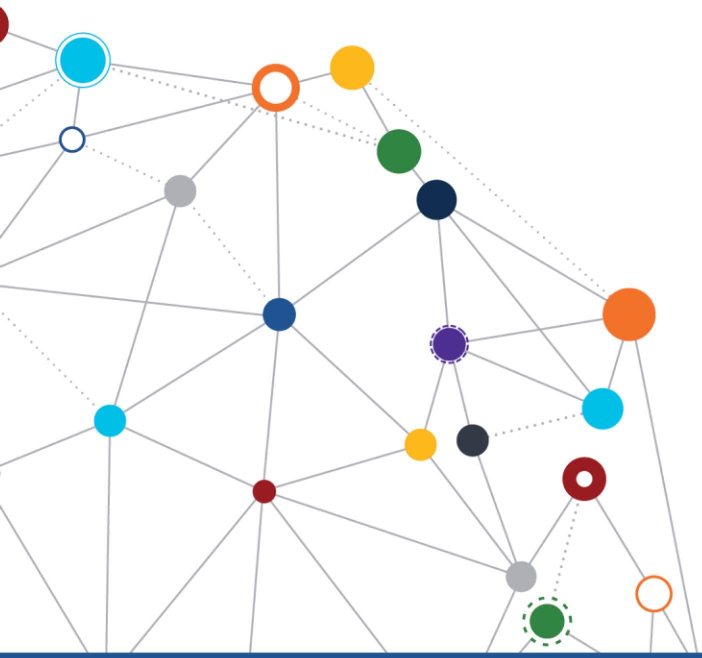
OFFICE OF
INFORMATION
AND TECHNOLOGY

Identity and Access Management (IAM) Enterprise Design Pattern

User Account Restoration

March 2019 | Enterprise Program Management Office



VA
U.S. Department of Veterans Affairs
Office of Information and Technology

Table of Contents

Table 1: Change Matrix

Version	Date	Description of Updates
1.0	3/4/2019	IAM Segment: User Account Restoration approved

1 Context

The Department of Veterans Affairs (VA) has a unified enterprise Identity and Access Management (IAM) program to coordinate secure access to VA resources for both internal and external users. IAM services are guided by the Office of Management and Budget (OMB) M 11-11,[1] the Federal Information Processing Standard (FIPS) 200, the National Institute of Standards and Technology (NIST) Guidelines (800-63 and 800-53 per Appendix D), and the Federal Identity, Credential, and Access Management (FICAM) initiative.

VA has two general populations of users who require access: (1) internal users include employees, contractors, trainees, and volunteers, and (2) external users, comprised of Veterans, beneficiaries, and health partners, including employees and contractors from other Government agencies. All require varying levels of access to interact with VA services.

2 Challenge

“Identity is the new perimeter,” a commonly used online phrase to indicate the growing significance of identity and access management to cyber security, followed the movement to cloud and mobile platform solutions. Hence, identifying and authenticating the user has become a significant factor in preventing unauthorized access and data breaches. From phishing to SMS intercept,[2] new threats are being refined. Single factor (SF) authentication has become high risk and even two-step verification methods (also known as two-factor authentication) are being compromised. In response to these challenges, multifactor authentication (MFA) is becoming the norm. Federal agencies have adopted Homeland Security Presidential Directive 12 (HSPD-12)[3] and personal identification verification (PIV) cards, while many enterprises have adopted smartcards, or hardware tokens. This leaves the broader user population with a mix of methods from service providers, with varying levels of usability and security.

The VA strives to make services accessible while protecting sensitive information and preventing the loss of funds through fraud. This drives VA IAM to design effective access management services. However, even a strong authentication strategy can be subverted by weak account restoration practices. Users can become frustrated by account takeover attacks when they have followed all the security best practices afforded by the provider.[3] VA requires

[1] Note that M 11-11 is a pending rescission. A draft OMB policy aligned with NIST 800-63 can be found at https://policy.cio.gov/identity-draft/.

[2] For more information on SS7 vulnerabilities, refer to https://secure-voice.com/ss7_attacks/.

