

ForgeRock and NIST

Special Publication 800-63-3

A paper by Rob Miller and Kelvin Brewer, with content from Steven Jarosz and Volker Scheuber, as well as key contributions from the ForgeRock Public Sector staff

Table of Contents

Introduction	2
NIST's Digital Identity Guidelines (SP 800-63-3)	2
Introduction to the Forgerock Platform	3
ForgeRock and NIST SP 800-63A	5
Enrollment and Identity Proofing	5
ForgeRock and NIST SP 800-63B	6
Authentication and Lifecycle Management	6
Authenticator Requirements Supported by ForgeRock	6
Authenticator Assurance Level 1 – AAL1	7
<i>Examples of Achieving AAL1 Using ForgeRock Intelligent Access</i>	8
Authenticator Assurance Level 2 – AAL2	9
<i>Examples of Achieving AAL2 Using ForgeRock Intelligent Access</i>	9
Authenticator Assurance Level 3 – AAL3	11
<i>Examples of Achieving AAL3 Using ForgeRock Intelligent Access</i>	11
ForgeRock and NIST SP 800-63C	13
Federation and Assertions	13
Closing Thoughts	14

Introduction

Positively identifying a digital entity is not easy. NIST's SP 800-63-3 actually says, "Digital Identity is hard." ForgeRock's Identity Platform, the most complete and flexible identity management solution in the industry, provides government agencies with an easy-to-use, simple-to-understand interface while handling the "hard" work of digital identity management behind the scenes.

Before NIST released the SP 800-63-3 guideline, the functionality to achieve full compliance was already built into the ForgeRock Identity Platform.

The purpose of this paper is to discuss how the ForgeRock platform approaches NIST SP 800-63-3 compliance, mapping the user authentication options to the applicable assurance levels.

Simple examples outline ways an administrator might configure the ForgeRock Identity Platform to achieve 800-63A, 800-63B, and 800-63C compliance.

NIST's Digital Identity Guidelines (SP 800-63-3)

NIST's latest iteration of the SP 800-63 series, SP 800-63-3, "Digital Identity Guidelines," makes it clear that it is no longer sufficient for an identity management implementation to meet a single level of assurance (LOA). Instead, the new guidelines require agencies to consider business and privacy risks combined with mission needs to select first, an Identity Assurance Level (IAL), second, an Authenticator Assurance Level (AAL), and third, for federated systems, a Federation Assurance Level (FAL).

Each of these new identity assurance levels have their own 800-63 special publication subset. Note that some of the information about assurance levels is taken unquoted out of the related NIST documentation for clarity and consistency.

NIST SP 800-63A, subtitled *Enrollment and Identity Proofing*, details the three different levels of mitigation — IAL1, IAL2, and IAL3 — based on risk profile and the potential harm caused by an attacker with a successfully authenticated false identity. With IAL1, all attributes are self-asserted, and no attempt is made to verify the real-world persona of the

identity claim. To achieve IAL2, the identity must exist in the real world and evidence must be provided to support the identity claim. IAL3 requires physical presence for identity proofing.

NIST SP 800-63B, subtitled *Authentication and Lifecycle Management*, details how to securely authenticate an individual to a credential service provider (CSP) to access digital services. Based on risk and proof of possession of authenticators bound to the claimant's account, there are three levels of AAL. AAL1 provides some assurance that the claimant possesses and controls a single or multi-factor authenticator through a secure authentication protocol. AAL2 provides higher confidence by using two distinct authentication factors over approved cryptographic techniques. AAL3 provides very high confidence by requiring the use of a hardware-based authenticator, verifier-based impersonation resistance, and two distinct authentication factors through approved cryptographic techniques.

NIST SP 800-63C, subtitled *Federation and Assertions*, addresses how an identity managed by one agency can be trusted, and used, at another agency without duplicating the identity. It also describes privacy-enhancing techniques, and methods that allow for strong multi-factor authentication (MFA), while the subject remains pseudonymous to the digital service. There are three levels of FAL. FAL1 allows the subscriber to enable the resource provider to receive a bearer assertion properly signed by the identity provider. FAL2 adds the requirement that the assertion be encrypted using approved cryptography such that the resource provider is the only party that can decrypt it. FAL3 requires the subscriber to present proof of possession of a cryptographic key referenced in the assertion in addition to the assertion artifact itself. The assertion is signed by the identity provider and encrypted to the resource provider using approved cryptography.

The standards themselves can be downloaded from the NIST website at the following links:

- [NIST 800-63-3: Digital Identity Guidelines](#)
- [800-63A: Enrollment and Identity Proofing](#)
- [800-63B: Authentication and Lifecycle Management](#)
- [800-63C: Federation and Assertions](#)

