DRAFT NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

COMPUTER SECURITY

National Institute of
Standards and Technology
U.S. Department of Commerce

DRAFT NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
Applied Cybersecurity Division
Information Technology Laboratory

James L. Fenton
Altmode Networks
Los Altos, CA

March 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting Under Secretary of Commerce for Standards and Technology and Director

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-63-3
Natl. Inst. Stand. Technol. Spec. Publ. 800-63-3, xxx pages (March 2017)
CODEN: NSPUE2

> Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.
>
> There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.
>
> Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at http://csrc.nist.gov/publications (http://csrc.nist.gov/publications).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL’s responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal systems. The Special Publication 800-series reports on ITL’s research, guidelines, and outreach efforts in system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

These guidelines provide technical requirements for Federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols and related assertions. This publication supersedes NIST SP 800-63-1 and SP 800-63-2.

Keywords

authentication; authentication assurance; authenticator; assertions; credential service provider; digital authentication; digital credentials; identity proofing; passwords; PKI.

Acknowledgements

The authors gratefully acknowledge Kaitlin Boeckl for her artistic graphics contributions to all documents in the SP 800-63-3 suite.

In addition, the authors would like to acknowledge the thought leadership and innovation of the original authors: Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, and Emad A. Nabbus. Without their tireless efforts, we would not have had the incredible baseline from which to evolve 800-63 to the document it is today.

Audience

Compliance with NIST Standards and Guidelines

Conformance Testing

Note to Reviewers

Requirements Notation and Conventions

The terms “SHALL” and “SHALL NOT” indicate requirements to be followed strictly in order to conform to the publication and from which no deviation is permitted.

The terms “SHOULD” and “SHOULD NOT” indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.

The terms “MAY” and “NEED NOT” indicate a course of action permissible within the limits of the publication.

The terms “CAN” and “CANNOT” indicate a possibility and capability, whether material, physical or causal or, in the negative, the absence of that possibility or capability.

Executive Summary

Digital identity is the online persona of a subject, and a single definition is widely debated internationally. The term persona is apropos as a subject can represent themselves online in many ways. An individual may have a digital identity for email, and another one for personal finances. A personal laptop can be someone's streaming music server yet also be a worker-bot in a distributed network of computers performing complex genome calculations. Without context, it is difficult to land on a single definition that satisfies all. Digital identity as a legal identity further complicates the definition and ability to use digital identities across a range of social and economic use cases. Digital identity is hard. Proving someone is who they say they are, remotely, via a digital service, is fraught with vulnerabilities of impersonation. After proving yourself, repeatedly proving it is you logging in is just as complicated and vulnerable as the original claim and proof of identity. As correctly captured by Peter Steiner in The New Yorker, "On the internet, nobody knows you're a dog." These guidelines provide mitigations to the vulnerabilities inherent online, while recognizing and encouraging that when accessing some, low-risk digital services, 'being a dog' is just fine, while other high-risk services need a level of confidence that the digital identity accessing the service is the legitimate proxy to the real life subject.

For these guidelines, 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 other words, accessing a digital service may not mean that the physical representation of the underlying subject is known. Identity proofing establishes that a subject is actually who they claim to be. Digital authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators associated with that subject's digital identity. For services in which return visits are applicable, successfully authenticating provides reasonable risk-based assurances that the subject that is accessing the service today is the same as that which accessed the service yesterday. Digital identity presents a technical challenge because this process often involves the proofing of individuals over an open network, and always involves the authentication of individual subjects over an open network to access digital government services. The processes and technologies to establish and use digital identities offer multiple opportunities for impersonation and other attacks.

These technical guidelines supersede NIST Special Publication (SP) 800-63-1 and SP 800-63-2. Once the agency completes the digital identity risk assessment of its service(s), these guidelines provide mitigations 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.

These guidelines retire the concept of traditional LOA as a single ordinal that drives all implementation specific requirements. Rather, by combining appropriate business and privacy risk management side-by-side with mission need, agencies will select IAL, AAL, and FAL as distinct options; while many systems will have the same numerical level for each of IAL, AAL, and FAL, this not a requirement and agencies should not assume they will be the same in any given system.

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

- **IAL** refers to the identity proofing process and the binding between one or more authenticators and the records pertaining to a specific subscriber.
- **AAL** refers to the authentication process itself.
- **FAL** refers to the assertion protocol utilized in a federated environment to communicate authentication and attribute information (if applicable) to a relying party (RP).

The separation of these categories provides agencies flexibility in the identity solutions they choose and increases the ability to include privacy-enhancing techniques as fundamental elements of identity systems at any assurance level. For example, these guidelines support scenarios that will allow pseudonymous interactions even when strong, multi-factor authenticators are used. In addition, these guidelines encourage minimizing the dissemination of identifying information by requiring federated identity providers (IdPs) to support a range of options for querying data, such as asserting whether an individual is older than a certain age rather than querying the entire date of birth. While many agency use cases will require individuals to be fully identified, these guidelines encourage pseudonymous access to government digital services wherever possible.

In today's environment, an organization's identity solution need not be a monolith, where all functionality is provided by one system or vendor. The market for identity services is componentized, allowing organizations and agencies to employ standards-based, pluggable identity solutions based on mission need. As such, SP 800-63 has been split into a suite of documents that may be used independently or in an integrated fashion depending on the component service(s) an agency requires.

Each document has adopted verbs that are internationally recognized in standards organizations as normative and requirements-based. When used in a normative statement in this publication, they are CAPITALIZED for ease of identification. For example, the use of SHALL is used to denote a mandatory requirement, while the use of SHOULD refers to a technique, technology, or process that is recommended but not mandatory. For more details on the definitions of these terms see the Requirements Notation and Conventions at the beginning of each document.

These documents may inform, but does not restrict or constrain, the development or use of standards for application outside of the Federal government, such as e-commerce transactions.

These guidelines are organized as follows:

SP 800-63-3 Digital Identity Guidelines (This document)

SP 800-63-3 provides 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. *This document contains both normative and informative material.*

SP 800-63A Enrollment and Identity Proofing (https://pages.nist.gov/800-63-3/sp800-63a.html)

NIST SP 800-63-A addresses how applicants can prove their identities and become enrolled as valid subscribers within an identity system. It provides requirements by which applicants can both proof and enroll at one of three different levels of risk mitigation in both remote and physically-present scenarios. *This document contains both normative and informative material.*

SP 800-63A sets requirements to achieve a given IAL. The three IALs reflect the options agencies may select based on their risk profile and the potential harm caused by an attacker making a successful false claim of an identity. The IALs are as follows:

IAL1 - There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as self-asserted.

