2 Introduction

This section is informative.

Digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known. Identity proofing establishes that a subject is who they claim to be. Digital authentication is the process of determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate. Successful authentication provides reasonable risk-based assurances that the subject accessing the service today is the same as that which previously accessed the service. Digital identity presents a technical challenge because this process often involves proofing individuals over an open network, and typically involves the authentication of individual subjects over an open network to access digital government services. There are multiple opportunities for impersonation and other attacks that fraudulently claim another subject's digital identity.

This recommendation provides agencies with technical guidelines for digital authentication of subjects to federal systems over a network. This recommendation also provides guidelines for credential service providers (CSPs), verifiers, and relying parties (RPs).

These guidelines describe the risk management processes for selecting appropriate digital identity services and the details for implementing identity assurance, authenticator assurance, and federation assurance levels based on risk. Risk assessment guidance in these guidelines supplements the *NIST Risk Management Framework* [NIST RMF] and its component special publications. This guideline does not establish additional risk management processes for agencies. Rather, requirements contained herein provide specific guidance related to digital identity risk while executing all relevant RMF lifecycle phases.

Digital authentication supports privacy protection by mitigating risks of unauthorized access to individuals' information. At the same time, because identity proofing, authentication, authorization, and federation involve the processing of individuals' information, these functions can also create privacy risks. These guidelines therefore include privacy requirements and considerations to help mitigate potential associated privacy risks.

These guidelines support the mitigation of the negative impacts induced by an authentication error by separating the individual elements of identity assurance into discrete, component parts. For non-federated systems, agencies will select two components, referred to as *Identity Assurance Level (IAL)* and *Authenticator Assurance Level (AAL)*. For federated systems, a third component, *Federation Assurance Level (FAL)*, is included. Section 5, Digital Identity Risk Management provides details on the risk assessment process. Section 6, Selecting Assurance Levels combines the results of the risk assessment with additional context to support agency selection of the appropriate IAL, AAL, and FAL combinations based on risk.

These guidelines do not consider nor result in a composite level of assurance (LOA) in the context of a single ordinal that drives implementation-specific requirements. Rather, by combining appropriate risk management for business, security, and privacy side-by-side with mission need, agencies will select IAL, AAL, and FAL as distinct options. Specifically, this document does not recognize the four LOA model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed. While many systems will have the same numerical level for each IAL, AAL, and FAL, this is not a requirement, and agencies should not assume they will be the same in any given system or application.

The components of identity assurance detailed in these guidelines are as follows:

- IAL refers to the identity proofing process.
- AAL refers to the authentication process.
- FAL refers to the assertion protocol used in a federated environment to communicate authentication and attribute information (if applicable) to an RP.

As such, SP 800-63 is organized as a suite of volumes as follows:

SP 800-63 *Digital Identity Guidelines*: Provides the risk assessment methodology and an overview of general identity frameworks, using authenticators, credentials, and assertions together in a digital system, and a risk-based process of selecting assurance levels. *SP 800-63 contains both normative and informative material.*

SP 800-63A *Enrollment and Identity Proofing*: Addresses how applicants can prove their identities and become enrolled as valid subjects within an identity system. It provides requirements for processes by which applicants can both proof and enroll at one of three different levels of risk mitigation in both remote and physically-present scenarios. *SP 800-63A contains both normative and informative material.*

SP 800-63B *Authentication and Lifecycle Management*: Addresses how an individual can securely authenticate to a CSP to access a digital service or set of digital services. This volume also describes the process of binding an authenticator to an identity. *SP 800-63B contains both normative and informative material.*

SP 800-63C *Federation and Assertions*: Provides requirements on the use of federated identity architectures and assertions to convey the results of authentication processes and relevant identity information to an agency application. Furthermore, this volume offers privacy-enhancing techniques to share information about a valid, authenticated subject, and describes methods that allow for strong multi-factor authentication (MFA) while the subject remains pseudonymous to the digital service. *SP 800-63C contains both normative and informative material.*

NIST anticipates that individual volumes in these guidelines will be revised asynchronously. At any time, the most recent revision of each should be used (e.g., if at a time in the future SP 800-63A-1 and SP 800-63B-2 are the most recent revisions of each volume, they should be used together even though the revision numbers do not match). To minimize the risk of compatibility

errors, a reference to the base document (i.e., SP 800-63 rather than SP 800-63-3) always refers to the current version of the document.

The following table states which sections of this volume are normative and which are informative:

Table 2-1 Normative and Informative Sections of SP 800-63-3

Section Name	Normative/Informative
1. Purpose	Informative
2. Introduction	Informative
3. Definitions and Abbreviations	Informative
4. Digital Identity Model	Informative
5. Digital Identity Risk Management	Normative
6. Selecting Assurance Levels	Normative
7. Federation Considerations	Informative
8. References	Informative

2.1 Applicability

Not all digital services require authentication or identity proofing; however, this guidance applies to all such transactions for which digital identity or authentication are required, regardless of the constituency (e.g. citizens, business partners, government entities).

Transactions not covered by this guidance include those associated with national security systems as defined in 44 U.S.C. § 3542(b)(2). Private sector organizations and state, local, and tribal governments whose digital processes require varying levels of assurance may consider the use of these standards where appropriate.

These guidelines primarily focus on agency services that interact with the non-federal workforce, such as citizens accessing benefits or private sector partners accessing information sharing collaboration spaces. However, it also applies to internal agency systems accessed by employees and contractors. These users are expected to hold a valid government-issued credential, primarily the Personal Identity Verification (PIV) card or a derived PIV. Therefore SP 800-63A and SP 800-63B are secondary to the requirements of FIPS 201 and its corresponding set of special publications and agency-specific instructions. However, SP 800-63C and the risk-based selection of an appropriate FAL applies, regardless of the credential type the internal user holds. FAL

selection provides agencies guidance and flexibility in how to PIV-enable their applications based on system risk.

2.2 Considerations, Other Requirements, and Flexibilities

Agencies may employ other risk mitigation measures and compensating controls not specified herein. Agencies need to ensure that any mitigations and compensating controls do not degrade the selected assurance level's intended security and privacy protections. Agencies may consider partitioning the functionality of a digital service to allow less sensitive functions to be available at a lower level of authentication and identity assurance.

Agencies may determine based on their risk analysis that additional measures are appropriate in certain contexts. In particular, privacy requirements and legal risks may lead agencies to determine that additional authentication measures or other process safeguards are appropriate. When developing digital authentication processes and systems, agencies should consult *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* [M-03-22]. See the *Use of Electronic Signatures in Federal Organization Transactions* [ESIG] for additional information on legal risks, especially those related to the need to 1) satisfy legal standards of proof and 2) prevent repudiation.

Additionally, federal agencies implementing these guidelines should adhere to their statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283 [FISMA], and related NIST standards and guidelines. FISMA directs federal agencies to develop, document, and implement agency-wide programs to provide security for the information and systems that support the agency's operations and assets. This includes the security authorization and accreditation (SA&A) of IT systems that support digital authentication. NIST recommends that non-federal entities implementing these guidelines follow equivalent standards to ensure the secure operations of their digital systems.

2.3 A Few Limitations

These technical guidelines do not address the authentication of subjects for physical access (e.g., to buildings), though some authenticators used for digital access may also be used for physical access authentication. Additionally, this revision of these guidelines does not explicitly address device identity, often referred to as machine-to-machine (such as router-to-router) authentication or interconnected devices, commonly referred to as the internet of things (IoT). That said, these guidelines are written to refer to generic subjects wherever possible to leave open the possibility for applicability to devices. Also excluded are specific requirements for issuing authenticators to devices when they are used in authentication protocols with people.

2.4 How to Use this Suite of SPs

The business model, marketplace, and composition of how identity services are delivered has drastically changed since the first version of SP 800-63 was released. Notably, CSPs can be componentized and comprised of multiple independently-operated and owned business entities. Furthermore, there may be a significant security benefit to using strong authenticators even if no

identity proofing is required. Therefore, in this revision, a suite of SPs under the 800-63 moniker has been created to facilitate these new models and make it easy to access the specific requirements for the function an entity may serve under the overall digital identity model.