Introduction to the ForgeRock Platform

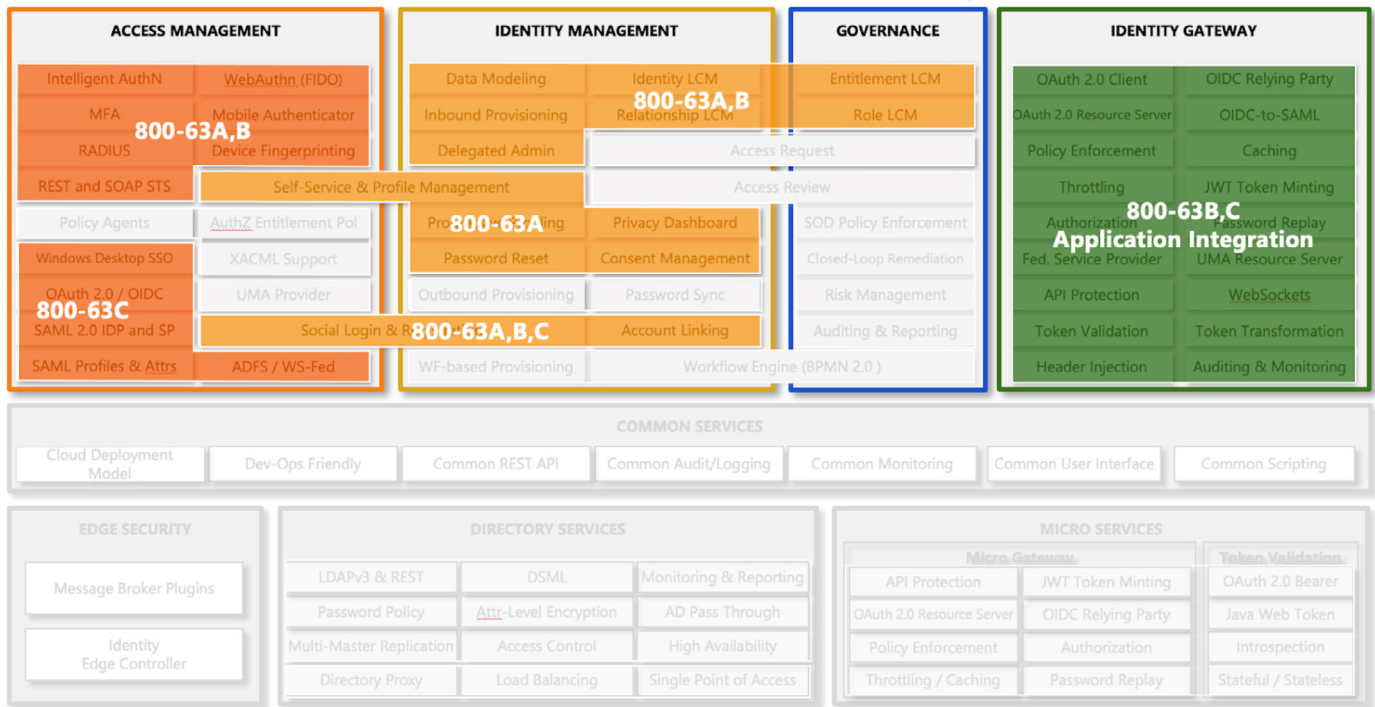
As the industry leader, ForgeRock continues to define the market with easy-to-use, state-of-the-art, artificial intelligence driven identity, credential, and access management. The ForgeRock Identity Platform provides the industry's most comprehensive and innovative set of tools and wraps them in a unique, user-friendly, administrator-driven graphical interface. Due to its open source beginnings, ForgeRock benefits from the involvement of an active and resilient community. ForgeRock is known as a robust and elastic ICAM solution, enabling millions of identities to securely access content throughout the U.S. federal government, state and local governments, and the education sector.

ForgeRock continues to innovate the standards and technologies used to facilitate access, with ForgeRock employees contributing to and leading standards boards. With the NIST SP 800-63-3 guidelines as a direct influence on ForgeRock development, ForgeRock provides public sector agencies the flexibility to quickly achieve and maintain compliance.

ForgeRock also attracts and partners with industry-leading technology companies. The result of these partnerships is a strong trust network whose integrations enrich identity and access processes, enabling multiple approaches to achieve compliance with the NIST SP 800-63-3 guidelines. More information about our trust network can be found at the [ForgeRock Marketplace](#).

The [ForgeRock Identity Platform](#) is broad and robust. Some key features of the platform used to achieve compliance with NIST SP 800-63-3 are:

- **Registration and end-user self-service:** User registration, forgotten username, password reset, and progressive profiling can be added to an authentication flow. Infusing these flows directly into the authentication tree means fewer clicks and less confusion for end users, landing them as authenticated users into the resource they were attempting to access. It also allows personalization of the self-service flows based on context.
- **Progressive profiling:** Intelligent Access trees allow progressive profile flows to be embedded directly into an authentication journey, creating a way for administrators to collect additional, consented user information within the context of the overall user journey.
- **Nodes and trees:** A key design principle of Intelligent Access is that trees are simple to design, build, and deploy. Using a simple drag-and-drop user interface (UI), administrators can create complex, yet user-friendly authentication journeys by linking nodes, creating loops, and nesting nodes within other nodes. The tree framework models the authentication journey using decision nodes to detect digital signals, make decisions, direct the authentication journey, and gather information. This information is used to determine risk and can inform downstream apps of the accumulated knowledge gained during the authentication journey, including, for example, the derived risk score.
- **Federation:** The ForgeRock Identity Platform supports all major federation and authorization standards, including SAML 2.0, WS-Federation, OAuth 2.0, OpenID Connect and User-Managed Access (UMA) and can be the identity provider, the service provider, and/or the relying party.



The ForgeRock platform offers many more features than those described above. For a comprehensive list, visit the ForgeRock Identity Platform [overview](#) and product [documentation](#).