IAL2 - Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing. Attributes could be asserted by Credential Service Providers (CSPs) to RPs in support of pseudonymous identity with verified attributes.

IAL3 - Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP. As with IAL2, attributes could be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.

SP 800-63B Authentication and Lifecycle Management (https://pages.nist.gov/800-63-3/sp800-63b.html)

For services in which return visits are applicable, a successful authentication provides reasonable risk-based assurances that the subscriber that is accessing the service today is the same as that which accessed the service yesterday. The robustness of this confidence is described by a categorization known as the AAL. NIST SP 800-63B addresses how an individual can securely authenticate to a CSP to access a digital service or set of digital services. *This document contains both normative and informative material.*

The three AALs define the subsets of options agencies can select based on their risk profile and the potential harm caused by an attacker taking control of an authenticator and accessing agencies' systems. The AALs are as follows:

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 through a secure authentication protocol.

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 secure authentication protocol(s). 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.

SP 800-63C Federation and Assertions (https://pages.nist.gov/800-63-3/sp800-63c.html)

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 guideline offers privacy enhancing techniques to share information about a valid, authenticated subject, as well as describing methods that allow for strong multi-factor authentication (MFA) while the subject remains pseudonymous to the digital service. *This document 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. The FALs are as follows:

FAL1 - Allows for the subscriber to enable the RP to receive a bearer assertion. The assertion is signed by the IdP using approved cryptography.

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 - 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 IdP and encrypted to the RP using approved cryptography.

These guidelines are agnostic to the vast array of identity services architectures that agencies can develop or acquire, and are meant to be applicable regardless of the approach an agency selects. However, where possible federation is encouraged, and the ability to mix and match IAL, AAL, and FAL is simplified when federated architectures are used. In addition, federation is a keystone in the ability to enhance the privacy of agency constituents as they access valuable government digital services.

Table of Contents

1. Purpose

This section is informative.

This recommendation and its companion documents, Special Publication (SP) 800-63A, SP 800-63B, and SP 800-63C, provide technical guidelines to agencies for the implementation of digital authentication.

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 other words, accessing a digital service may not mean that the physical representation of the underlying subject is known. Identity proofing establishes that a subject is actually 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 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 that is accessing the service today is the same as that which accessed the service yesterday. Digital identity presents a technical challenge because this process often involves the proofing of 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 to fraudulently claim another subject's digital identity.

This recommendation provides technical guidelines to agencies to allow a subject to remotely authenticate to a federal system. This recommendation also provides guidelines for credential service providers (CSPs), verifiers, and relying parties (RPs).

This document suite describes the risk management processes for selecting appropriate digital identity services, as well as the details for implementing identity assurance, authenticator assurance, and federation assurance levels based on risk. Risk assessment guidance in this 800-63 suite supplements the NIST Risk Management Framework (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 for agency application while executing all relevant RMF lifecycle phases.

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 expect a composite level of assurance (LOA) in the context of a single ordinal that drives all 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, instead requiring agencies to individually select levels corresponding to each function being performed. While many systems will have the same numerical level for each of 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 and the binding between one or more authenticators and the records pertaining to a specific subscriber.
- **AAL** refers to the authentication process itself.
- **FAL** refers to the assertion protocol utilized 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 documents as follows:

- SP 800-63-3 *Digital Identity Guidelines* - Provides the risk assessment methodology as well as 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. *This document 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. *This document 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 document 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. In addition, this guideline offers privacy enhancing techniques to share information about a valid, authenticated subject, as well as describing methods that allow for strong multi-factor authentication (MFA) while the subject remains pseudonymous to the digital service. *This document contains both normative and informative material.*

NIST anticipates that individual documents in this suite will be revised asynchronously with each other and with this document. At any given 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 document, they should be used together even though the revision numbers do not match).

2.1. Applicability

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

Transactions not covered by this guidance include those that are 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, for example citizens accessing benefits or private sector partners accessing information sharing collaboration spaces. However, it also applies to internal agency systems that are accessed by employees and contractors. These users are expected to hold a valid government issued credential, primarily the PIV card or a derived PIV, therefore 800-63A and 800-83B are secondary to the requirements of FIPS 201 and its corresponding set of special publications and agency specific instructions. However, 800-63C and the risk-based selection of an appropriate FAL does apply regardless of the credential type the internal user holds. FAL selection provides agencies guidance and flexibility in how the PIV-enable their applications based on system risk.

2.2. Considerations, Other Requirements, and Flexibilities

Within a given LOA, 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 intended security and privacy of the selected assurance levels. 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, while more sensitive functions are available only at a higher LOA.

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 that are related to the need to satisfy legal standards of proof and prevent repudiation.

Additionally, Federal agencies implementing these guidelines should adhere to the requirements of Title III of the E-Government Act, entitled the *Federal Information Security Management Act* [FISMA], and related NIST standards and guidelines. FISMA directs Federal agencies to develop, document, and implement agency-wide programs to provide information security for the information and systems that support the operations and assets of the agency. This includes the security authorization of IT systems that support digital authentication. It is recommended that non-Federal entities implementing these guidelines follow equivalent standards of security management, certification and accreditation to ensure the secure operations of their digital systems.

2.3. A Few Limitations

These technical guidelines do not address the authentication of a person who is physically present, for example, for access to buildings, even though some authenticators that are used remotely may also be used for local authentication. In addition, these guidelines do not yet specifically address machine-to-machine (such as router-to-router) authentication or specific guidance for authentication and authorization of interconnected devices, commonly referred to as the “internet of things (IoT)”. Also excluded are specific requirements for issuing authenticators to devices when they are used in authentication protocols with people.

This document suite focuses on authenticators that are difficult to forge because they contain some type of secret information that is not available to unauthorized parties and that is preferably not used in unrelated contexts. Biometric authentication uses human characteristics that, in some cases, may be available to an attacker. Accordingly, the use of biometrics for authentication is limited to activation of a specific physical authenticator to which it is strongly bound, and the number of consecutive activation failures is limited, beyond which another activation factor or authenticator is required. This document suite also supports the use of biometrics to prevent repudiation of registration, and to verify that the same individual participates in all phases of the registration process.

2.4. How to Use this Suite of SPs

The business model, marketplace, and the composition of the way identity services are delivered has drastically changed since the first version of SP 800-63 was released. Notably, CSPs can be componentized and composed of multiple independently operated and owned business entities. In addition, there may be a significant security benefit to the use of strong authenticators even if no identity proofing is required. Therefore, 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 authentication model. Each document stands alone. However, it is expected that all CSPs, even componentized, will be required to meet the requirements in [SP 800-63A] (sp800-63a.html) and [SP 800-63B] (sp800-63b.html). If the CSP also participates in an identity federation, which is generally preferred over use of an RP acting as its own CSP, meeting the requirements of [SP 800-63C] (sp800-63c.html) also applies.