2.5 Change History

2.5.1 SP 800-63-1

NIST SP 800-63-1 updated NIST SP 800-63 to reflect current authenticator (then referred to as "token") technologies and restructured it to provide a better understanding of the digital identity architectural model used here. Additional (minimum) technical requirements were specified for the CSP, protocols used to transport authentication information, and assertions if implemented within the digital identity model.

2.5.2 SP 800-63-2

NIST SP 800-63-2 was a limited update of SP 800-63-1 and substantive changes were made only in Section 5, *Registration and Issuance Processes*. The substantive changes in the revised draft were intended to facilitate the use of professional credentials in the identity proofing process, and to reduce the need to send postal mail to an address of record to issue credentials for level 3 remote registration. Other changes to Section 5 were minor explanations and clarifications.

2.5.3 SP 800-63-3

NIST SP 800-63-3 is a substantial update and restructuring of SP 800-63-2. SP 800-63-3 introduces individual components of digital authentication assurance — AAL, IAL, and FAL — to support the growing need for independent treatment of authentication strength and confidence in an individual's claimed identity (e.g., in strong pseudonymous authentication). A risk assessment methodology and its application to IAL, AAL, and FAL has been included in this guideline. It also moves the whole of digital identity guidance covered under SP 800-63 from a single document describing authentication to a suite of four documents (to separately address the individual components mentioned above) of which SP 800-63-3 is the top-level document.

Other areas updated in 800-63-3 include:

- Renamed to "Digital Identity Guidelines" to properly represent the scope includes identity proofing and federation, and to support expanding the scope to include device identity, or machine-to-machine authentication in future revisions.
- Terminology changes, including the use of authenticator in place of token to avoid conflicting use of the word token in assertion technologies.
- Updates to authentication and assertion requirements to reflect advances in both security technology and threats.
- Requirements on the storage of long-term secrets by verifiers.
- Restructured identity proofing model.
- Updated requirements regarding remote identity proofing.
- Clarification on the use of independent channels and devices as "something you have".

- **Removal** of pre-registered knowledge tokens (authenticators), with the recognition that they are special cases of (often very weak) passwords.
- Requirements regarding account recovery in the event of loss or theft of an authenticator.
- **Removal** of email as a valid channel for out-of-band authenticators.
- Expanded discussion of re-authentication and session management.
- Expanded discussion of identity federation; restructuring of assertions in the context of federation.

3 Definitions and Abbreviations

See Appendix A for a complete set of definitions and abbreviations.

4 Digital Identity Model

This section is informative.

4.1 Overview

The digital identity model used in these guidelines reflects technologies and architectures currently available in the market. More complex models that separate functions — such as issuing credentials and providing attributes — among a larger number of parties are also available and may have advantages in some application classes. While a simpler model is used in this document, it does not preclude agencies from separating these functions. Additionally, certain enrollment, identity proofing, and issuance processes performed by the CSP are sometimes delegated to an entity known as either the registration authority (RA) or identity manager (IM). A close relationship between the RA and CSP is typical, and the nature of this relationship may differ among RAs, IMs, and CSPs. The type of relationship and its requirements is outside of the scope of this document. Accordingly, the term CSP will be inclusive of RA and IM functions. Finally, a CSP may provide other services in addition to digital identity services. In these situations, the requirements specified throughout these guidelines only apply to the CSP function(s), not the additional services.

Digital identity is the unique representation of a subject engaged in an online transaction. The process used to verify a subject's association with their real-world identity is called *identity proofing*. In these guidelines, the party to be proofed is called an *applicant*. When the applicant successfully completes the proofing process, they are referred to as a *subscriber*.

The strength of identity proofing is described by an ordinal measurement called the IAL. At IAL1, identity proofing is not required, therefore any attribute information provided by the applicant is self-asserted, or should be treated as self-asserted and not verified (even if provided by a CSP to an RP). IAL2 and IAL3 require identity proofing, and the RP may request the CSP assert information about the subscriber, such as verified attribute values, verified attribute references, or pseudonymous identifiers. This information assists the RP in making authorization decisions. An RP may decide that it requires IAL2 or IAL3, but may only need specific attributes, resulting in the subject retaining some degree of pseudonymity. This privacy-enhancing approach is a benefit of separating the strength of the proofing process from that of the authentication process. An RP may also employ a federated identity approach where the RP outsources all identity proofing, attribute collection, and attribute storage to a CSP.

In these guidelines, the party to be authenticated is called a *claimant* and the party verifying that identity is called a *verifier*. When a claimant successfully demonstrates possession and control of one or more authenticators to a verifier through an authentication protocol, the verifier can verify that the claimant is a valid subscriber. The verifier passes on an assertion about the subscriber, who may be either pseudonymous or non-pseudonymous, to the RP. That assertion includes an identifier, and may include identity information about the subscriber, such as the name, or other attributes that were collected in the enrollment process (subject to the CSP's policies, the RP's

needs, and consent for disclosure of attributes given by the subject). Where the verifier is also the RP, the assertion may be implicit. The RP can use the authenticated information provided by the verifier to make authorization decisions.

Authentication establishes confidence that the claimant has possession of an authenticator(s) bound to the credential, and in some cases in the attribute values of the subscriber (e.g., if the subscriber is a U.S. citizen, is a student at a particular university, or is assigned a particular number or code by an agency or organization). Authentication does not determine the claimant's authorizations or access privileges; this is a separate decision, and is out of these guidelines' scope. RPs can use a subscriber's authenticated identity and attributes with other factors to make authorization decisions. Nothing in this document suite precludes RPs from requesting additional information from a subscriber that has successfully authenticated.

The strength of the authentication process is described by an ordinal measurement called the AAL. AAL1 requires single-factor authentication and is permitted with a variety of different authenticator types. At AAL2, authentication requires two authentication factors for additional security. Authentication at the highest level, AAL3, additionally requires the use of a hardware-based authenticator and verifier impersonation resistance.

The various entities and interactions that comprise the digital identity model used here are illustrated in Figure 4-1.

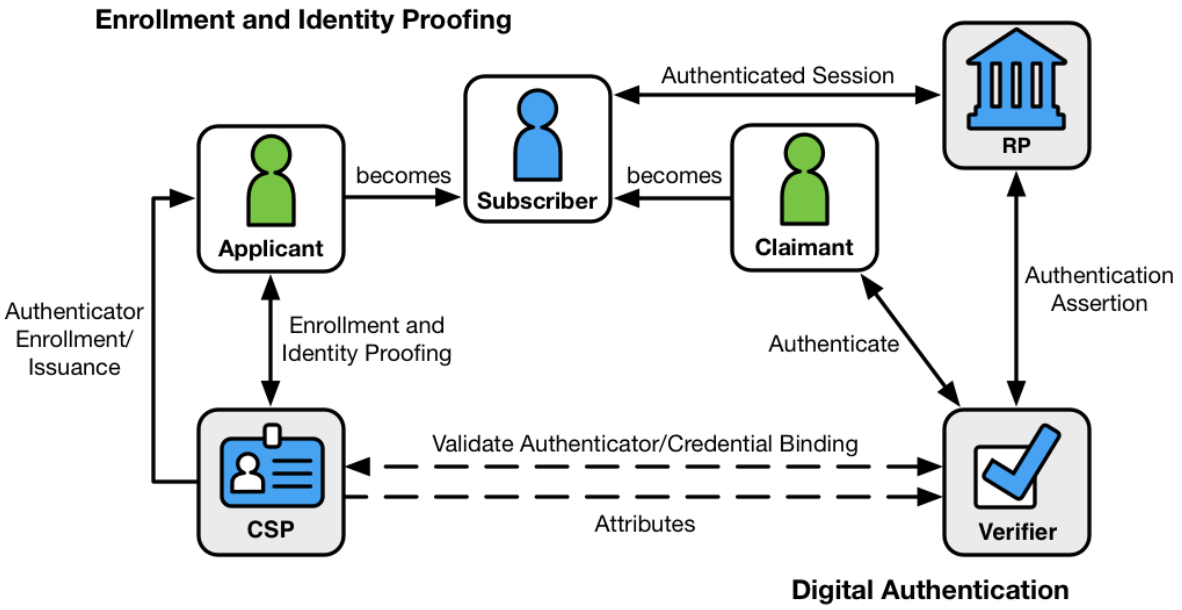


Figure 4-1 Digital Identity Model

The left side of the diagram shows the enrollment, credential issuance, lifecycle management activities, and various states of an identity proofing and authentication process. The usual sequence of interactions is as follows:

1. An applicant applies to a CSP through an enrollment process.
2. The CSP identity proofs that applicant. Upon successful proofing, the applicant becomes a subscriber.
3. Authenticator(s) and a corresponding credential are established between the CSP and the subscriber.
4. The CSP maintains the credential, its status, and the enrollment data collected for the lifetime of the credential (at a minimum). The subscriber maintains his or her authenticator(s).