[3] For more information on Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, refer to https://www.dhs.gov/homeland-security-presidential-directive-12.

[3] For more information on two-factor vulnerabilities, refer to https://www.zdnet.com/article/password-reset-flaw-at-frontier-allowed-account-takeovers/.

enterprise guidance on the design of account restoration to provide consistent security and limit risks. The progression of how IAM services are engaged by users and system owners can be seen in Figure 1. This document focuses on the area highlighted in red.

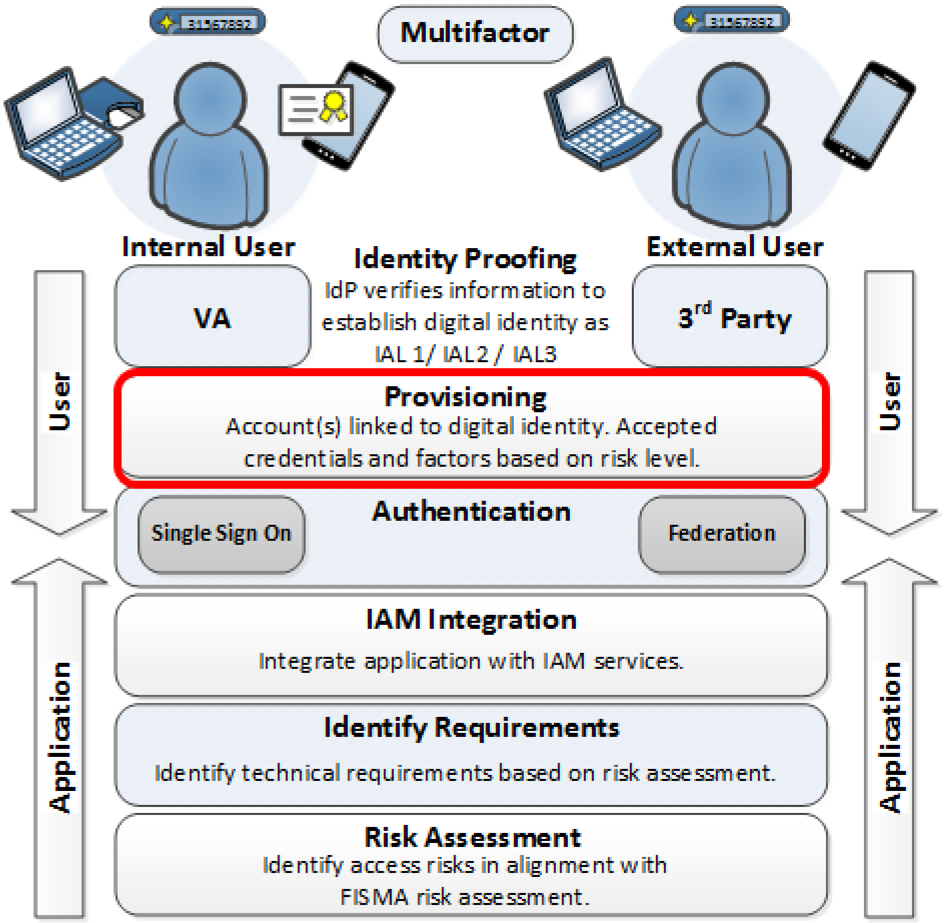

Multifactor
Internal User
External User
Identity Proofing
IdP verifies information to establish digital identity as IAL 1/ IAL2 / IAL3
VA
3rd Party
User
User
Provisioning
Account(s) linked to digital identity. Accepted credentials and factors based on risk level.
Authentication
Single Sign On
Federation
IAM Integration
Integrate application with IAM services.
Identify Requirements
Identify technical requirements based on risk assessment.
Risk Assessment
Identify access risks in alignment with FISMA risk assessment.
Application
Application

Figure 1: Overview of IAM Progression[4]

3 Guidance

Account restoration is the process of restoring access to a subscriber that has already been through the identity proofing process and provisioned an authenticator. There are multiple reasons that account restoration may be needed: devices may be lost, damaged, stolen from the owner, or compromised; or memorized secrets or look-up secrets may be forgotten or

[4] Figure 1 was created by the VA Office of Information and Technology (OIT) Architecture and Engineering Service (AES) Enterprise Design Pattern (EDP) Team from information obtained from VA OIT IAM Subject Matter Experts (SMEs) and the National Institute of Standards and Technology (NIST) Publication 800-63A at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

exposed. The account restoration process must be equivalent to the maximum risk level of the identity proofing and authenticator provisioned.