2.5. Relationship to Other Standards and Guidelines

This document has been written to satisfy the needs of federal agencies. However, with the expansion of citizen services throughout the world that require identity and authentication assurance, as well as an increasing number of use cases that promote international identity federation and interoperability, these guidelines are intended to achieve alignment to national and international standards that describe levels of identity assurance. Table 2-1 provides a representative snapshot of mappings to various international and national assurance documents. This is not meant to imply that there is direct correlation between the IALs and AALs in this document and the levels in those standards, but that it is seen that this document fulfills the criteria as demonstrated in those standards.

Table 2-1. 800-63 Informative Mapping to Other Standards and Guidelines

SP 800-63	[eIDAS]	[GPG 45]	[RSDOPS]	[STORK 2.0]	[ISO 29115]	[ISO 29003]	[Canada]
N/A	N/A	N/A	Level 01	N/A	N/A	N/A	N/A
AAL/IAL1	Low	Level 1	Level 1	QAA Level 1	LoA 1	LoA 1	IAL/CAL 1
N/A	N/A	Level 2	Level 2	QAA Level 2	LoA 2	LoA 2	IAL/CAL 2
AAL/IAL2	Substantial	Level 3	Level 3	QAA Level 3	LoA 3	LoA 3	IAL/CAL 3
AAL/IAL3	High	Level 4	N/A2	QAA Level 4	LoA 4	LoA 4	IAL/CAL 4

2.6. Change History

2.6.1. 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 to provide a better understanding of the digital authentication architectural model used here. Additional (minimum) technical requirements were specified for the CSP, protocols utilized to transport authentication information, and assertions if implemented within the digital authentication model. Other changes to NIST SP 800-63 included:

- Recognition of more types of tokens, including pre-registered knowledge token, look-up secret token, out-of-band token, as well as some terminology changes for more conventional token types;
- Detailed requirements for assertion protocols and Kerberos;
- A new section on token and credential management;
- Simplification of guidelines for password entropy and throttling;
- Emphasis that the document is aimed at Federal IT systems;
- Recognition of different models, including a broader digital authentication model (in contrast to the simpler model common among Federal IT systems shown in Figure 1) and an additional assertion model, the Proxy Model, presented in Figure 6;
- Clarification of differences between Levels 3 and 4 in Table 12; and
- New guidelines that permit leveraging existing credentials to issue derived credentials.

The subsequent sections of NIST SP 800-63-1 presented a series of recommendations for the secure implementation of RAs, CSPs, Verifiers, and RPs. It should be noted that secure implementation of any one of these can only provide the desired LOA if the others are also implemented securely. Therefore, the following assumptions were made in NIST SP 800-63-1:

- RAs, CSPs, and Verifiers are trusted entities. Agencies implementing any of the above trusted entities have some assurance that all other trusted entities with which the agency interacts are also implemented appropriately for the desired security level.
- The RP is not considered a trusted entity. However, in some authentication systems the Verifier maintains a relationship with the RP to facilitate secure communications and may employ security controls which only attain their full value when the RP acts responsibly. The subscriber also trusts the RP to properly perform the requested service and to follow all relevant privacy policy.
- It is assumed that there exists a process of certification through which agencies can obtain the above assurance for trusted entities which they do not implement themselves.
- A trusted entity is considered to be implemented appropriately if it complies with the recommendations in this document and does not behave maliciously.
- While it is generally assumed that trusted entities will not behave maliciously, this document does contain some recommendations to reduce and isolate any damage done by a malicious or negligent trusted entity.

2.6.2. 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 use 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.

2.6.3. SP 800-63-3

NIST SP 800-63-3 is a substantial update and restructuring of SP 800-63-2. 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 individuals claimed identity (for example, 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 800-63 from a single document describing authentication to a suite of four documents, of which SP 800-63-3 is the top-level document.

Other areas of update to SP 800-63-2 include:

- Renamed to “Digital Identity Guidelines” to properly represent the scope to include identity proofing and federation, as well as support expansion of scope to device identity, or machine-to-machine authentication, in future revisions.
- Terminology changes, primarily 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.
- Expanded discussion of reauthentication and session management.
- Expanded discussion of identity federation; restructuring of assertions in the context of federation.

3. Definitions and Abbreviations

This section is informative.

A wide variety of terms are used in the area of digital identity. While the definitions of many terms are consistent with the earlier versions of SP 800-63, some have changed in this revision. Since there is no single, consistent definition for many of these terms, careful attention to how the terms are defined here is warranted.

The definitions in this section are primarily those that are referenced in this document. Refer to the other documents in the SP 800-63 document suite for additional definitions and abbreviations specific to their content.

Address of Record

The validated and verified location (physical or digital) where an individual can receive communications using approved mechanisms.

Applicant

A subject undergoing the processes of registration and identity proofing.

Assertion

A statement from a verifier to an RP that contains identity information about a subscriber. Assertions may also contain verified attributes.

Assurance

The degree of confidence in the vetting process used to establish the identity of a claimant to whom a credential was, or credentials were, issued, and the degree of confidence that the claimant who uses the credential is the same as the subscriber to whom the credential was issued.

Asymmetric Keys

Two related keys, consisting of a public key and a private key, that are used to perform complementary operations such as encryption and decryption or signature verification and generation.

Attack

An attempt by an unauthorized entity to fool a verifier or an RP into believing that the unauthorized individual in question is the subscriber.

Attacker

A party who acts with malicious intent to compromise a system.

Attribute

A quality or characteristic ascribed to someone or something.

Authentication

Process of determining the validity of one or more credentials used to claim a digital identity.

Authentication Protocol

A defined sequence of messages between a claimant and a verifier that demonstrates that the claimant has possession and control of one or more valid authenticators to establish their identity, and, optionally, demonstrates that the claimant is communicating with the intended verifier.

Authenticator

Something that the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. In previous editions of SP 800-63, this was referred to as a *token*.

Authenticator Assurance Level (AAL)

A category describing the authentication process proving that the claimant is in control of a given subscriber's authenticator(s).

Authenticator Secret

The secret value contained within an authenticator.

Authenticity

The property that data originated from their purported source.

Biometrics

Automated recognition of individuals based on their behavioral and biological characteristics.

In this document, biometrics may be used to unlock authenticators and prevent repudiation of registration.

