC 20420 ...

[6] Citrix Gateway - DigitalVA

2. Implementation Roadmap

The following is a **concise SSO implementation roadmap** tailored for VA IT systems:

Phase 1: Strategy & Governance

- **Define Objectives**: Centralize authentication, improve security, enhance user experience.
- **Align with Standards**: OMB M-11-11, NIST SP 800-63/53, FICAM, VA Handbook 6500 & Directive 6510.
- **Establish Governance**: Create SSO policy, compliance checks, and audit requirements.

Phase 2: Architecture & Design

- **Select SSO Model**: Internal (Entra ID) and external (Okta) federation.
- **Define Assurance Levels (AAL)**: Map apps to AAL1–AAL3 per NIST guidelines.
- **Plan Session Management**: Secure cookies, HTTPS-only, proper expirations.
- **Integrate MFA & Adaptive Auth**: Step-up authentication for sensitive resources.

Phase 3: Technology & Integration

- **Choose Protocols**: SAML 2.0, OIDC for federation; OAuth for authorization.
- **Implement Token Security**: Cryptographically strong secrets, secure storage.
- **Legacy Systems**: Use DIA-based proxy for apps that cannot directly integrate.

Phase 4: Deployment & Testing

- **Pilot Rollout**: Start with low-risk apps, validate session handling and reauthentication.
- **Security Testing**: Penetration tests, replay protection, rate limiting.
- **Accessibility & Compliance**: Section 508, FIPS, VA TRM standards.

Phase 5: Operations & Monitoring

- **Logging & Auditing**: Maintain authentication logs per VA retention policy.
- **Continuous Monitoring**: Detect anomalies, enforce lockout thresholds.
- **Periodic Review**: Validate AAL compliance, update policies as standards evolve.

✅ **Key Milestones**:

1. Governance framework approved
2. Architecture finalized
3. Pilot completed
4. Full rollout across VA systems
5. Continuous compliance & monitoring

3. Design Patterns

🛡️ VA Internal vs External Authentication Design Patterns

Internal User Authentication (VA Employees, Contractors, Volunteers)

1. **PIV-First Strategy**
   - **Requirement**: PIV credentials per OMB M-11-11 used for all internal network, facility, and system access [1][2].
   - **Implementation**: Integrated with Active Directory and internal SSO (Entra ID) service for seamless enterprise login [3][2].
2. **Session Management**
   - Use secure cookies over HTTPS, HttpOnly flags, scoped to minimal domain, no HTML5 storage [2].
   - Session secrets generated via SP 800-90A–compliant RNG with ≥64 bits entropy, invalidated on logout [2].
3. **Adaptive Authentication & Step-Up**
   - Step-up flows using MFA (PIV-based or elevated authenticator) when accessing higher-assurance resources [2].
   - Scheduled reauthentication per AAL: AAL2 max 12 hrs/30 min idle; AAL3 max 12 hrs/15 min idle [2].
4. **Proxy & DIA for Legacy**

- Non-SAML/PIV◊ use compliant proxy within Device Isolation Architecture (DIA) to uphold AAL and prevent credential replay [2].

External User Authentication (Veterans, Beneficiaries, Partners)

1. **Federated Identity with CSPs**
   - Uses SSOe with SAML, leveraging trusted identity providers like Login.gov, [4][1].
2. **Level of Assurance (LOA)-Driven Flows**
   - **LOA1**: Basic auth via CSP, limited access.
   - **LOA3**: Strong identity proofing for protected VA systems (to access personal or health data) leveraging stricter credentials [5][1].
3. **Adaptive & Step-Up Authentication**
   - External users may initiate at LOA1, then require step-up (MFA/higher proofing) to reach LOA2/3 for sensitive actions [1][5].
4. **Account Lifecycle & Recovery**
   - External account restoration uses same assurance-level-linked MFA and verified identity proof mechanisms [6][7].
5. **Federation Protocol Controls**
   - Applications must enforce “max authentication age” and use SAML forceAuthn or OIDC prompt=login to require fresh logins [2].

🧩 **Shared Design Components**

- **Session Binding & Security**
  Session secrets aligned with AAL levels; secure cookies; token validations in URLs or POSTs [2].
- **Rate Limiting & Brute Force Defense**
  Lock accounts after ≤ 100 failed attempts; introduce CAPTCHA, delays, IP analysis [2].

- **Adaptive Authentication**
  Via NIST 800-53 IA-10: trigger reauthentication for new security risks or high AAL access [2].
- **Reauthentication Policies**
  Enforce time-bound reauth thresholds: AAL1 = 30 days; AAL2/3 = 12 hrs with inactivity limits [2].
- **Logging & Monitoring**
  Full authentication/audit logs retained per VA policy to facilitate SIEM, compliance, breach detection [1][2].

These design patterns ensure VA systems authenticate both internal and external users securely, flexibly, and in compliance with VA and federal IAM standards.VA IT systems should follow these **design patterns for internal and external user authentication**:

✅ **Internal Users (Employees, Contractors, Volunteers)**

- **PIV-First Authentication**: Use Personal Identity Verification (PIV) cards as the primary credential per OMB M-11-11.
- **Entra ID Integration**: Implement Single Internal Sign-On tied to Active Directory for centralized login.
- **Session Security**: Enforce HTTPS-only sessions, secure cookies (HttpOnly, Secure), and SP 800-90A-compliant session secrets.
- **Adaptive & Step-Up Authentication**: Require MFA or reauthentication for higher-assurance resources.
- **Legacy Support**: Use compliant proxies within Device Isolation Architecture (DIA) for apps that cannot support Entra ID.

✅ **External Users (Veterans, Partners, Public)**

- **Federated Identity via External SSO**: Integrate with Credential Service Providers (Login.gov, Okta) using SAML.
- **Assurance-Level Driven Access**: Apply NIST SP 800-63 LOA/AAL standards (e.g., LOA1 for basic access, LOA3 for sensitive data).

- **Step-Up Authentication**: Elevate authentication when accessing sensitive services.
- **Account Recovery**: Use MFA and identity proofing for account restoration.
- **Federation Controls**: Enforce max authentication age and use forceAuthn (SAML) or prompt=login (OIDC) for reauthentication.

🔒 **Shared Security Practices**

- **Session Binding**: Strong cryptographic secrets, no insecure storage, proper expiration.
- **Rate Limiting**: Lock accounts after failed attempts, use CAPTCHA and anomaly detection.
- **Reauthentication Policy**: AAL1 = 30 days; AAL2/3 = 12 hours with inactivity limits.
- **Audit & Monitoring**: Maintain logs per VA policy for compliance and incident response.

References

[1] User Identity Authentication EDP ExSum - data.va.gov

[2] Identity and Access Management (IAM) Enterprise Design Pattern

[3] VA Enterprise Design Patterns - 1.1 (Privacy and Security) Internal ...

[4] Single Sign-on External (SSOe)

[5] Authentication Patterns | department-of-veterans-affairs/va.gov-team ...

[6] Identity and Access Management (IAM) Enterprise Design Pattern

[7] Identity and Access Management (IAM) Enterprise Design Pattern