Other sequences are less common, but could also achieve the same functional requirements.

The right side of Figure 4-1 shows the entities and interactions involved in using an authenticator to perform digital authentication. A subscriber is referred to as a claimant when he or she needs to authenticate to a verifier. The interactions are as follows:

1. The claimant proves possession and control of the authenticator(s) to the verifier through an authentication protocol.
2. The verifier interacts with the CSP to validate the credential that binds the subscriber's identity to their authenticator and to optionally obtain claimant attributes.
3. The CSP or verifier provides an assertion about the subscriber to the RP, which may use the information in the assertion to make an authorization decision.
4. An authenticated session is established between the subscriber and the RP.

In all cases, the RP should request the attributes it requires from a CSP before authenticating the claimant. In addition, the claimant should be requested to consent to the release of those attributes prior to generation and release of an assertion.

In some cases, the verifier does not need to communicate in real time with the CSP to complete the authentication activity (e.g., some uses of digital certificates). Therefore, the dashed line between the verifier and the CSP represents a logical link between the two entities. In some implementations, the verifier, RP, and CSP functions may be distributed and separated as shown in Figure 4-1. However, if these functions reside on the same platform, the interactions between the components are local messages between applications running on the same system rather than protocols over shared, untrusted networks.

As noted above, a CSP maintains status information about the credentials it issues. CSPs will generally assign a finite lifetime when issuing credentials to limit the maintenance period. When the status changes, or when the credentials near expiration, credentials may be renewed or re-issued; or, the credential may be revoked and destroyed. Typically, the subscriber authenticates to the CSP using their existing, unexpired authenticator and credential in order to request issuance of a new authenticator and credential. If the subscriber fails to request authenticator and credential re-issuance prior to their expiration or revocation, they may be required to repeat the enrollment process to obtain a new authenticator and credential. Alternatively, the CSP may choose to accept a request during a grace period after expiration.

4.2 Enrollment and Identity Proofing

Normative requirements can be found in SP 800-63A, *Enrollment and Identity Proofing*.

The previous section introduced the participants in the conceptual digital identity model. This section provides additional details regarding the participants' relationships and responsibilities in enrollment and identity proofing.

An individual, referred to as an *applicant* at this stage, opts to be identity proofed by a CSP. If the applicant is successfully proofed, the individual is then termed a subscriber of that CSP.

The CSP establishes a mechanism to uniquely identify each subscriber, register the subscriber's credentials, and track the authenticators issued to that subscriber. The subscriber may be given authenticators at the time of enrollment, the CSP may bind authenticators the subscriber already has, or they may be generated later as needed. Subscribers have a duty to maintain control of their authenticators and comply with CSP policies in order to maintain active authenticators. The CSP maintains enrollment records for each subscriber to allow recovery of authenticators, for example, when they are lost or stolen.

4.3 Authentication and Lifecycle Management

Normative requirements can be found in SP 800-63B, *Authentication and Lifecycle Management*.

4.3.1 Authenticators

The classic paradigm for authentication systems identifies three factors as the cornerstones of authentication:

- Something you know (e.g., a password).
- Something you have (e.g., an ID badge or a cryptographic key).
- Something you are (e.g., a fingerprint or other biometric data).

MFA refers to the use of more than one of the above factors. The strength of authentication systems is largely determined by the number of factors incorporated by the system — the more factors employed, the more robust the authentication system. For the purposes of these guidelines, using two factors is adequate to meet the highest security requirements. As discussed in Section 5.1, other types of information, such as location data or device identity, may be used by an RP or verifier to evaluate the risk in a claimed identity, but they are not considered authentication factors.

In digital authentication the claimant possesses and controls one or more authenticators that have been registered with the CSP and are used to prove the claimant's identity. The authenticator(s) contains secrets the claimant can use to prove that he or she is a valid subscriber, the claimant authenticates to a system or application over a network by proving that he or she has possession and control of one or more authenticators.

The secrets contained in authenticators are based on either public key pairs (asymmetric keys) or shared secrets (symmetric keys). A public key and a related private key comprise a public key pair. The private key is stored on the authenticator and is used by the claimant to prove possession and control of the authenticator. A verifier, knowing the claimant's public key through some credential (typically a public key certificate), can use an authentication protocol to verify the claimant's identity by proving that the claimant has possession and control of the associated private key authenticator.

Shared secrets stored on authenticators may be either symmetric keys or memorized secrets (e.g., passwords and PINs), as opposed to the asymmetric keys described above, which subscribers need not share with the verifier. While both keys and passwords can be used in similar protocols, one important difference between the two is how they relate to the subscriber. While symmetric keys are generally stored in hardware or software that the subscriber controls, passwords are intended to be memorized by the subscriber. Since most users choose short passwords to facilitate memorization and ease of entry, passwords typically have fewer characters than cryptographic keys. Furthermore, whereas systems choose keys at random, users attempting to choose memorable passwords will often select from a very small subset of the possible passwords of a given length, and many will choose very similar values. As such, whereas cryptographic keys are typically long enough to make network-based guessing attacks untenable, user-chosen passwords may be vulnerable, especially if no defenses are in place.

In this volume, authenticators always contain a secret. Some of the classic authentication factors do not apply directly to digital authentication. For example, a physical driver's license is something you have, and may be useful when authenticating to a human (e.g., a security guard), but is not in itself an authenticator for digital authentication. Authentication factors classified as something you know are not necessarily secrets, either. Knowledge-based authentication, where the claimant is prompted to answer questions that are presumably known only by the claimant, also does not constitute an acceptable secret for digital authentication. A biometric also does not constitute a secret. Accordingly, these guidelines only allow the use of biometrics for authentication when strongly bound to a physical authenticator.

A digital authentication system may incorporate multiple factors in one of two ways:

1. The system may be implemented so that multiple factors are presented to the verifier; or
2. Some factors may be used to protect a secret that will be presented to the verifier.

For example, item 1 can be satisfied by pairing a memorized secret (what you know) with an out-of-band device (what you have). Both authenticator outputs are presented to the verifier to authenticate the claimant. For item 2, consider a piece of hardware (the authenticator) that contains a cryptographic key (the authenticator secret) where access is protected with a fingerprint. When used with the biometric, the cryptographic key produces an output that is used to authenticate the claimant.

As noted above, biometrics, when employed as a single factor of authentication, do not constitute acceptable secrets for digital authentication — but they do have their place in the authentication of digital identities. Biometric characteristics are unique personal attributes that can be used to

verify the identity of a person who is physically present at the point of verification. They include facial features, fingerprints, iris patterns, voiceprints, and many other characteristics. SP 800-63A, *Enrollment and Identity Proofing* recommends that biometrics be collected in the enrollment process to later help prevent a registered subscriber from repudiating the enrollment, and to help identify those who commit enrollment fraud.

4.3.2 Credentials

As described in the preceding sections, a credential binds an authenticator to the subscriber, via an identifier, as part of the issuance process. A credential is stored and maintained by the CSP, though the claimant may possess it. The claimant possesses an authenticator, but is not necessarily in possession of the credential. For example, database entries containing the user attributes are considered to be credentials for the purpose of this document but are possessed by the verifier. X.509 public key certificates are a classic example of credentials the claimant can, and often does, possess.