Claimant

A subject whose identity is to be verified using one or more authentication protocols.

Claimed Identity

A declaration of unvalidated and unverified personal attributes by the applicant.

Credential

An object or data structure that authoritatively binds an identity, via an identifier or identifiers, and, optionally, additional attributes, to at least one authenticator possessed and controlled by a subscriber.

While common usage often assumes that the credential is maintained by the subscriber, this document also uses the term to refer to electronic records maintained by the CSP which establish a binding between the subscriber's authenticator(s) and identity.

Credential Service Provider (CSP)

A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. The CSP may encompass Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.

Cryptographic Key

A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, key requirements shall meet the minimum requirements stated in Table 2 of NIST SP 800-57 Part 1.

See also Asymmetric Keys, Symmetric Key.

Cryptographic Authenticator

An authenticator where the secret is a cryptographic key.

Digital Authentication

The process of establishing confidence in user identities presented digitally to a system. In previous editions of SP 800-63, this was referred to as *Electronic Authentication*.

Digital Signature

An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation but not confidentiality protection.

Electronic Authentication (E-Authentication)

See *Digital Authentication*.

Federal Information Security Management Act (FISMA)

Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Federal Information Processing Standard (FIPS)

Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions. See background information for more details.

FIPS documents are available online through the FIPS home page: http://www.nist.gov/itl/fips.cfm (http://www.nist.gov/itl/fips.cfm)

Federation

A process that allows for the conveyance of identity and authentication information across a set of networked systems.

Federation Assurance Level

A category describing the assertion protocol utilized by the federation to communicate authentication and attribute information (if applicable) to an RP.

Identity

An attribute or set of attributes that uniquely describe a subject within a given context.

Identity Assurance Level (IAL)

A category that conveys the degree of confidence that the applicant’s claimed identity is their real identity.

Identity Proofing

The process by which a CSP and an RA collect and verify information about a person for the purpose of issuing credentials to that person.

Identity Provider (IdP)

The party that manages the subscriber’s primary authentication credentials and issues assertions derived from those credentials. This is commonly the CSP as discussed within this document suite.

Memorized Secret

A type of authenticator consisting of a character string that is intended to be memorized or memorable by the subscriber, permitting the subscriber to demonstrate *something they know* as part of an authentication process.

Multi-Factor

A characteristic of an authentication system or an authenticator that requires more than one authentication factor for successful authentication. MFA can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors.

The three authentication factors are something you know, something you have, and something you are.

Network

An open communications medium, typically the Internet, that is used to transport messages between the claimant and other parties. Unless otherwise stated, no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking) and passive (e.g., eavesdropping) attack at any point between the parties (e.g., claimant, verifier, CSP, RP).

Password

See *memorized secret*.

Personal Identification Number (PIN)

A memorized secret typically consisting only of decimal digits.

Personally Identifiable Information (PII)

As defined by OMB Circular [A-130], Personally Identifiable Information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Private Key

The secret part of an asymmetric key pair that is used to digitally sign or decrypt data.

Pseudonymous Identifier

A meaningless but unique number that does not allow the RP to infer anything regarding the subscriber but which does permit the RP to associate multiple interactions with the subscriber's claimed identity.

Public Key

The public part of an asymmetric key pair that is used to verify signatures or encrypt data.

Public Key Certificate

A digital document issued and digitally signed by the private key of a certificate authority that binds an identifier to a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. See also [RFC 5280] (https://pages.nist.gov/800-63-3/sp800-63b.html#RFC5280).

Public Key Infrastructure (PKI)

A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration

The process through which an applicant applies to become a subscriber of a CSP and has their identity validated by the CSP.

Relying Party (RP)

An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.

Remote

(*In the context of remote authentication or remote transaction*) An information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single organization's security controls.

> Note: Any information exchange across the Internet is considered remote.

Risk Assessment

The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations, resulting from the operation of a system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Risk Management

The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

Shared Secret

A secret used in authentication that is known to the subscriber and the verifier.

Special Publication (SP)

A type of publication issued by NIST. Specifically, the SP 800-series reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

Subscriber

A party who has received a credential or authenticator from a CSP.

Subject

A person, organization, device, hardware, network, software, or service.

Symmetric Key

A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.

Valid

In reference to identity evidence, the quality of not being expired or revoked.

Verifier

An entity that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.

4. Digital Identity Model

This section is informative.

4.1. Overview

Digital identity is the unique representation of a subject engaged in an online transaction. Identity proofing establishes that a subject is actually who they claim to be. Digital authentication is the process of establishing confidence in individual identities presented digitally to a system. Systems can use the authenticated identity to determine if a subject is authorized to perform an online transaction. In most cases, the authentication and transaction take place across an open network such as the Internet; however, in some cases, access to the network may be limited and access control decisions may take this into account.

The digital identity model used in these guidelines reflects current technologies and architectures available in the market. More complex models that separate functions - such as issuing credentials and providing attributes - among larger numbers of parties are also available and may have advantages in some classes of applications. While a simpler model is used in this document, it does not preclude agencies from separating these functions. In addition, certain enrollment, identity proofing, and issuance processes performed by the CSP are sometimes delegated to an entity known as the RA or identity manager (IM). A close relationship between the RA/IM and CSP is typical, and the nature of this relationship may differ among RAs, IMs, and CSPs. The types of relationship and their requirements is outside of the scope of this document. Accordingly, the term CSP will be used to be inclusive of RA and IM functions.

Digital authentication begins with enrollment. The usual sequence for enrollment proceeds as follows. An applicant applies to a CSP. If approved, the CSP creates a credential and binds it to one or more authenticators. The credential includes at least one identifier, which can be pseudonymous, and possibly one or more attributes that the CSP has verified. The authenticators may be issued by the CSP, provided directly by the subscriber, or provided by a third party. The authenticators and credential may be used in subsequent authentication events.

The process used to verify an applicant's association with their real world identity is called *identity proofing*. 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 subscriber is self-asserted or should be treated as self-asserted and not verified. At IAL2 and IAL3, identity proofing is required, and the CSP may be requested by an RP to assert information about the subscriber, such as verified attribute values, verified attribute claims, or pseudonymous identifiers. This information assists the RP in making access control or authorization decisions. An RP may decide that its required IAL is 2 or 3, but may only need specific attributes, perhaps those that retain a degree of pseudonymity for the subject. This privacy enhancing approach is one of the benefits 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 this document suite, 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 verified in the enrollment process (subject to the policies of the CSP and the needs of the application). 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 access control or authorization decisions.