For a complete list of classes and certifications, visit [ForgeRock University](#), part of [ForgeRock Backstage](#).

ForgeRock and NIST SP 800-63A

Enrollment and Identity Proofing

The guideline addresses how applicants prove their identities and enroll as valid subscribers within an identity system. Identity proofing and enrollment is possible at one of three different risk levels for scenarios where the applicant is remote or physically present.

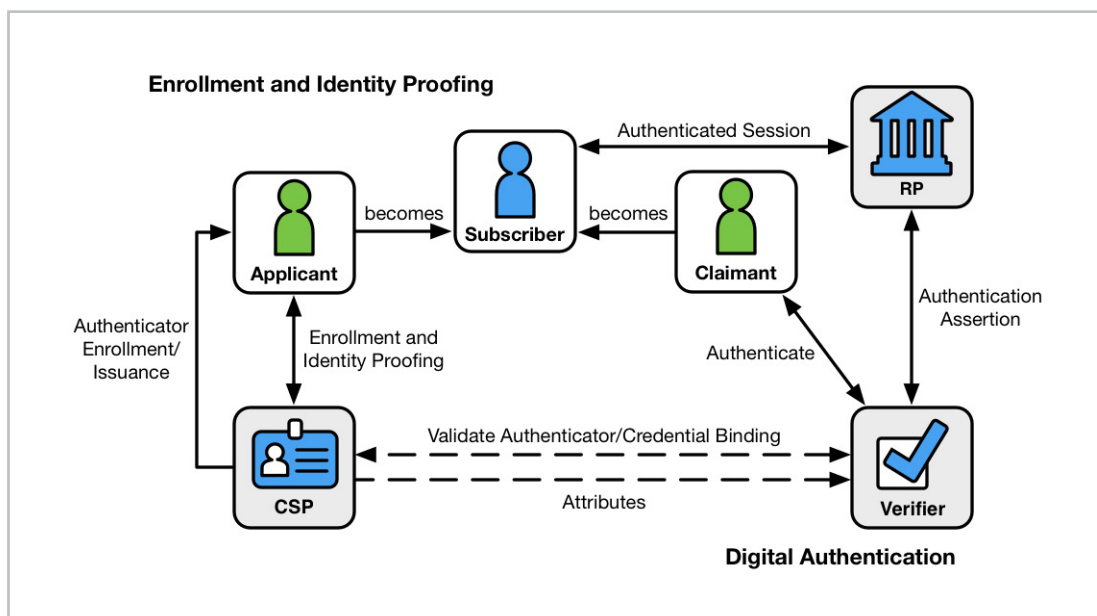
IAL1: No requirement to link the applicant to a specific real-life identity.

IAL2: Proof that the applicant is properly associated to the real-world existence of the claimed identity through the use of remote or physically-present identity proofing.

IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP.

ForgeRock Identity Management provides registration and [progressive profiling](#) services and works with major identity proofing services in order to acquire and record assurance levels for each of the attributes under ForgeRock's management. Each of the attributes stored can have associated meta-data indicating the asserted identity assurance level (IAL) from the authoritative source. In addition, ForgeRock Directory Services can encrypt all personally identifiable information (PII) data, at rest and in motion, based upon FIPS 140-2 algorithms. For additional information, see ForgeRock Identity Management [overview](#) or [documentation](#), and the ForgeRock Directory Services [overview](#) or [documentation](#).

Where appropriate, such as with some implementations of IAL1 and IAL2, ForgeRock's self-registration can be used to ease administrator load and end-user friction. Self-registration allows the applicant to register with an agency with minimal or no administrator interaction. Further exploration of this service can be found in the ForgeRock Identity Management [self-registration](#) and [self-service](#) documentation.



Source: <https://pages.nist.gov/800-63-3/sp800-63-3.html#63Sec4-Figure1>

ForgeRock and NIST SP 800-63B

Authentication and Lifecycle Management

Where the SP 800-63A covers an applicant's initial visit, the SP 800-63B guideline covers the successive authentications of that same subscriber when returning to use an agency's applications and services. To achieve guideline compliance, the authenticator mechanism must assure that the person accessing an agency's resources today is the same person, with the same identity, who accessed the resources yesterday. Each assurance level coincides with a level of risk comparable to the information provided by the agency resource.

The ForgeRock Identity Platform provides all required components to achieve NIST SP 800-63B compliance at all levels. Through its flexible architecture, ForgeRock allows agencies to select the authenticator type(s) necessary to meet the complex needs of their user base and achieve the required authenticator assurance level defined by their program or mission.

ForgeRock provides context-aware authentication and authorization services that match NIST's notion of "componentization," where strong authentication is a component of a comprehensive access management system.

The ForgeRock Identity Platform supports the notion of AAL with ForgeRock Access Management and Identity Gateway working together as a complete solution. This satisfies the requirement to provide risk-based and context-aware capabilities to adapt to evolving security

requirements against a dynamic, contextual session. (For more information, see the ForgeRock Access Management overview, the ForgeRock Access Management documentation, the ForgeRock Identity Gateway overview, and the ForgeRock Identity Gateway documentation.










AAL1-3 requires single-factor and multi-factor combinations that allow subscribers to choose authentication factors, and, depending on the choice, may require the subscriber to add one additional factor to achieve the highest assurance level, AAL3. ForgeRock's authentication trees offer an excellent solution to enable this complexity. See below for examples using ForgeRock Access Management trees and nodes.