4.3.3 Authentication Process

The authentication process begins with the claimant demonstrating to the verifier possession and control of an authenticator that is bound to the asserted identity through an authentication protocol. Once possession and control have been demonstrated, the verifier verifies that the credential remains valid, usually by interacting with the CSP.

The exact nature of the interaction between the verifier and the claimant during the authentication protocol is extremely important in determining the overall security of the system. Well-designed protocols can protect the integrity and confidentiality of communication between the claimant and the verifier both during and after the authentication, and can help limit the damage that can be done by an attacker masquerading as a legitimate verifier.

Additionally, mechanisms located at the verifier can mitigate online guessing attacks against lower entropy secrets — like passwords and PINs — by limiting the rate at which an attacker can make authentication attempts, or otherwise delaying incorrect attempts. Generally, this is done by keeping track of and limiting the number of unsuccessful attempts, since the premise of an online guessing attack is that most attempts will fail.

The verifier is a functional role, but is frequently implemented in combination with the CSP, the RP, or both. If the verifier is a separate entity from the CSP, it is often desirable to ensure that the verifier does not learn the subscriber's authenticator secret in the process of authentication, or at least to ensure that the verifier does not have unrestricted access to secrets stored by the CSP.

4.4 Federation and Assertions

Normative requirements can be found in SP 800-63C, *Federation and Assertions*.

Overall, SP 800-63 does not presuppose a federated identity architecture; rather, these guidelines are agnostic to the types of models that exist in the marketplace, allowing agencies to deploy a

digital authentication scheme according to their own requirements. However, identity federation is preferred over a number of siloed identity systems that each serve a single agency or RP.

Federated architectures have many significant benefits, including, but not limited to:

- Enhanced user experience. For example, an individual can be identity proofed once and reuse the issued credential at multiple RPs.
- Cost reduction to both the user (reduction in authenticators) and the agency (reduction in information technology infrastructure).
- Data minimization as agencies do not need to pay for collection, storage, disposal, and compliance activities related to storing personal information.
- Pseudonymous attribute assertions as agencies can request a minimized set of attributes, to include claims, to fulfill service delivery.
- Mission enablement as agencies can focus on mission, rather than the business of identity management.

The following sections discuss the components of a federated identity architecture should an agency elect this type of model.

4.4.1 Assertions

Upon completion of the authentication process, the verifier generates an assertion containing the result of the authentication and provides it to the RP. The assertion is used to communicate the result of the authentication process, and optionally information about the subscriber, from the verifier to the RP. Assertions may be communicated directly to the RP, or can be forwarded through the subscriber, which has further implications for system design.

An RP trusts an assertion based on the source, the time of creation, how long the assertion is valid from time of creation, and the corresponding trust framework that governs the policies and processes of CSPs and RPs. The verifier is responsible for providing a mechanism by which the integrity of the assertion can be confirmed.

The RP is responsible for authenticating the source (the verifier) and for confirming the integrity of the assertion. When the verifier passes the assertion through the subscriber, the verifier must protect the integrity of the assertion in such a way that it cannot be modified. However, if the verifier and the RP communicate directly, a protected session may be used to preserve the integrity of the assertion. When sending assertions across an open network, the verifier is responsible for ensuring that any sensitive subscriber information contained in the assertion can only be extracted by an RP that it trusts to maintain the information's confidentiality.

Examples of assertions include:

- Security Assertion Markup Language (SAML) assertions are specified using a mark-up language intended for describing security assertions. They can be used by a verifier to make a statement to an RP about the identity of a claimant. SAML assertions may optionally be digitally signed.

- OpenID Connect claims are specified using JavaScript Object Notation (JSON) for describing security, and optionally, user claims. JSON user info claims may optionally be digitally signed.
- Kerberos tickets allow a ticket-granting authority to issue session keys to two authenticated parties using symmetric key based encapsulation schemes.

4.4.2 Relying Parties

An RP relies on results of an authentication protocol to establish confidence in the identity or attributes of a subscriber for the purpose of conducting an online transaction. RPs may use a subscriber's authenticated identity (pseudonymous or non-pseudonymous), the IAL, AAL, and FAL (FAL indicating the strength of the assertion protocol), and other factors to make authorization decisions. The verifier and the RP may be the same entity, or they may be separate entities. If they are separate entities, the RP normally receives an assertion from the verifier. The RP ensures that the assertion came from a verifier trusted by the RP. The RP also processes any additional information in the assertion, such as personal attributes or expiration times. The RP is the final arbiter concerning whether a specific assertion presented by a verifier meets the RP's established criteria for system access regardless of IAL, AAL, or FAL.

5 Digital Identity Risk Management

This section is normative.

This section and the corresponding risk assessment guidance supplement the *NIST Risk Management Framework* [NIST RMF] and its component special publications. This does not establish additional risk management processes for agencies. Rather, requirements contained herein provide specific guidance related to digital identity risk that agency RPs SHALL apply while executing all relevant RMF lifecycle phases.

5.1 Overview

In today's digital services, combining proofing, authenticator, and federation requirements into a single bundle sometimes has unintended consequences and can put unnecessary implementation burden on the implementing organization. It is quite possible that an agency can deliver the most effective set of identity services by assessing the risk and impacts of failures for each individual component of digital authentication, rather than as a single, all-encompassing LOA. To this end, these guidelines recognize that an authentication error is not a singleton that drives all requirements.

This volume details requirements to assist agencies in avoiding:

1. Identity proofing errors (i.e., a false applicant claiming an identity that is not rightfully theirs);
2. Authentication errors (i.e., a false claimant using a credential that is not rightfully theirs); and
3. Federation errors (i.e., an identity assertion is compromised).

From the perspective of an identity proofing failure, there are two dimensions of potential failure:

1. The impact of providing a service to the wrong subject (e.g., an attacker successfully proofs as someone else).
2. The impact of excessive identity proofing (i.e., collecting and securely storing more information about a person than is required to successfully provide the digital service).

As such, agencies SHALL assess the risk of proofing, authentication, and federation errors separately to determine the required assurance level for each transaction.

Section 5.3 provides impact categories specific to digital identity to assist in the overall application of the RMF.

Risk assessments determine the extent to which risk must be mitigated by the identity proofing, authentication, and federation processes. These determinations drive the relevant choices of applicable technologies and mitigation strategies, rather than the desire for any given technology driving risk determinations. Once an agency has completed the overall risk assessment; selected

individual assurance levels for identity proofing, authentication, and federation (if applicable); and determined the processes and technologies they will employ to meet each assurance level, agencies SHALL develop a "Digital Identity Acceptance Statement", in accordance with SP 800-53 IA-1 a.1. See Section 5.5 for more detail on the necessary content of the Digital Identity Acceptance Statement.

5.2 Assurance Levels

An agency RP SHALL select, based on risk, the following individual assurance levels:

- IAL: The robustness of the identity proofing process to confidently determine the identity of an individual. IAL is selected to mitigate potential identity proofing errors.
- AAL: The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier. AAL is selected to mitigate potential authentication errors (i.e., a false claimant using a credential that is not rightfully theirs).
- FAL: The robustness of the assertion protocol the federation uses to communicate authentication and attribute information (if applicable) to an RP. FAL is optional as not all digital systems will leverage federated identity architectures. FAL is selected to mitigate potential federation errors (an identity assertion is compromised).

A summary of each of the identity, authenticator, and federation assurance levels is provided below.

Table 5-1 Identity Assurance Levels

Identity Assurance Level
IAL1: At IAL1, attributes, if any, are self-asserted or should be treated as self-asserted.
IAL2: At IAL2, either remote or in-person identity proofing is required. IAL2 requires identifying attributes to have been verified in person or remotely using, at a minimum, the procedures given in SP 800-63A.
IAL3: At IAL3, in-person identity proofing is required. Identifying attributes must be verified by an authorized CSP representative through examination of physical documentation as described in SP 800-63A.