As each IAM area impacts the overall security of the transaction, it is important to properly protect each area of the identity lifecycle according to the acceptable risk level of the service accessed. Projects that are required to use the Veteran-Focused Integration Process (VIP)[5] are subject to the VA Assessment and Authorization (A&A) Process,[6] which is based on the Risk Management Framework (RMF).[7] Every subscriber accessing a VA service will have an identity proofing assurance level (IAL) at which they were proofed; and an authentication assurance level (AAL) at which an authenticator was issued, which will drive account restoration requirements.[8] This document will discuss account restoration requirements related to IAL and AAL.

3.1 VA Users

All VA internal users must undergo identity proofing before initiating any type of support operations at VA. The identity proofing process is part of the overall process for the binding and issuance of a PIV card.[9] There are different practices that apply that are based on the level of account restoration need.

A new PIV card is needed – The subscriber must contact the VA PIV Office. The evidence supplied for previous identity proofing must be used to confirm the binding of the subscriber to the card. The subscriber biometric should be verified. According to VA policy, lost PIV cards or authenticators must be reported to the VA PIV Office immediately.

- A new PIV personal identification number (PIN) is needed – If a user's PIN has been compromised or forgotten, the subscriber must contact a representative of the VA PIV Office to reset the subscriber's PIN. The PIV representative should verify the subscriber's identity against the PIV card and confirm the subscriber's biometric.

[5] Refer to the VIP 3.2 Guide, December 2018, at https://vaww.vaco.portal.va.gov/sites/OIT/epmo/vip/Policy%20%20Guidance/VIP%20Guide%203.2.pdf.

[6] Refer to the VIP Security Guide at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=27). The VIP Security Guide provides details about the A&A process and how it reflects an implementation of NIST guidance and VA security policies. For additional information on VA Assessment and Authorization, refer to https://www.va.gov/PROPATH/map_library/process_AAA_ext.pdf.

[7] Refer to the NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems,* at https://pages.nist.gov/800-63-3/sp800-63-3.html. In addition, the VA Handbook 6500, *Risk Management Framework for VA Information Systems*, can be referenced at https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2.

[8] Refer to the *IAM Risk Assessment* Enterprise Design Pattern (EDP) at https://www.oit.va.gov/library/recurring/edp/.

[9] Refer to the *IAM Identity Proofing* Enterprise Design Pattern (EDP) at https://www.oit.va.gov/library/recurring/edp/.

- A new hardware token is needed - The subscriber may use the PIV card to complete the enrollment process for a new hardware token. A hardware token may be required for some elevated access activities.
- A new Derived PIV Credential (DPC) is needed – The subscriber may use the PIV card to complete the enrollment process for a new DPC. A DPC is used when MFA is needed for a mobile or other device, where a PIV card cannot be used.

3.2 External User Authenticators

External users are dependent on the external credential service provider (CSP) to enforce compliance with best practices. Account restoration is based on the associated assurance level.

3.2.1External Users at IAL1 and Authenticators at AAL1

For IAL1, there is no requirement to link the applicant to a specific real-life identity. AAL1 provides minimal assurance that the subscriber controls the authenticator being used. At IAL1 and AAL1, the external CSP may restore account access by confirming subscriber control over a known account or device. This could be an email or SMS notification to a mobile device.

3.2.2External Users at IAL2 and Authenticators at AAL2

For subscribers that have been identity proofed at IAL2, or need to restore an authenticator at AAL2 or higher, the following applies.

- If all authenticators have been lost for a factor needed for MFA, the subscriber must repeat the identity proofing process to bind a new authenticator to the subscriber.