ForgeRock also helps agencies achieve AAL3 (the highest level) using FIDO2 capable devices or browsers. This can be achieved using ForgeRock's implementation of WebAuthn (FIDO2) plus one-time passwords (OTP), with or without the need for third-party hardware. Third-party authenticators, such as YubiKeys, may be required by an implementation today. As maturing hardware and features, including fingerprint readers, become commonplace, the need for third-party hardware will diminish. Agencies that already possess or wish to pilot these more mature platforms can use ForgeRock as it exists today to achieve this advanced use case.










Authenticator Requirements Supported by ForgeRock

All authenticator requirements covered in SP 800-63B section 5.1 are supported by the ForgeRock Identity Platform and the ForgeRock Marketplace. The next three sections discuss each authenticator type relative to the authenticator assurance levels AAL1, AAL2, and AAL3.

AAL1 Permitted Authenticator Types










	Memorized Secrets		Look-Up Secrets		Out-of-Band Devices
	Single-Factor OTP Device		Multi-Factor OTP Devices		Single-Factor Cryptographic Software
	Single-Factor Cryptographic Devices		Multi-Factor Cryptographic Software		Multi-Factor Cryptographic Devices

AAL2 Permitted Authenticator Types					
	Multi-Factor OTP Devices		Multi-Factor Cryptographic Software		Multi-Factor Cryptographic Devices
	Memorized Secrets	+	Look-up Secret Out-of-Band SF OTP Device	SF Crypto Software SF Crypto Device	

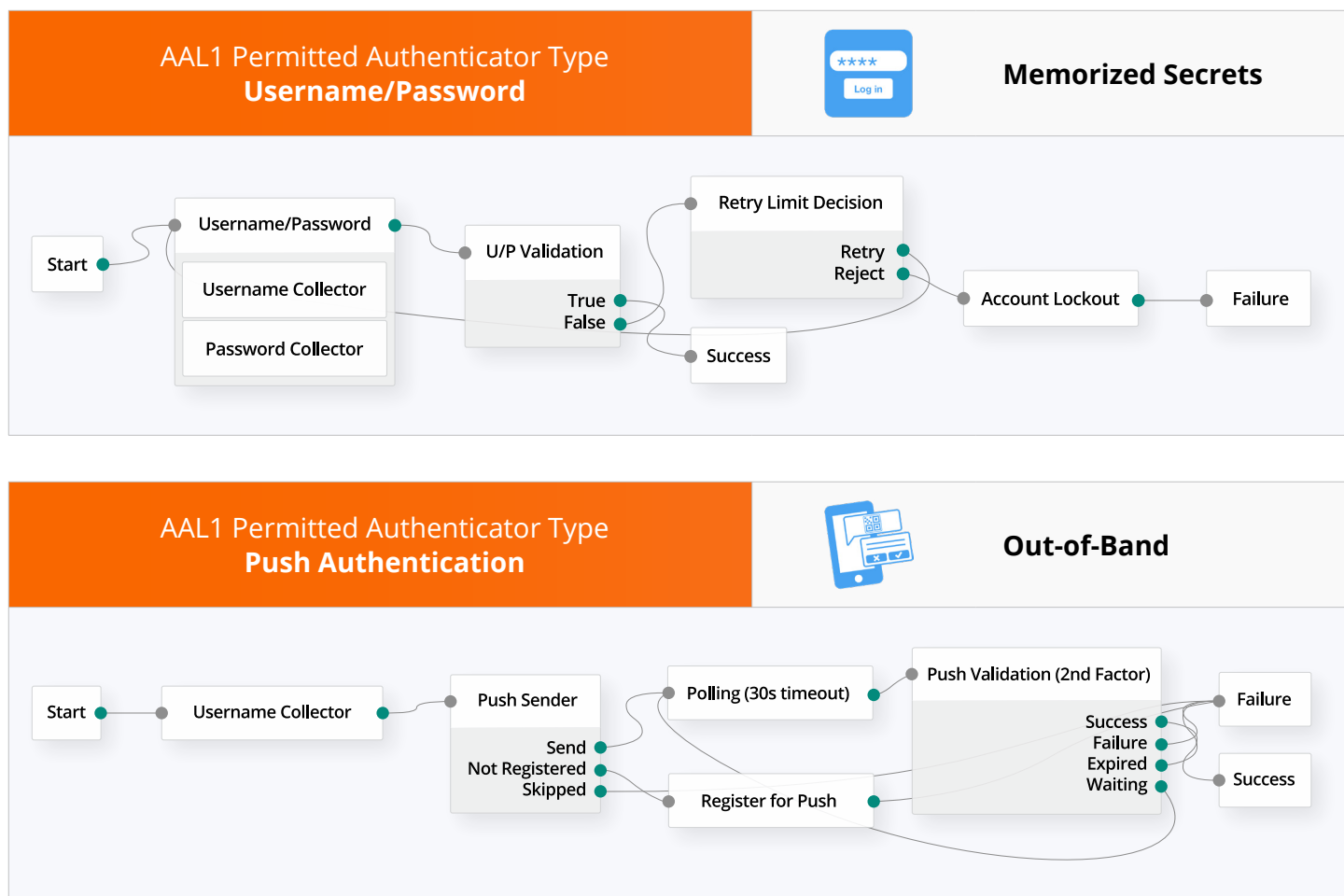
AAL3 Permitted Authenticator Types					
	Multi-Factor Cryptographic Devices			Single-Factor Cryptographic Devices	<div><div>+</div><div></div></div> Memorized Secrets
	Single-Factor OTP Device	<div><div>+</div><div></div></div>	Multi-Factor Cryptographic Devices	<div><div>/</div><div></div></div> Multi-Factor Cryptographic Software	
	Single-Factor OTP Device	<div><div>+</div><div></div></div>	Single-Factor Cryptographic Software	<div><div>+</div><div></div></div> Memorized Secrets	