Table 5-2 Authenticator Assurance Levels

Authenticator Assurance Level
AAL1: AAL1 provides some assurance that the claimant controls an authenticator registered to the subscriber. AAL1 requires single-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator(s) through a secure authentication protocol.
AAL2: AAL2 provides high confidence that the claimant controls authenticator(s) registered to the subscriber. Proof of possession and control of two different authentication factors is required through a secure authentication protocol. Approved cryptographic techniques are required at AAL2 and above.
AAL3: AAL3 provides very high confidence that the claimant controls authenticator(s) registered to the subscriber. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a "hard" cryptographic authenticator that provides verifier impersonation resistance.

Table 5-3 Federation Assurance Levels

Federation Assurance Level
FAL1: FAL1 permits the RP to receive a bearer assertion from an identity provider (IdP). The IdP must sign the assertion using approved cryptography.
FAL2: FAL2 adds the requirement that the assertion be encrypted using approved cryptography such that the RP is the only party that can decrypt it.
FAL3: FAL3 requires the subscriber to present proof of possession of a cryptographic key referenced in the assertion along with the assertion itself. The assertion must be signed using approved cryptography and encrypted to the RP using approved cryptography.

When described generically or bundled, these guidelines will refer to IAL, AAL, and FAL as ***xAL***.

5.3 Risk and Impacts

This section provides details on the impact categories used to determine IAL, AAL, and FAL.

Potential Impact Categories: To determine the appropriate level of assurance of the user's asserted identity, agencies SHALL assess the potential risks and identify measures to minimize their impact.

Authentication, proofing, and federation errors with potentially worse consequences require higher levels of assurance. Business process, policy, and technology may help reduce risk.

Categories of harm and impact include:

1. Inconvenience, distress, or damage to standing or reputation;
2. Financial loss or agency liability;
3. Harm to agency programs or public interests;
4. Unauthorized release of sensitive information;
5. Personal safety; and
6. Civil or criminal violations.

Required assurance levels for digital transactions are determined by assessing the potential impact of each of the above categories using the potential impact values described in Federal Information Processing Standard (FIPS) 199 [FIPS 199].

The three potential impact values are:

1. Low impact,
2. Moderate impact, and
3. High impact.

5.3.1 Business Process vs. Online Transaction

The assurance level determination is only based on transactions that are part of a digital system. An online transaction may not be equivalent to a complete business process that requires offline processing, or online processing in a completely segmented system. In selecting the appropriate assurance levels, the agency should assess the risk associated with online transactions they are offering via the digital service, not the entire business process associated with the provided benefit or service. For example, in an online survey, personal information may be collected, but it is never made available online to the submitter after the information is saved. In this instance, it is important for the information to be carefully protected in backend systems, but there is no reason to identity proof or even authenticate the user providing the information for the purposes of their own access to the system or its associated benefits. The online transaction is solely a submission of the data. The entire business process may require a significant amount of data validation, without ever needing to know if the correct person submitted the information. In this scenario, there is no need for any identity proofing nor authentication.

Another example where the assessed risk could differ if the agency evaluated the entire business process rather than the online transaction requirements is a digital service that accepts résumés to apply for open job postings. In this use case, the digital service allows an individual to submit – or at least does not restrict an individual from submitting – a résumé on behalf of anyone else, and in subsequent visits to the site, access the résumé for various purposes. Since the résumé information is available to the user in later sessions, and is likely to contain personal information, the agency must select an AAL that requires MFA, even though the user self-asserted the personal information. In this case, the requirements of [EO 13681] apply and the application

must provide at least AAL2. However, the identity proofing requirements remain unclear. The entire business process of examining a résumé and ultimately hiring and onboarding a person requires a significant amount of identity proofing. The agency needs a high level of confidence that the job applicant is in fact the subject of the résumé submitted online if a decision to hire is made. Yet this level of proofing is not required to submit the résumé online. Identity proofing is not required to complete the digital portion of the transaction successfully. Identity proofing the submitter would create more risk than required in the online system as excess personal information would be collected when no such information is needed for the portion of the hiring process served by the digital job application portal and may reduce usability. Therefore, the most appropriate IAL selection would be 1. There is no need to identity proof the user to successfully complete the online transaction. This decision for the online portal itself is independent of a seemingly obvious identity proofing requirement for the entire business process, lest a job be offered to a fraudulent applicant.

5.3.2 Impacts per Category

This section defines the potential impacts for each category of harm. Each assurance level, IAL, AAL, and FAL (if accepting or asserting a federated identity) SHALL be evaluated separately.

> Note: If an error in the identity system causes no measurable consequences for a category, there is no impact.

Potential impact of inconvenience, distress, or damage to standing or reputation:

- Low: at worst, limited, short-term inconvenience, distress, or embarrassment to any party.
- Moderate: at worst, serious short-term or limited long-term inconvenience, distress, or damage to the standing or reputation of any party.
- High: severe or serious long-term inconvenience, distress, or damage to the standing or reputation of any party. This is ordinarily reserved for situations with particularly severe effects or which potentially affect many individuals.

Potential impact of financial loss:

- Low: at worst, an insignificant or inconsequential financial loss to any party, or at worst, an insignificant or inconsequential agency liability.
- Moderate: at worst, a serious financial loss to any party, or a serious agency liability.
- High: severe or catastrophic financial loss to any party, or severe or catastrophic agency liability.

Potential impact of harm to agency programs or public interests:

- Low: at worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests.

- Moderate: at worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests.
- High: a severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.

Potential impact of unauthorized release of sensitive information:

- Low: at worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS 199.
- Moderate: at worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS 199.
- High: a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS 199.

Potential impact to personal safety:

- Low: at worst, minor injury not requiring medical treatment.
- Moderate: at worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.
- High: a risk of serious injury or death.

The potential impact of civil or criminal violations is:

- Low: at worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.
- Moderate: at worst, a risk of civil or criminal violations that may be subject to enforcement efforts.
- High: a risk of civil or criminal violations that are of special importance to enforcement programs.

5.4 Risk Acceptance and Compensating Controls

The SP 800-63 suite specifies baseline requirements for digital identity services based on assurance level. Agencies SHOULD implement identity services per the requirements in these guidelines and SHOULD consider additional techniques and technologies to further secure and privacy-enhance their services.

Agencies MAY determine alternatives to the NIST-recommended guidance, for the assessed *x*ALs, based on their mission, risk tolerance, existing business processes, special considerations for certain populations, availability of data that provides similar mitigations to those described in this suite, or due to other capabilities that are unique to the agency.

Agencies SHALL demonstrate comparability of any chosen alternative, to include any compensating controls, when the complete set of applicable SP 800-63 requirements is not implemented. For example, an agency may choose a National Information Assurance Partnership (NIAP) protection profile over FIPS, where the profile is equivalent to or stronger than the FIPS requirements. That said, agencies SHALL NOT alter the assessed *x*AL based on agency capabilities. Rather, the agency MAY adjust their implementation of solutions based on the agency's ability to mitigate risk via means not explicitly addressed by SP 800-63 requirements. The agency SHALL implement procedures to document both the justification for any departure from normative requirements and detail the compensating control(s) employed.

This guidance addresses only those risks associated with authentication and identity proofing errors. NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems [SP 800-30] recommends a general methodology for managing risk in federal systems.

5.5 Digital Identity Acceptance Statement

Agencies SHOULD include this information in existing artifacts required to achieve a SA&A.

The statement SHALL include, at a minimum:

1. Assessed *x*AL,
2. Implemented *x*AL,
3. Rationale, if implemented *x*AL differs from assessed *x*AL,
4. Comparability demonstration of compensating controls when the complete set of applicable 800-63 requirements are not implemented, and
5. If not accepting federated identities, rationale.

5.6 Migrating Identities

As these guidelines are revised, CSPs SHALL consider how changes in requirements affect their user population. In some instances, the user population will be unaffected, yet in others, the CSP will require users undergo a transitional activity. For example, CSPs may request users — upon initial logon since last revision — to supply additional proofing evidence to adhere to new IAL requirements. This SHALL be a risk-based decision, made in context of the CSP, any RPs that use the CSP, mission, and the population served. The following considerations serve only as a guide to agencies when considering the impacts of requirements changes:

1. If the RP is experiencing identity-related fraud, a migration may prove beneficial. If not, migration may not be an added value.