Authentication establishes confidence in the claimant's identity, and in some cases in attributes about the subscriber (for example 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. RPs can use a subscriber's authenticated identity and attributes with other factors to make access control or 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, requires the use of a hardware-based authenticator and one other factor.

As part of authentication, mechanisms such as device identity or geo-location may be used to identify or prevent possible authentication false positives. While these mechanisms do not directly increase the AAL, they can aid in enforcing security policies and mitigate risks. In many cases, the authentication process and services will be shared by many applications and agencies. However, it is the individual agency or application acting as the RP that shall make the decision to grant access or process a transaction based on the specific application requirements.

The various entities and interactions that comprise the digital identity model used here are illustrated below in Figure 4-1. 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 the interactions related to using an authenticator to perform digital authentication. When the subscriber needs to authenticate to perform a transaction, he or she becomes a claimant 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. In a federated identity architecture, the CSP or verifier provides an assertion about the subscriber to the RP, which may use the information in the assertion to make an access control or 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 prior to authentication of 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 rather than a physical link. 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 his or her 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, he or she 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.

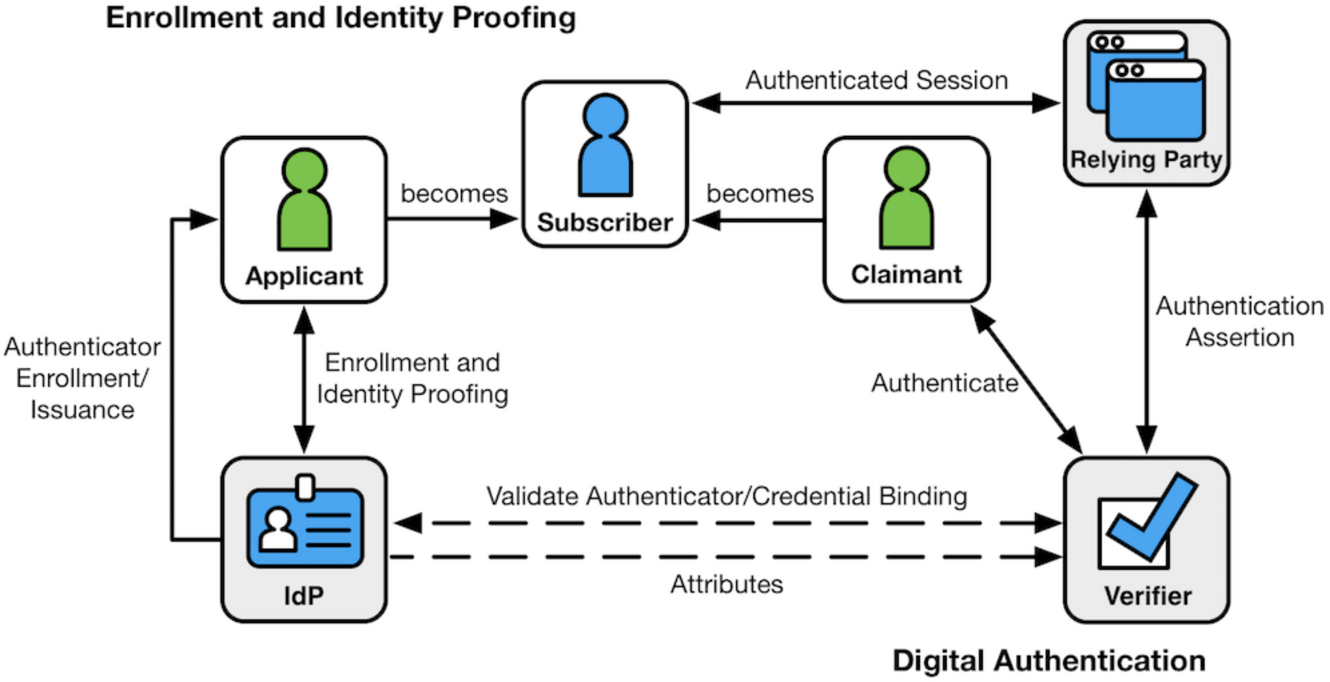


Figure 4-1. Digital Identity Model

4.2. Enrollment and Identity Proofing

Normative requirements can be found in [SP 800-63A] (sp800-63a.html), *Enrollment and Identity Proofing*.

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

An individual, referred to as an *applicant* at this stage, requests credentials from a CSP. If the applicant is successfully proofed and a credential is created by a CSP and authenticator(s) are bound to it, 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 their responsibilities to the CSP. 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] (sp800-63b.html), *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 (for example, a password).
- Something you have (for example, an ID badge or a cryptographic key).
- Something you are (for example, a fingerprint or other biometric data).

MFA refers to the use of more than one of the factors listed above. The strength of authentication systems is largely determined by the number of factors incorporated by the system. Implementations that use two different factors are typically considered stronger than those that use only one factor. 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 document, authenticators always contain a secret. Some of the classic authentication factors do not apply directly to digital authentication. For example, an ID badge 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 can be confirmed from public databases, also does not constitute an acceptable secret for digital authentication. More generally, something you are does not generally 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, 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 in the authentication process to authenticate the claimant. An impostor must steal the encrypted key (by stealing the hardware) and replicate the fingerprint to use the authenticator. This specification considers such a device to effectively provide two factor authentication, although the actual authentication protocol between the verifier and the claimant simply proves possession of the key.

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 this specification. 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] (sp800-63a.html), *Enrollment and Identity Proofing* recommends that biometrics be used in the enrollment process for higher LOAs to later help prevent a subscriber who is registered from repudiating the enrollment, to help identify those who commit enrollment fraud, and to unlock authenticators.

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. 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 it 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] (sp800-63c.html), *Federation and Assertions*.

Overall, SP 800-63-3 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 can reuse the issued credential at multiple RPs.
- Cost reduction to both the user (reduction in authenticators) and the agency (reduction in IT 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. If the verifier is implemented in combination with the RP, the assertion is implicit. If the verifier is a separate entity from the RP, as in typical federated identity models, 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, and the corresponding trust framework that governs the policies and process 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 by the subscriber. However, if the verifier and the RP communicate directly, a protected session may be used to provide the integrity protection. 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 access control or 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, supplements the NIST Risk Management Framework (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 that agencies 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 upon 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, the 800-63 suite recognizes that an authentication error is not a singleton that drives all requirements.