If the external CSP has retained all evidence from the initial identity proofing, the process may be abbreviated to the following.

- The subscriber must authenticate using a remaining factor to prove possession.
- The external CSP must validate the biometric captured during the identity proofing.

All account restoration events must send a notice to the subscriber address of record. All communications must use an encrypted tunnel.

4 Application of Practices

The following use case represents application of the MFA practices described in this document.

4.1 Account Restoration for an External User

4.1.1Purpose

Updated Federal policy has been released with new requirements for authentication. External users must comply with new VA policies for authentication to services that access sensitive information. An external CSP is required that is compliant with Federal and VA policy that can provision proof of subscribers at IAL2 and provision authenticators at AAL2.

4.1.2 Assumptions

- The external CSP was determined to be technically viable and approved by the VA Access and Identity Management (AIM) Program Management Office (PMO).
- The external user completed identity proofing at IAL2.
- The external user was provisioned an authenticator at AAL2.

4.1.3 Use Case Description

- An external user contacts VA to report that the user has forgotten the user’s password and cannot access the user account.
- As the external user is using federated login, the external user is directed to the external CSP for support.
- The external CSP looks up the identity evidence on file for the user and validates the evidence again.
- The external user provides a biometric for verification against the one on file.
- A new authenticator is issued to the external user, who confirms access is restored.

4.2 Key Practices

Table 5 highlights key practices identified in this Enterprise Design Pattern (EDP).

Table 2: Key Practices for IAM User Account Restoration

Category	Area	Description
Identity and Access Management	User Account Restoration	VA Users: • A new personal identity verification (PIV) card is needed – The subscriber must contact the VA PIV Office, as the evidence supplied for previous identity proofing must be used to confirm the binding of the subscriber to the card. The subscriber biometric should be verified. • A new PIV personal identification number (PIN) is needed – The subscriber must contact a representative of the PIV office to reset the subscriber PIN. The PIV representative should verify the subscriber’s

Category	Area	Description
		identity against the PIV card, and confirm the biometric. • A new hardware token is needed - The subscriber may use the PIV card to complete the enrollment process for a new hardware token. • A new Derived PIV Credential (DPC) is needed – The subscriber may use the PIV card to complete the enrollment process for a new DPC.
Identity and Access Management	User Account Restoration	External Users: At identity assurance level (IAL)1 and authentication assurance level (AAL)1, the external credential service provider (CSP) may restore account access by confirming subscriber control over a known account or device.
Identity and Access Management	User Account Restoration	External Users: For subscribers that have been identity proofed at IAL2, or need to restore an authenticator at AAL2 or higher, the following applies. If all authenticators have been lost for a factor needed for multifactor authentication (MFA), the subscriber must repeat the identity proofing process to bind a new authenticator to the subscriber. This process may be abbreviated to the following, if the external CSP has retained all evidence from the initial identity proofing. • The subscriber must authenticate using a remaining factor to prove possession. • The external CSP must validate the biometric captured during the identity proofing.
Identity and Access Management	User Account Restoration	External Users: All account restoration events must send a notice to the subscriber address of record. All communications must use an encrypted tunnel.

5 Impacts

If risk management is not used to define the technical requirements for IAM components of VA solutions, the following risks are increased:

- FISMA non-compliance, contributing to a material weakness, or other audit findings by external agencies with oversight
- Inadequate technical protections for sensitive data that may contribute to unauthorized access, data breach, or fraud

Appendix A: References

- DEA User Stories: https://vaww.portal2.va.gov/sites/asd/TechStrat/IPTS/SitePages/Home.aspx
- FISMA User Stories: https://vaww.portal2.va.gov/sites/asd/AERB/FISMASecurityCompliance/SitePages/Home.aspx
- TRM: http://trm.oit.va.gov/
- NIST 800-63-3: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
- VA 6500.3: http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=733&FType=2
- VA 6510 (under revision): http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=823&FType=2

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.

Statement of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and shall not be used for advertising or product endorsement purposes.