Authenticator Assurance Level 1 – AAL1

AAL1 protects low-risk content and requires the subscriber to control either a single-factor or a multi-factor authenticator bound to his or her account. It also mandates the use of secure communication protocols. ForgeRock provides the flexibility to use any of the authenticator types required by AAL1.

AAL1 Compliance is achieved using any of the following authenticator types:					
	Memorized Secrets Password, PIN, KBA		Look-Up Secrets Printed or electronic list of OTPs or PINs or codes		Out-of-Band Devices Push authentication through mobile app
	Single-Factor OTP Devices H/TOTP generators, YubiKeys or Google Authenticator		Multi-Factor OTP Devices PIN or biometrically protected H/TOTP generators, YubiKeys		Single-Factor Cryptographic Software Software-based FIDO, U2F
	Single-Factor Cryptographic Devices YubiKey with FIDO, U2F		Multi-Factor Cryptographic Software WebAuthN		Multi-Factor Cryptographic Devices PIV or CAC

Examples of Achieving AAL1 Using ForgeRock Intelligent Access



Note: Each use case illustrated above demonstrates how to easily achieve the desired assurance level. Administrators can create more complex designs by dragging and dropping additional nodes into the tree and moving flowlines between nodes. Administrators might choose a more complex tree to reduce end-user friction or add additional journey characteristics or collection points. To learn more, see [Authentication Nodes and Trees](#) in the [ForgeRock product documentation](#).

Authenticator Assurance Level 2 – AAL2







AAL2 requires a high confidence that the subscriber controls the authenticators bound to his or her account. AAL2 requires proof of possession and control of two authentication factors, and communication must use approved cryptographic protocols.

AAL2 Compliance is achieved using any of the following authenticator types:

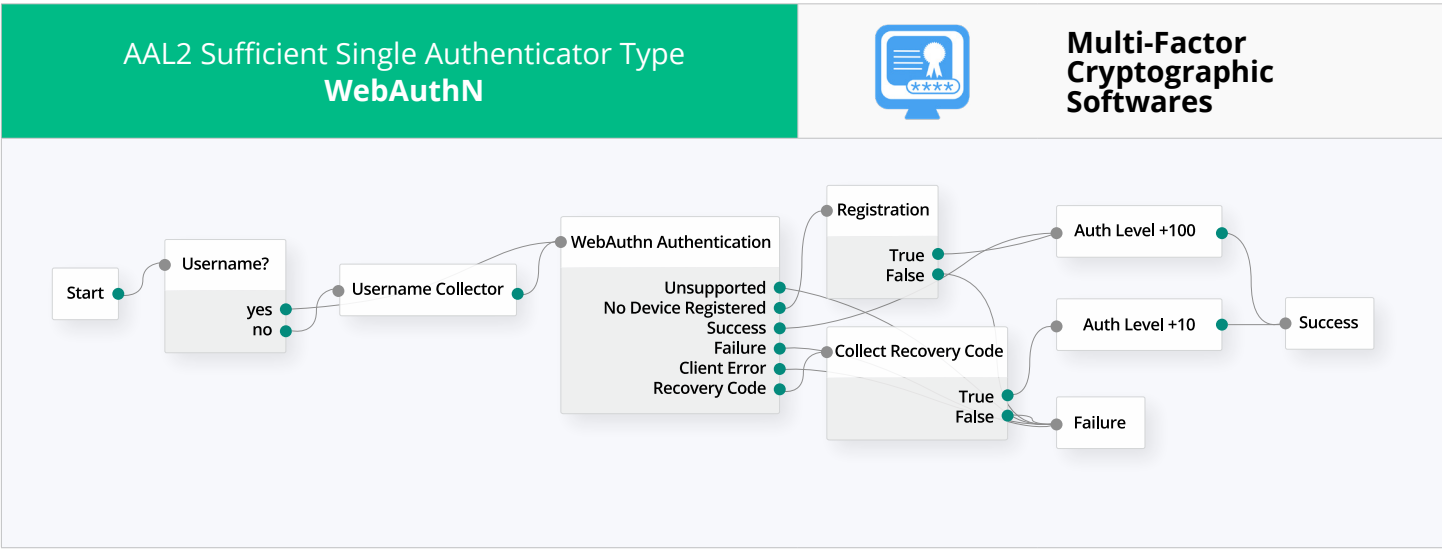
 <div>Multi-Factor OTP Devices PIN or biometrically protected H/TOTP generators, YubiKeys</div>	 <div>Multi-Factor Cryptographic Software WebAuthN</div>	 <div>Multi-Factor Cryptographic Devices PIV or CAC</div>
---	--	---