This guideline details requirements to assist agencies in avoiding (1) authentication errors (i.e., a false claimant using a credential that is not rightfully theirs), (2) identity proofing errors (i.e., a false claimant claiming an identity that is not rightfully theirs), and (3) federation errors (an identity assertion is compromised). From the perspective of an identity proofing failure, there are two dimensions of potential failure:

- The impact of providing a service to the wrong subject (e.g., an attacker successfully proofs as someone else).
- 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, authentiation, 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 will employ to meet each assurance level, agencies SHALL develop a "Digital Identity Acceptance Statement", in accordance with NIST 800-53r5 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

The individual assurance levels that will be selected based on risk are as as follows:

- 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 the identifier of a specific individual. AAL is selected to 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 utilized by the federation 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.

Identity Assurance Level
IAL1 - At IAL1, attributes, if any, are self-asserted or should be treated as self-asserted.
IAL2 - IAL2 introduces the need for either remote or in-person identity proofing. IAL2 requires identifying attributes to have been verified in person or remotely using, at a minimum, the procedures given in [SP 800-63A] (sp800-63a.html).
IAL3 - At IAL3, in-person identity proofing is required. Identifying attributes must be verified by an authorized representative of the CSP through examination of physical documentation as described in [SP 800-63A] (sp800-63a.html).

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.

Federation Assurance Level
FAL1 - FAL1 permits the RP to receive a bearer assertion from an identity provider (IdP). The assertion must be signed by the IdP 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 in addition to the assertion artifact itself. The assertion must be signed using approved cryptography and encrypted to the RP using approved cryptography.

When described generically or bundled, this guideline will refer to the combination of IAL, AAL, and FAL as ***xAL***.

5.3. Risk and Impacts

This section provides details on the impact categories that SHALL be assessed to determine IAL, AAL, and FAL.

Potential Impact Categories: To determine the appropriate level of assurance in 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:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- 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, “Standards for Security Categorization of Federal Information and Information Systems.”

The three potential impact values are:

- Low impact
- Moderate impact
- 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, sensitive PII may be collected, but it is never made available online to the person after the information is submitted. 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 resumes to apply for open job postings. In this use case, the digital service allows–or at least does not restrict–an individual to submit a resume on behalf of anyone else, and in subsequent visits to the site, access the resume for various purposes. Since the resume information is available to the user in later sessions, and is likely to contain PII, the agency must select an AAL that requires MFA, even though the user self-asserted the PII. 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 resume 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 resume submitted online if a decision to hire is made. Yet this level of proofing is not required to submit the resume 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 seemlingly obvious identiy 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 PUB 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 PUB 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 PUB 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 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 are encouraged to consider additional techniques and technologies to further secure and privacy-enhance their services.

Agencies MAY determine to partially implement the NIST recommended guidance based on their mission risk tolerance, existing business processes, special considerations for certain populations, availablity 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 compensating controls when the complete set of applicable 800-63 requirements are not implemented. That said, agencies SHALL NOT alter the assessed value based on agency capabilities. Rather, the agency MAY adjust implementation of solutions based the agency's ability to mitigate risk via means not explicitly addressed by 800-63 requirements. The agency SHALL implement prodecures to document both the justification for any departure from normative requirements and detail the compensating control 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" 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 Authorization and Accreditation (A&A).

The statement SHALL include, at a minimum:

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

6. Selecting Assurance Levels

This section is informative. The results of the risk assessment 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 xAL selection.

First, compare the impact profile from the risk assessment 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 potential 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. 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 user submit personal informatin in 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 identify of the user. In this case, an ‘effective proofing process’ would be to not proof at all. This allows the user of the health tracker system to be pseudonymous.

Despite the user being pseudonymous, the agency should still protect the application wiith AAL2 or AAL3 because a malicous actor could gain access to the users PHI by compromising the account. If it is a targeted attack, the malicious actor may know the users identity, creating the same negative impact to the user as if the agency has identity proofed.

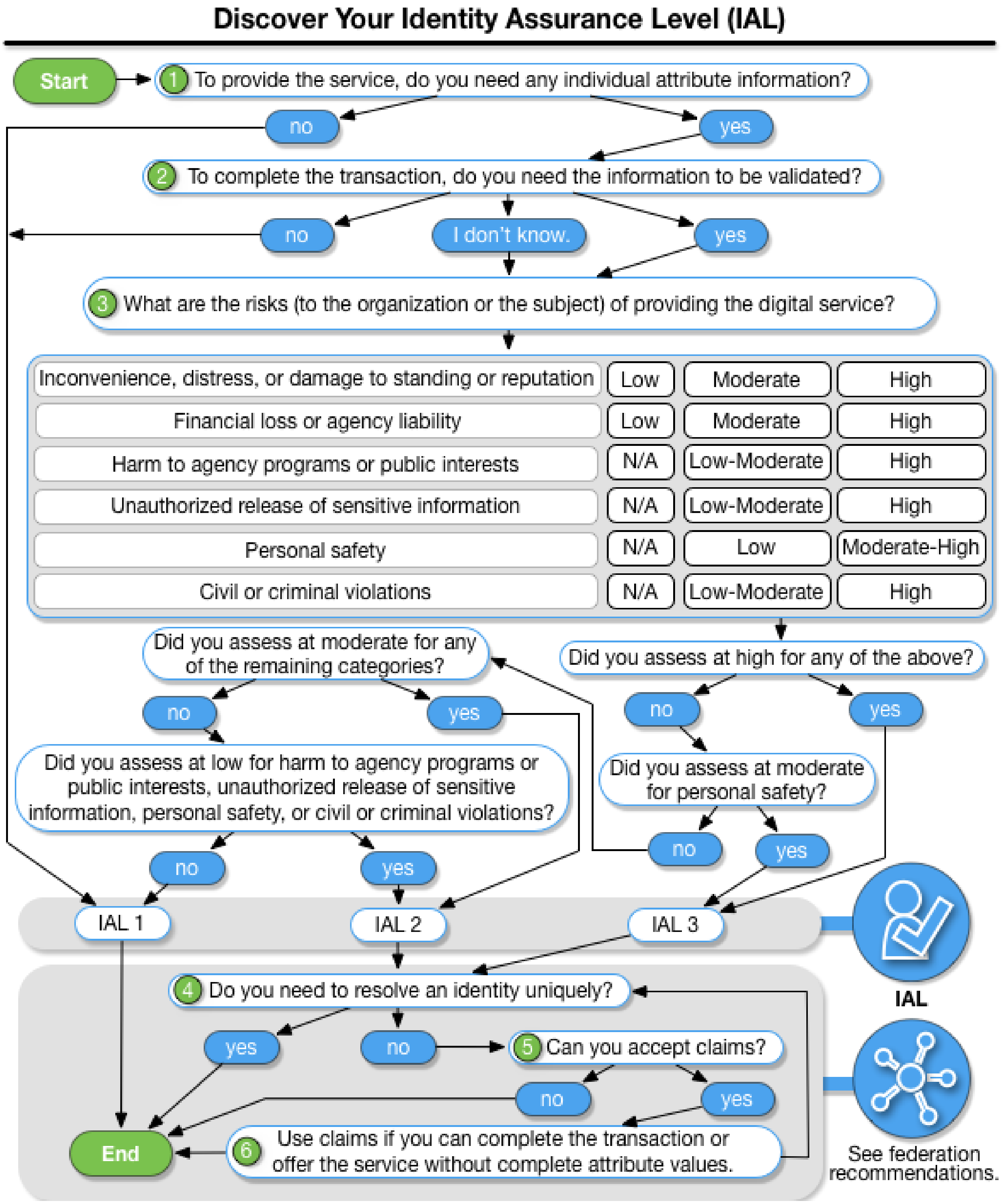
> Note: An agency can accept a higher assurance level than those required in the table above. For example, in a federated transaction, an agency can accept an IAL3 identity if their application is assessed at IAL2. The same holds true for authenticators; stronger authenticators can be used at RPs that 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 privacy requirements (./sp800-63c.html#sec9) in SP 800-63C for more details.