2. New, stronger, or user-friendly authentication options are added to individual AALs the CSP could issue new authenticators or allow users to register authenticators they already have.
3. Federation requirements may or may not have a user impact. For example, consent requirements or infrastructure requirements could necessitate an infrastructure or protocol upgrade.
4. Addition or removal of *x*ALs may not require a migration, but would trigger a new risk assessment to determine if a change is necessary for the RP.

The guidance does not prescribe that any migration needs to occur, only that it be considered as revisions are released. It is up to the CSP and RP, based on their risk tolerance and mission, to determine the best approach.

6 Selecting Assurance Levels

This section is normative.

The risk assessment results are the primary factor in selecting the most appropriate levels. This section details how to apply the results of the risk assessment with additional factors unrelated to risk to determine the most advantageous *x*AL selection.

First, compare the risk assessment impact profile to the impact profiles associated with each assurance level, as shown in Table 6-1 below. To determine the required assurance level, find the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment.

Table 6-1 Maximum Potential Impacts for Each Assurance Level

	Assurance Level		
Impact Categories	**1**	**2**	**3**
Inconvenience, distress or damage to standing or reputation	Low	Mod	High
Financial loss or agency liability	Low	Mod	High
Harm to agency programs or public interests	N/A	Low/Mod	High
Unauthorized release of sensitive information	N/A	Low/Mod	High
Personal Safety	N/A	Low	Mod/High
Civil or criminal violations	N/A	Low/Mod	High

In analyzing risks, the agency SHALL consider all of the expected direct and indirect results of an authentication failure, including the possibility that there will be more than one failure, or harms to more than one person or organization. The definitions of potential impacts contain some relative terms, like "serious" or "minor," whose meaning will depend on context. The agency SHOULD consider the context and the nature of the persons or entities affected to decide the relative significance of these harms. Over time, the meaning of these terms will become more definite as agencies gain practical experience with these issues. The analysis of harms to agency programs or other public interests depends strongly on the context; the agency SHOULD consider these issues with care.

It is possible that the assurance levels may differ across IAL, AAL, and FAL. For example, suppose an agency establishes a "health tracker" application in which users submit personal

information in the form of personal health information (PHI). In line with the terms of EO 13681 requiring "that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication," the agency is required to implement MFA at AAL2 or AAL3.

EO 13681 also requires agencies employ "an effective identity proofing process, as appropriate" when personal information is released. This does not mean that proofing at IAL2 or IAL3 (to match the required AAL) is necessary. In the above example, there may be no need for the agency system to know the actual identity of the user. In this case, an "effective proofing process" would be to not proof at all, therefore the agency would select IAL1. This allows the user of the health tracker system to be pseudonymous.

Despite the user being pseudonymous, the agency should still select AAL2 or AAL3 for authentication because a malicious actor could gain access to the user's PHI by compromising the account.

> Note: An agency can accept a higher assurance level than those required in the table above. For example, in a federated transaction, an agency can accept an IAL3 identity if their application is assessed at IAL2. The same holds true for authenticators: stronger authenticators can be used at RPs that have lower authenticator requirements. However, RPs will have to ensure that this only occurs in federated scenarios with appropriate privacy protections by the CSP such that only attributes that have been requested by the RP and authorized by the subscriber are provided to the RP and that excessive personal information does not leak from the credential or an assertion. See the privacy considerations in SP 800-63C for more details.

> Note: The upshot of potentially having a different IAL, AAL, and FAL within a single application stems from the fact that this document no longer supports the notion of an overall LOA — the "low watermark" approach to determining LOA no longer applies. An application with IAL1 and AAL2 should not be considered any less secure or privacy-enhancing than an application with IAL2 and AAL2. The only difference between these applications is the amount of proofing required, which may not impact the security and privacy of each application. That said, if an agency incorrectly determines the *x*AL, security and privacy could very well be impacted.

6.1 Selecting IAL

The IAL decision tree in Figure 6-1 combines the results from the risk assessment with additional considerations related to identity proofing services to allow agencies to select the most appropriate identity proofing requirements for their digital service offering.

The IAL selection does not mean the digital service provider will need to perform the proofing themselves. More information on whether an agency can federate is provided in Section 7.

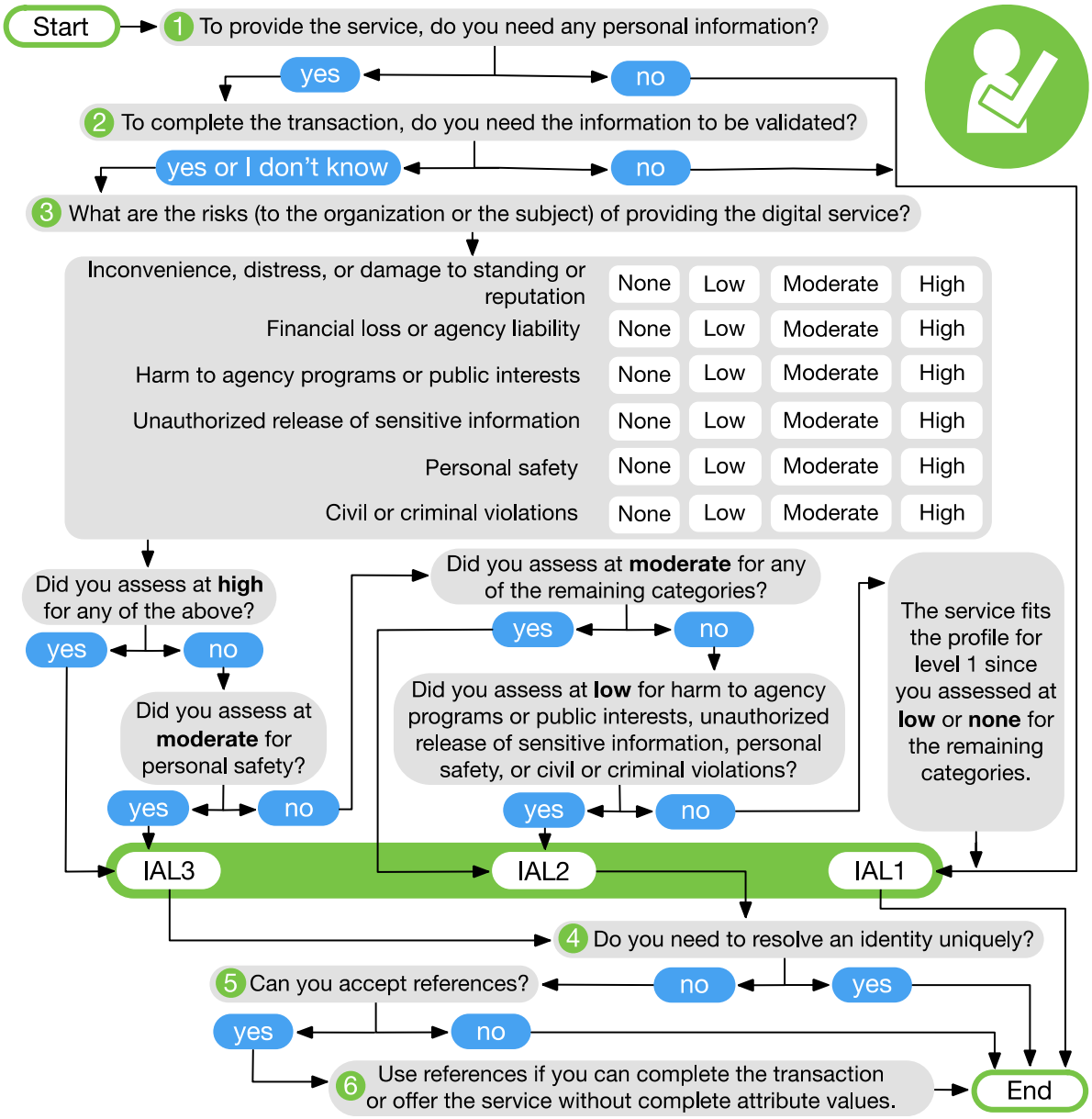
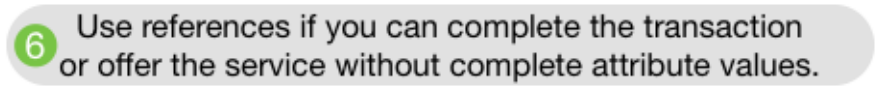