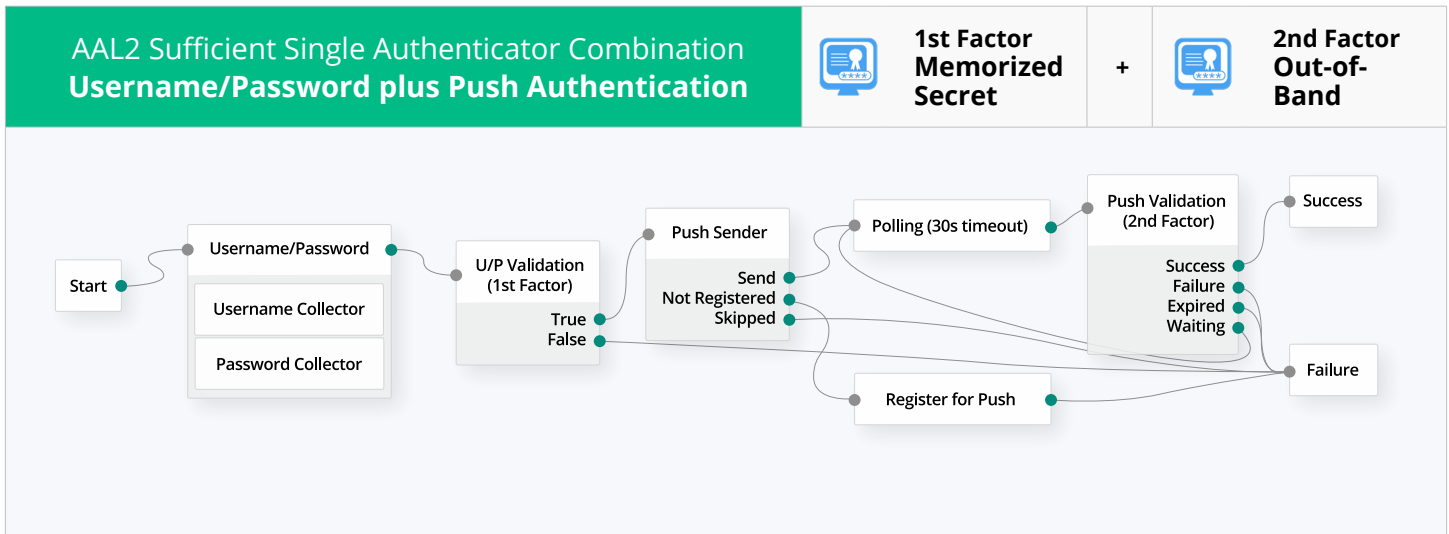
OR

AAL2 Permitted Authenticator Combinations - 1st factor + any of the 2nd factors

1st Factor	+ 2nd Factor
 <div>Memorized Secrets Password, PIN, KBA</div>	<div> Look-up Secret</div> <div> Out-of-Band</div> <div> SF OTP Device</div> <div> SF Crypto Software</div> <div> SF Crypto Device</div>