> Note: The upshot of potentially having a different IAL, AAL, and FAL withing 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 xAL, 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.


Discover Your Identity Assurance Level (IAL)
Start
1 To provide the service, do you need any individual attribute information?
no
yes
2 To complete the transaction, do you need the information to be validated?
no
I don't know.
yes
3 What are the risks (to the organization or the subject) of providing the digital service?
Did you assess at moderate for any of the remaining categories?
no
yes
Did you assess at high for any of the above?
no
yes
Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?
Did you assess at moderate for personal safety?
no
yes
no
yes
IAL 1
IAL 2
IAL 3
IAL
4 Do you need to resolve an identity uniquely?
yes
no
5 Can you accept claims?
no
yes
End
6 Use claims if you can complete the transaction or offer the service without complete attribute values.
See federation recommendations.

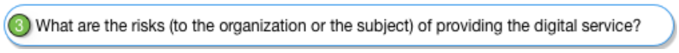
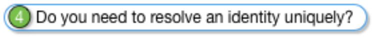
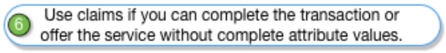
Inconvenience, distress, or damage to standing or reputation	Low	Moderate	High
Financial loss or agency liability	Low	Moderate	High
Harm to agency programs or public interests	N/A	Low-Moderate	High
Unauthorized release of sensitive information	N/A	Low-Moderate	High
Personal safety	N/A	Low	Moderate-High
Civil or criminal violations	N/A	Low-Moderate	High

Figure 6-1. Selecting IAL

1 To provide the service, do you need any individual attribute information?

The risk assessment and selection of IAL 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 beginning 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.
 5 Can you accept claims?
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 determined they need, and identify which ones can suffice as claims and which ones 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 control of the digital service provider.
 6 Use claims if you can complete the transaction or offer the service without complete attribute values.
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 claims from a CSP (or multiple CSPs), since it has been determined that complete attribute values are not needed to deliver the digital service.

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 of whether the agency can federate is provided in Section 7.