Figure 6-1 Selecting IAL

1 To provide the service, do you need any personal information?
The risk assessment and IAL selection can be short circuited by answering this question first. If the service does not require any personal information to execute any digital transactions, the system can operate at IAL1.
2 To complete the transaction, do you need the information to be validated? If personal information is needed, the RP needs to determine if validated and verified attributes are required, or if self-asserted attributes are acceptable. If even a single validated and verified attribute is needed, then the provider will need to accept attributes that have been IAL2 or IAL3 proofed. Again, the selection of IAL can be short circuited to IAL1 if the agency can deliver the digital service with self-asserted attributes only.
3 What are the risks (to the organization or the subject) of providing the digital service? At this point, the agency understands that some level of proofing is required. Step 3 is intended to look at the potential impacts of an identity proofing failure to determine if IAL2 or IAL3 is the most appropriate selection. The primary identity proofing failure an agency may encounter is accepting a falsified identity as true, therefore providing a service or benefit to the wrong or ineligible person. In addition, proofing, when not required, or collecting more information than needed is a risk in and of itself. Hence, obtaining verified attribute information when not needed is also considered an identity proofing failure. This step should identify if the agency answered Step 1 and 2 incorrectly, realizing they do not need personal information to deliver the service. Risk should be considered from the perspective of the organization and to the user, since one may not be negatively impacted while the other could be significantly harmed. Agency risk management processes should commence with this step.
4 Do you need to resolve an identity uniquely? Step 4 is intended to determine if the personal information required by the agency will ultimately resolve to a unique identity. In other words, the agency needs to know the full identity of the subject accessing the digital service, and pseudonymous access, even with a few validated and verified attributes, is not possible. If the agency needs to uniquely identify the subject, the process can end. However, the agency should consider if Step 5 is of value to them, as the acceptance of claims will reduce exposure to the risk of over collecting and storing more personal information than is necessary.

Step 5 focuses on whether the digital service can be provided without having access to full attribute values. This does not mean all attributes must be delivered as claims, but this step does ask the agency to look at each personal attribute they have deemed necessary, and identify which can suffice as claims and which need to be complete values. A federated environment is best suited for receiving claims, as the digital service provider is not in control of the attribute information to start with. If the application also performs all required identity proofing, claims may not make sense since full values are already under the digital service provider's control.



If the agency has reached Step 6, claims should be used. This step identifies the digital service as an excellent candidate for accepting federated attribute references from a CSP (or multiple CSPs), since it has been determined that complete attribute values are not needed to deliver the digital service.

> Note: Agencies should also consider their constituents' demographics when selecting the most appropriate proofing process. While not a function of IAL selection, certain proofing processes may be more appropriate for some demographics than others. Agencies will benefit as this type of analysis ensures the greatest opportunity for their constituents to be proofed successfully.

6.2 Selecting AAL

The AAL decision tree in Figure 6-2 combines the results from the risk assessment with additional considerations related to authentication to allow agencies to select the most appropriate authentication requirements for their digital service offering.

The AAL selection does not mean the digital service provider will need to issue authenticators themselves. More information on whether the agency can federate is provided in Section 7.

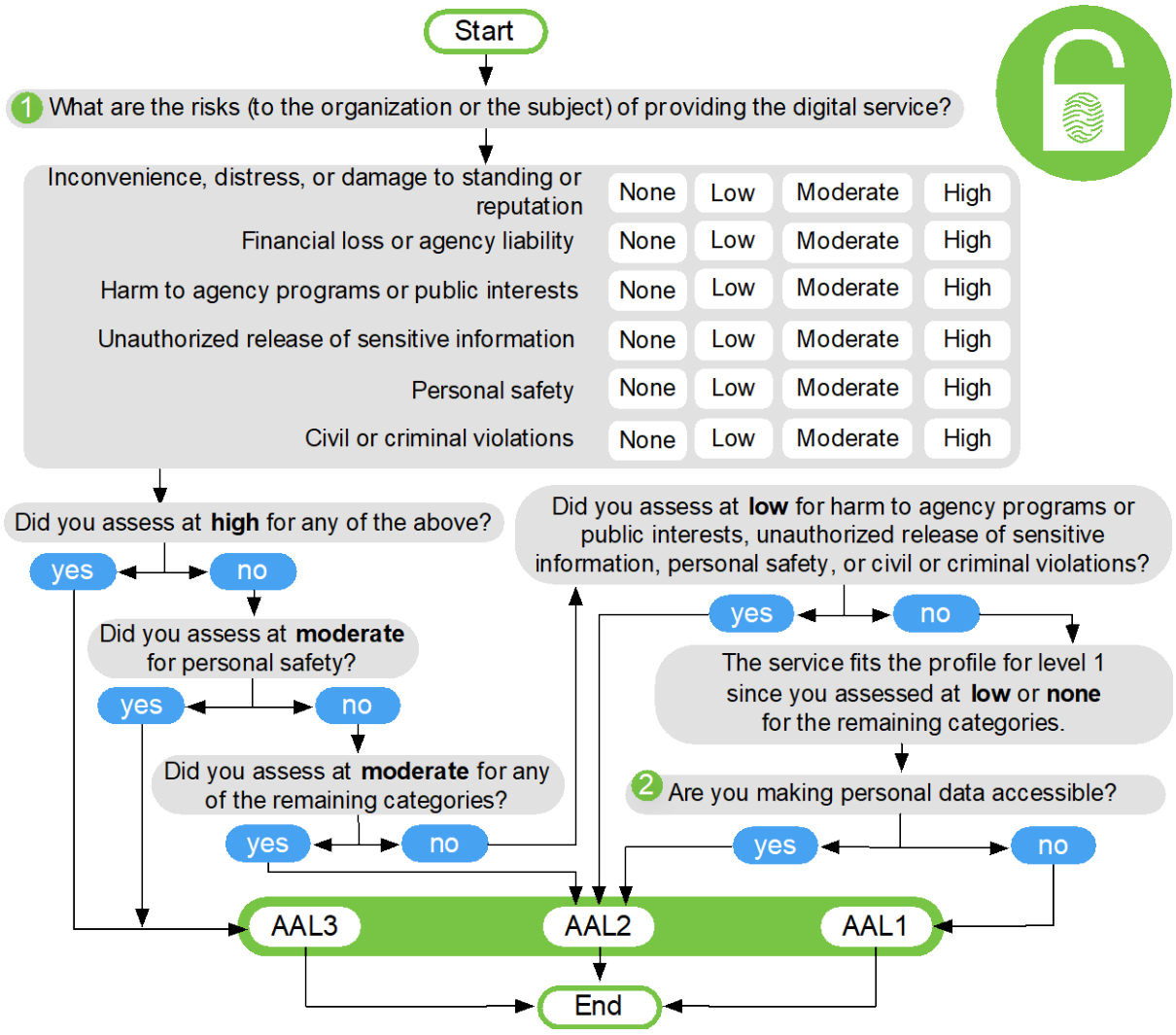


Figure 6-2 Selecting AAL

1 What are the risks (to the organization or the subject) of providing the digital service?

Step 1 asks agencies to look at the potential impacts of an authentication failure. In other words, what would occur if an unauthorized user accessed one or more valid user accounts? Risk should be considered from the perspective of the organization and to a valid user, since one may not be negatively impacted while the other could be significantly harmed. Agency risk management processes should commence with this step.

2 Are you making personal data accessible?

MFA is required when any personal information is made available online. Since the other paths in this decision tree already drive the agency to an AAL that requires MFA, the question of personal information is only raised at this point. That said, personal information release at all AALs should be considered when performing the risk assessment. An important point at this step is that the collection of personal information, if not made available online, does not need to be validated or verified to require an AAL of 2 or higher. Release of even self-asserted personal information requires account protection via MFA. Even though self-asserted information can be falsified, most users will provide accurate information to benefit from the digital service. As such, self-asserted data must be protected appropriately.