Examples of Achieving AAL2 Using ForgeRock Intelligent Access

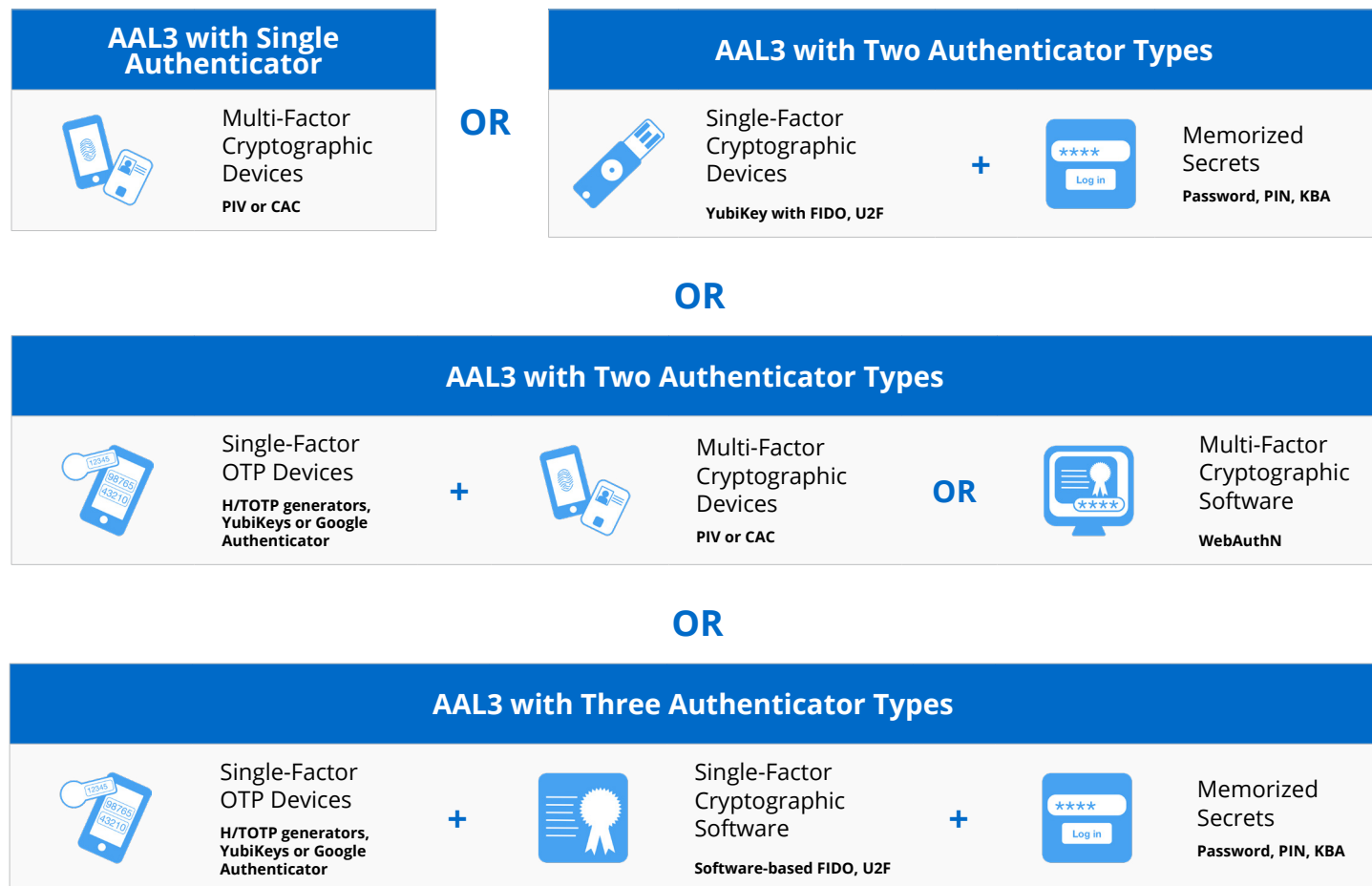




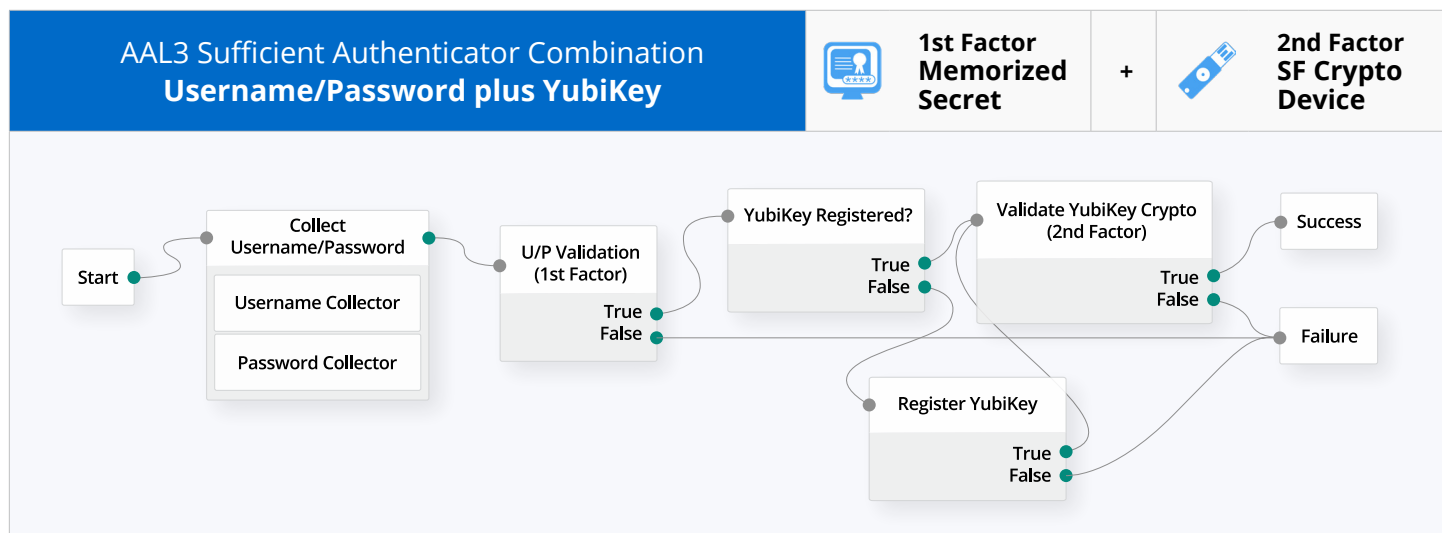
Note: Each use case illustrated above demonstrates how to easily achieve the desired assurance level. Administrators can create more complex designs by dragging and dropping additional nodes into the tree and moving flowlines between nodes. Administrators might choose a more complex tree to reduce end-user friction or add additional journey characteristics or collection points. To learn more, see [Authentication Nodes and Trees](#) in the [ForgeRock product documentation](#).