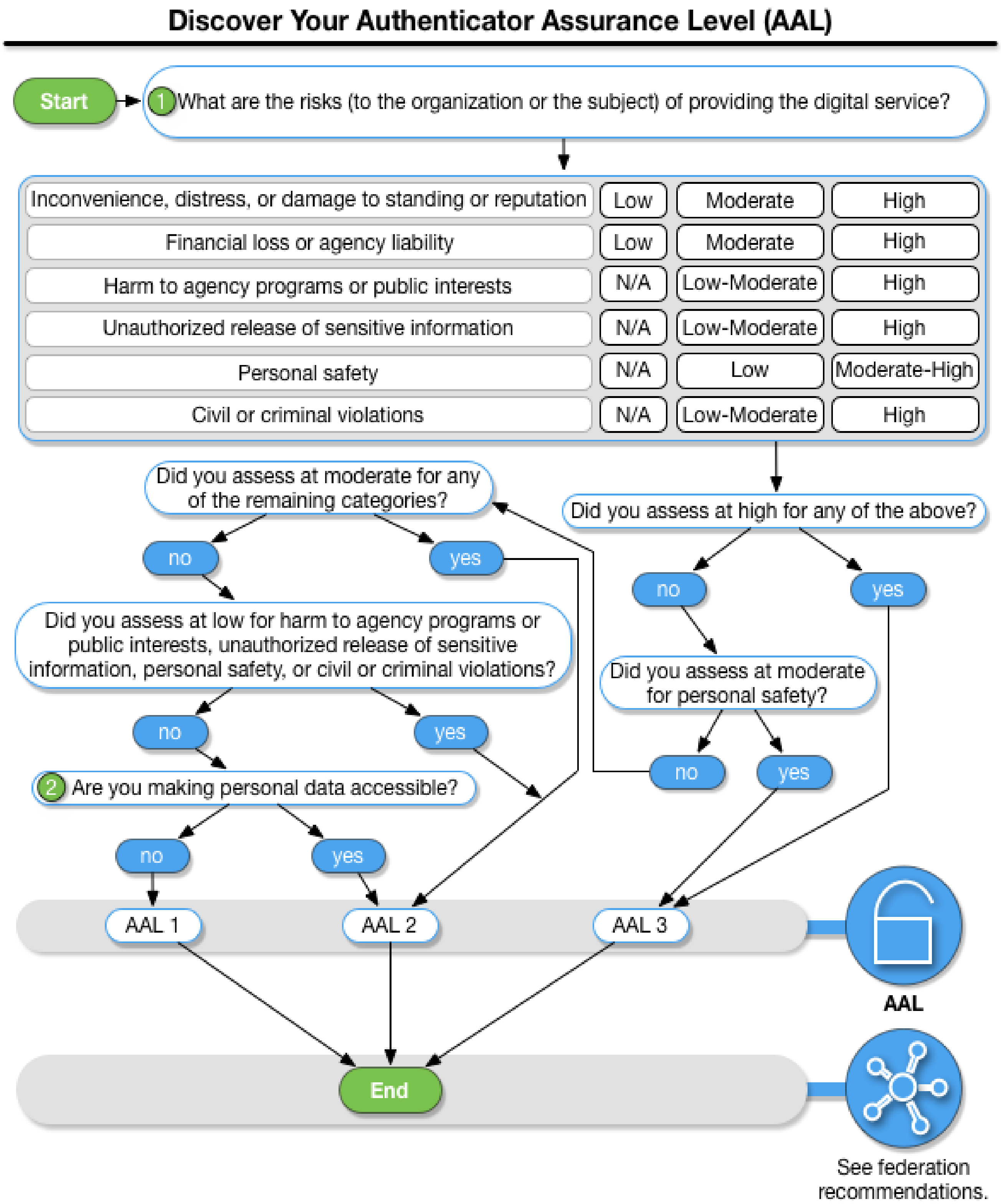

Discover Your Authenticator Assurance Level (AAL)
Start
1 What are the risks (to the organization or the subject) of providing the digital service?
Inconvenience, distress, or damage to standing or reputation
Low
Moderate
High
Financial loss or agency liability
Low
Moderate
High
Harm to agency programs or public interests
N/A
Low-Moderate
High
Unauthorized release of sensitive information
N/A
Low-Moderate
High
Personal safety
N/A
Low
Moderate-High
Civil or criminal violations
N/A
Low-Moderate
High
Did you assess at moderate for any of the remaining categories?
no
yes
Did you assess at high for any of the above?
no
yes
Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?
no
yes
Did you assess at moderate for personal safety?
no
yes
2 Are you making personal data accessible?
no
yes
AAL 1
AAL 2
AAL 3
AAL
End
See federation recommendations.

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 beginning 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 regarding 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

All FALs require assertions to have a baseline of protections, including signatures, expirations, audience restrictions, and others enumerated in [SP 800-63C] (sp800-63c.html#sec5). 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.

RPs should use a back-channel presentation mechanism (sp800-63c.html#sec6) 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. Since the assertion reference is presented by the RP directly to the IdP, the IdP can often take steps to identify and authenticate the RP during this step. Furthermore, since the assertion is fetched by the RP directly from the IdP over an authenticated protected channel, there are fewer opportunities for an attacker to inject an assertion into an RP.

FAL2 and higher require the assertion itself to be encrypted such that the intended RP is the only party that can decrypt it. This method not only improves the enforcement of audience restriction at RPs (since an unintended RP won't be able to decrypt an assertion), but also increases privacy protection by protecting the assertion message itself in addition to having it be passed along authenticated protected channels. RPs that allow front-channel presentation of assertions should require at least FAL2 to protect the content of the assertion, since the assertion can be seen by the subscriber and handled by the subscriber's browser.

FAL3 further requires that the subscriber prove possession of a key in addition to the ability to present an assertion or assertion reference. This method allows the RP to strongly verify the binding of the assertion to the subscriber by means of a key held by the subscriber. This key is referenced in the assertion and represents the subscriber.

Increasing the FAL increases the complexity of the deployment and management of a federation system, as RP keys need to be managed at FAL2 and FAL3 and subscriber keys additionally need to be managed at FAL3. Therefore, RPs should add advanced functionality where it is feasible and warranted for the application.

6.4. Combining xALs

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

The ability to combine varying xALs 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.

The technical guidelines detailed in NIST SP 800-63-3 and its companion volumes are agnostic to the authentication and identity proofing architecture an agency selects. However, there are scenarios an agency may encounter which make identity federation potentially more attractive than establishing identity services local to the agency or individual applications. The following list details the scenarios where an agency may consider federation as a viable option. This list does not factor in any economic benefits or weaknesses of federation vs. localized identity architectures.

Federate authenticators when:

- Potential users already have an authenticator at or above required AAL.
- Multiple credential form factors are required to cover all possible user communities.
- Agency does not have infrastructure to support authentication management (e.g., account recovery, authenticator issuance, help desk).
- Desire to allow the primary authentication to be modified and upgraded over time without changing the RP's implementation.
- 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.
- Potential users come from multiple communities, each with its own existing identity infrastructure.

Federate attributes when:

- Pseudonymity is required, necessary, feasible, or important to stakeholders accessing the service.
- Access to the service only requires a partial attribute list.
- Access to the service only requires at least one attribute claim.
- Agency is not the authoritative source or issuing source for required attributes.
- 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.

8. References

This section is informative.

[EO 13681] *Executive Order 13681, Improving the Security of Consumer Financial Transactions* (October 17, 2014), available at: https://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions (https://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions).

[M-04-04] *OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies* (December 16, 2003), available at: https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf (https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf).

[NSTIC] *National Strategy for Trusted Identities in Cyberspace* (April, 2011), available at: https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf (https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf).

[ESIG] Federal CIO Council, *Use of Electronic Signatures in Federal Organization Transactions* (January 25, 2013), available at: https://cio.gov/wp-content/uploads/downloads/2014/03/Use_of_ESignatures_in_Federal_Agency_Transactions_v1-0_20130125.pdf (https://cio.gov/wp-content/uploads/downloads/2014/03/Use_of_ESignatures_in_Federal_Agency_Transactions_v1-0_20130125.pdf).

[FISMA] *Federal Information Security Management Act*, available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf (http://csrc.nist.gov/drivers/documents/FISMA-final.pdf).

[HSPD-12] Department of Homeland Security, *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors* (August 27, 2004), available at: https://www.dhs.gov/homeland-security-presidential-directive-12 (https://www.dhs.gov/homeland-security-presidential-directive-12).

[M-03-22] OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (September 26, 2003), available at: http://www.whitehouse.gov/omb/memoranda/m03-22.html (http://www.whitehouse.gov/omb/memoranda/m03-22.html).

[A-130] OMB Circular A-130, *Managing Federal Information as a Strategic Resource* (July 28, 2016), available at: https://www.whitehouse.gov/omb/circulars_default (https://www.whitehouse.gov/omb/circulars_default).

[SP 800-30] NIST Special Publication 800-30, *Guide for Conducting Risk Assessments* (September 2012), available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf).

[SP 800-37] NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach* (February 2010), available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf).

[SP 800-53A] NIST Special Publication 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans* (December 2014), available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf).

[GPG 45] UK Cabinet Office, Good Practice Guide 45, *Identity proofing and verification of an individual*, November 3, 2014, available at: https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual (https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual).

[RSDOPS] UK Cabinet Office, Good Practice Guide 43, *Requirements for Secure Delivery of Online Public Services (RSDOPS)*, November 3, 2014, available at: https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services (https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services).

[STORK 2.0] European Union, *Secure idenTity acrOss boRders linKed 2.0*, 2014, available at: https://www.eid-stork2.eu/ (https://www.eid-stork2.eu/).

[eIDAS] European Union, *REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (23 July 2014)*, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG).

[ISO 29115] International Standards Organization, ISO/IEC 29115 *Information technology – Security techniques – Entity authentication assurance framework*, April 1, 2013, available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45138 (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45138).