6.3 Selecting FAL

The FAL decision tree in Figure 6-3 combines the results from the risk assessment with additional considerations related to federation to allow agencies to select the most appropriate requirements for their digital service offering.

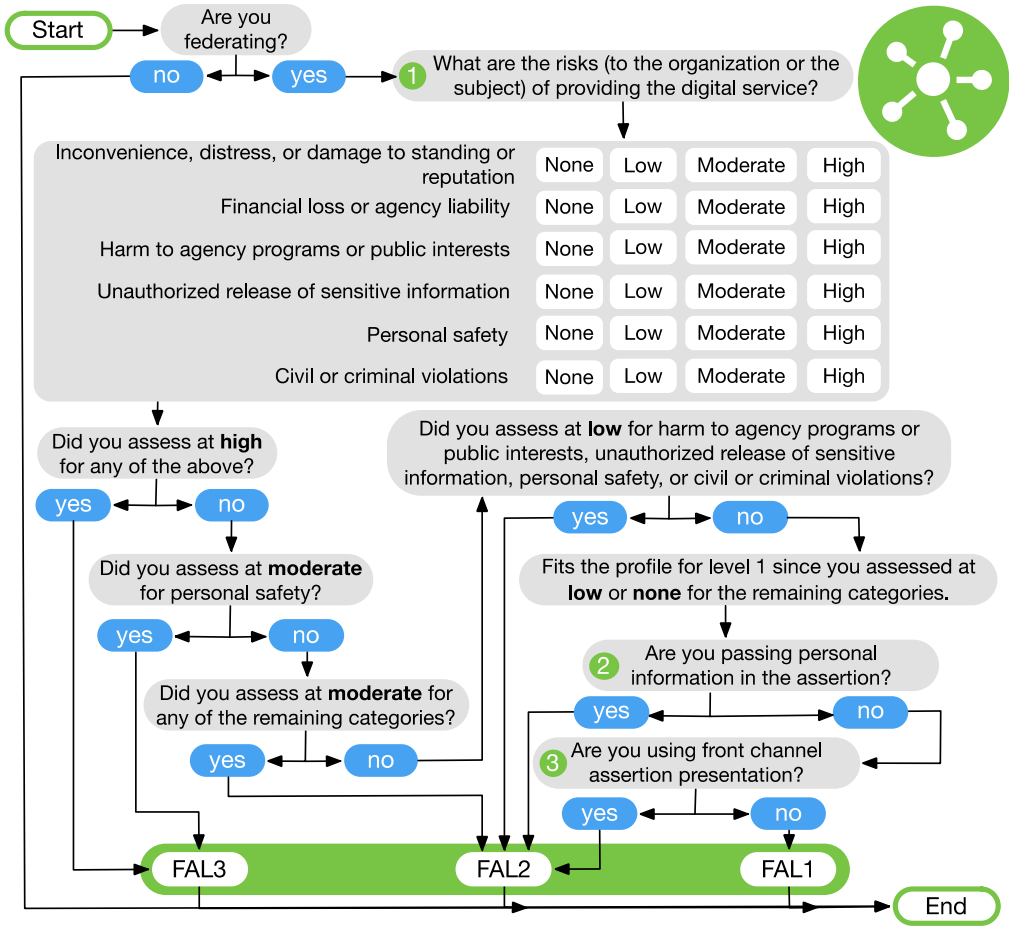
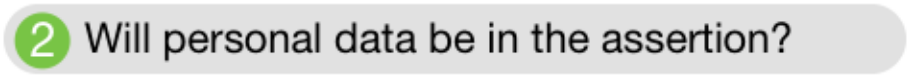


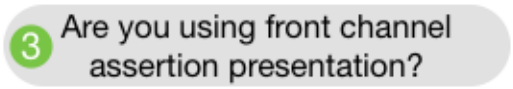
Figure 6-3 Selecting FAL

1 What are the risks (to the organization or the subject) of providing the digital service?

Step 1 asks agencies to look at the potential impacts of a federation failure. In other words, what would occur if an unauthorized user could compromise an assertion? Examples of compromise include use of assertion replay to impersonate a valid user or leakage of assertion information through the browser. Risk should be considered from the perspective of the organization and to the subscriber, since one may not be negatively impacted while the other could be significantly harmed. Agency risk management processes should commence with this step.



FAL2 is required when any personal information is passed in an assertion. Personal information release at all FALs should be considered when performing the risk assessment. FAL2 or higher is required when any personal information is contained in an assertion, as the audience and encryption requirements at FAL1 are not sufficient to protect personal information from being released. Release of even self-asserted personal information requires assertion protection via FAL2. Even though self-asserted information can be falsified, most users will provide accurate information to benefit from the digital service. However, when personal information is available to the RP via an authorized API call, such information need not be included in the assertion itself. Since the assertion no longer includes personal information, it need not be encrypted and this FAL requirement does not apply.



RPs should use a back-channel presentation mechanism as described in SP 800-63C, Section 7.1 where possible as such mechanisms allow for greater privacy and security. Since the subscriber handles only an assertion reference and not the assertion itself, there is less chance of leakage of attributes or other sensitive information found in the assertion to the subscriber's browser or other programs. As the RP directly presents the assertion reference to the IdP, the IdP can often take steps to identify and authenticate the RP during this step. Furthermore, as the RP fetches the assertion directly from the IdP over an authenticated protected channel, there are fewer opportunities for an attacker to inject an assertion into an RP.

All FALs require assertions to have a baseline of protections, including signatures, expirations, audience restrictions, and others enumerated in SP 800-63C. When taken together, these measures make it so that assertions cannot be created or modified by an unauthorized party, and that an RP will not accept an assertion created for a different system.

6.4 Combining *x*ALs

This guideline introduces a model where individual *x*ALs can be selected without requiring parity to each other. While options exist to select varying *x*ALs for a system, in many instances the same level will be chosen for all *x*ALs.

The ability to combine varying *x*ALs offers significant flexibility to agencies, but not all combinations are possible due to the nature of the data collected from an individual and the

authenticators to protect that data. Table 6-2 details valid combinations of IAL and AAL to ensure personal information remains protected by MFA.

Table 6-2 Acceptable Combinations of IAL and AAL

	AAL1	AAL2	AAL3
IAL1: Without personal data	Allowed	Allowed	Allowed
IAL1: With personal data	**NO**	Allowed	Allowed
IAL2	**NO**	Allowed	Allowed
IAL3	**NO**	Allowed	Allowed

> Note: Per Executive Order 13681 [EO 13681], the release of personal data requires protection with MFA, even if the personal data is self-asserted and not validated. When the transaction does not make personal data accessible, authentication may occur at AAL1, although providing an option for the user to choose stronger authentication is recommended. In addition, it may be possible at IAL1 to self-assert information that is not personal, in which case AAL1 is acceptable.

7 Federation Considerations

This section is informative.

This guideline and its companion volumes are agnostic to the authentication and identity proofing architecture an agency selects. However, there are scenarios an agency may encounter that make identity federation potentially more efficient and effective than establishing identity services local to the agency or individual applications. The following list details scenarios where, if any apply, the agency may consider federation a viable option. This list does not take into consideration any economic benefits or weaknesses of federation vs. localized identity architectures.

Federate authenticators when:

1. Potential users already have an authenticator at or above required AAL.
2. Multiple credential form factors are required to cover all possible user communities.
3. Agency does not have infrastructure to support authentication management (e.g., account recovery, authenticator issuance, help desk).
4. There is a desire to allow primary authenticators to be added and upgraded over time without changing the RP's implementation.
5. There are different environments to be supported, as federation protocols are network-based and allow for implementation on a wide variety of platforms and languages.
6. Potential users come from multiple communities, each with its own existing identity infrastructure.

Federate attributes when:

1. Pseudonymity is required, necessary, feasible, or important to stakeholders accessing the service.
2. Access to the service only requires a partial attribute list.
3. Access to the service only requires at least one attribute reference.
4. The agency is not the authoritative source or issuing source for required attributes.
5. Attributes are only required temporarily during use (such as to make an access decision), such that agency does not need to locally persist the data.