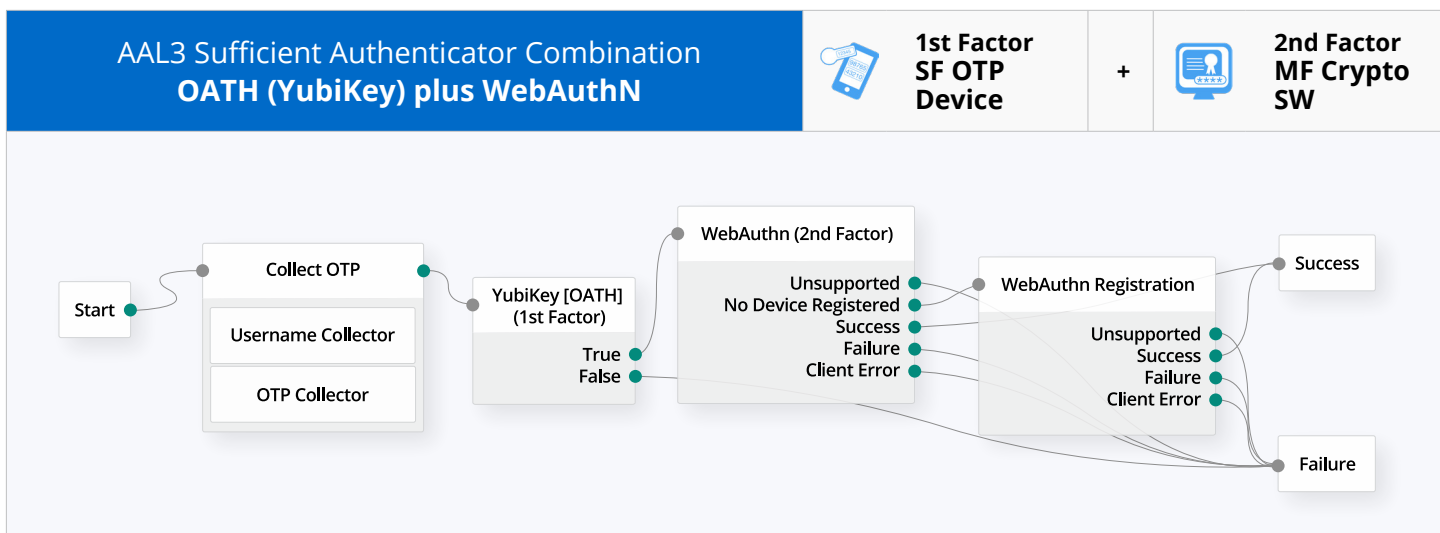
Authenticator Assurance Level 3 – AAL3

AAL3 requires a very high confidence that the subscriber controls the authenticators bound to his or her account. This includes proof of possession and control of a hardware-based authenticator as well as an impersonation-resistant authenticator. AAL3 requires two authentication factors and communication must be performed over approved cryptographic protocols.



Examples of Achieving AAL3 Using ForgeRock Intelligent Access





Note: Each use case illustrated above demonstrates how to easily achieve the desired assurance level. Administrators can create more complex designs by dragging and dropping additional nodes into the tree and moving flowlines between nodes. Administrators might choose a more complex tree to reduce end-user friction or add additional journey characteristics or collection points. To learn more, see [Authentication Nodes and Trees](#) in the [ForgeRock product documentation](#).

ForgeRock and NIST SP 800-63C

Federation and Assertions

NIST SP 800-63C provides requirements when using federated identity architectures and assertions to convey the results of authentication processes and relevant identity information to an agency application. In addition, this volume offers privacy-enhancing techniques to share information about a valid, authenticated subject and describes methods that allow for strong MFA while the subject remains pseudonymous to the digital service. SP 800-63C contains both normative and informative material.

The three FALs reflect the options agencies can select based on their risk profile and the potential harm caused by an attacker taking control of federated transactions.

FAL1: Allows for the subscriber to enable the resource provider to receive a bearer assertion cryptographically signed by the identity provider.

FAL2: Adds the requirement that the assertion be encrypted using approved cryptography such that the resource provider is the only party that can decrypt it.

FAL3: Requires the subscriber to present proof of possession of the assertion artifact and the cryptographic key referenced in the assertion. The assertion must also follow FAL1 and FAL2.

Federation is built into the ForgeRock Identity Platform. ForgeRock's [federation services](#) are based on open standards, such as SAML, OpenID Connect, OAuth 2.0, and UMA. These services provide value for both provider and consumer entities, to include: identity provider (IdP), service provider (SP), authorization server (AS), relying party (RP), and other types. FAL compliance is outlined in the table below.

FAL	Requirements	How ForgeRock Meets the Requirements		
		SAML 2.0 (WSFed)	OAuth 2.0	OIDC 1.0
1	Bearer assertion	IdP Web Browser SSO Profile, ST	AS, STS	AS, STS
	Signed by IdP	•	•	•
2	Bearer assertion	IdP Web Browser SSO Profile, ST	AS, STS	AS, STS
	Signed by IdP	•	•	•
	Encrypted to RP	•	•	•
3	Holder of key assertion	STS	AS - RFC 7800	AS - RFC 7800, STS
	Signed by IdP	•	•	•
	Encrypted to RP	•	•	•

Closing Thoughts

A solid and innovative security mindset is difficult to achieve, but ForgeRock and NIST share such a mindset. This mindset drives ForgeRock. It's why the ForgeRock Identity Platform is the most innovative and comprehensive ICAM and identity governance platform on the market. ForgeRock leads the ICAM market because we listen to our customers. We listen to the demands of the industry. We contribute to and lead top standards boards. We develop enduring trust relationships with other strong security companies. And, and we implement the best, most flexible product available. ForgeRock meets and exceeds the stringent, evolving needs government agencies require to accomplish their missions and achieve their objectives. Government agencies that use the ForgeRock Identity Platform find SP 800-63-3 compliance simple to achieve, easy to maintain, and fully future proof.

About ForgeRock

ForgeRock, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is privately held, and headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit www.forgerock.com or follow ForgeRock on social media.

Follow Us

