

[NIST Website \(<http://www.nist.gov>\)](http://www.nist.gov)[About NIST \(\[http://www.nist.gov/public_affairs/nandyou.cfm\]\(http://www.nist.gov/public_affairs/nandyou.cfm\)\)](http://www.nist.gov/public_affairs/nandyou.cfm)[usnistgov on Github \(<https://github.com/usnistgov>\)](https://github.com/usnistgov)

Fri, 10 Jun 2016 12:15:22 -0400

DRAFT NIST Special Publication 800-63-3

Digital Authentication Guideline

Paul A. Grassi

James L. Fenton

COMPUTER SECURITY



DRAFT NIST Special Publication 800-63-3

Digital Authentication Guideline

Paul A. Grassi

*Applied Cybersecurity Division**Information Technology Laboratory*

James L. Fenton

*Altnode Networks**Los Altos, CA*

Month TBD 2016



U.S. Department of Commerce

Penny Pritzker, Secretary

National Institute of Standards and Technology

*Willie E. May, 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 information 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 (MonthTBD 2016)

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 information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This recommendation, along with accompanying recommendations in the SP 800-63 document set, provide technical guidelines for Federal agencies implementing digital authentication and is not intended to constrain the development or use of standards outside of this purpose. The recommendation covers remote authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. It defines technical requirements for each of four levels of assurance in 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 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

Trademark Information

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.

Executive Summary

Digital authentication is the process of establishing confidence in user identities digitally presented to an information system. Digital authentication presents a technical challenge when this process involves the authentication of individual people over an open network for the purpose of digital government and commerce.

The suite of SP 800-63-3 documents provides technical guidelines to agencies to allow an individual to authenticate his or her identity to a Federal digital service. This document 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 address only traditional, widely implemented methods for digital authentication, based on secrets. With these methods, the individual to be authenticated proves that he or she knows or possesses a valid authenticator or combination of authenticators.

These technical guidelines supplement OMB guidance, *E-Authentication Guidance for Federal Agencies* [OMB M-04-04] and supersede NIST SP 800-63-1 and SP 800-63-2. OMB M-04-04 defines four levels of assurance, Levels 1 to 4, in terms of the consequences of authentication errors and misuse of credentials. Level 1 is the lowest assurance level, and Level 4 is the highest. The OMB guidance defines the required level of identity assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides agencies with the criteria for determining the level of identity assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence of each application or transaction.

OMB guidance outlines a five-step process by which agencies should meet their digital authentication assurance requirements:

1. Conduct a risk assessment of the government system.
2. Map identified risks to the appropriate assurance level.
3. Select technology based on digital authentication technical guidance.
4. Validate that the implemented system has met the required assurance level.
5. Periodically reassess the information system to determine technology refresh requirements.

This document suite provides guidelines for implementing the third step of the above process. A new approach for digital authentication solutions is required by these guidelines, separating the individual elements of identity assurance into discrete, component parts. For non-federated systems, agencies will select and combine two (2) individual components, referred to as *Identity Assurance Level (IAL)* and *Authenticator Assurance Level (AAL)*. For federated systems, a third component, *Federation Assurance Level (FAL)*, is required.

- IAL refers to the robustness of the identity proofing process and the binding between an authenticator and the records pertaining to a specific individual.
- AAL refers to the robustness of the authentication process itself.
- FAL refers to the robustness of the assertion protocol utilized by the federation to communicate authentication and attribute information (if applicable) to a relying party.

The separation of these metrics supports applications requiring strong authentication that may be pseudonymous, and the separation of authenticator issuance from the establishment of credentials binding those authenticators to individuals.

Accordingly, with this revision, SP 800-63 has been split into a family of documents organized as follows:

- SP 800-63-3 *Digital Authentication Guideline* - Provides guidance on general authentication issues and for using authenticators, credentials, and assertions together in an information system.
- SP 800-63A *Enrollment and Identity Proofing* - Deals with the processes by which a credential, and authenticator(s) associated with that credential, can be bound to a specific individual. This typically happens when that individual is enrolled in an identity system, through the identity proofing process.

- SP 800-63B *Authentication and Lifecycle Management* - provides guidance on the selection, use, and management of authenticators (formerly called *tokens*) to authenticate a remote subscriber to an identity system at specified authenticator assurance levels.
- SP 800-63C *Federation and Assertions* - Provides guidance on the use of federated identity and assertions to convey the results of authentication processes to a relying party.

IAL and AAL Summary

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

Identity Assurance Level 1 – At this level, attributes provided in conjunction with the authentication process, if any, are self-asserted.

Identity Assurance Level 2 – IAL 2 introduces the need for either remote or in-person identity proofing. IAL 2 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).

Identity Assurance Level 3 – At IAL 3, 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 1 - AAL 1 provides single factor digital authentication, giving some assurance that the same claimant who participated in previous transactions is accessing the protected transaction or data. AAL 1 allows a wide range of available authentication technologies to be employed and requires only a single authentication factor to be used. It also permits the use of any of the authentication methods of higher authenticator assurance levels. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she possesses and controls the authenticator.

Authenticator Assurance Level 2 – AAL 2 provides higher assurance that the same claimant who participated in previous transactions is accessing the protected transaction or data. Two different authentication factors are required. Various types of authenticators, including multi-factor Software Cryptographic Authenticators, may be

used as described in SP 800-63B (sp800-63b.html). AAL 2 also permits any of the authentication methods of AAL 3. AAL 2 authentication requires cryptographic mechanisms that protect the primary authenticator against compromise by the protocol threats for all threats at AAL 1 as well as verifier impersonation attacks. Approved cryptographic techniques are required for all assertion protocols used at AAL 2 and above.

Authenticator Assurance Level 3 – AAL 3 is intended to provide the highest practical digital authentication assurance. Authentication at AAL 3 is based on proof of possession of a key through a cryptographic protocol. AAL 3 is similar to AAL 2 except that only “hard” cryptographic authenticators are allowed. The authenticator is required to be a hardware cryptographic module validated at Federal Information Processing Standard (FIPS) 140 Level 2 or higher overall with at least FIPS 140 Level 3 physical security. AAL 3 authenticator requirements can be met by using the PIV authentication key of a FIPS 201 compliant Personal Identity Verification (PIV) Card.

M-04-04 Levels of Assurance Requirements

The following table shows the new requirements for M-04-04 Level of Assurance, mapping corresponding Identity, Authenticator, and Federation Assurance Levels. Further details and normative requirements are provided in are provided in SP 800-63A (./sp800-63a.md), SP 800-63B (./sp800-63b.md), and SP 800-63C (./sp800-63c.md) respectively.

Level of Assurance (LOA)	Identity Assurance Level (IAL)	Authenticator Assurance Level (AAL)	Federation Assurance Level (FAL)
1	1	1, 2 or 3	TBD
2	1 or 2	2 or 3	TBD
3	1 or 2	2 or 3	TBD
4	1, 2 or 3	3	TBD

This mapping takes advantage of the ability to separate distinct identity elements per assurance level. For example, an agency is allowed to adopt multi-factor authentication (MFA) at LOA1. High assurance authenticators are allowed at low

levels of assurance, where no identity is needed, because the authenticator will not leak any person information. See privacy requirements (..sp800-63c/sec8_privacy.md) in SP 800-63C for more details.

Agency mission need will assist in determining the acceptable IAL at a given LOA. Since agencies should limit the collection of personal data in order to provide services and allow for strong pseudonymity, a specific IAL is not explicitly required for each LOA. For example, an agency may establish a “health tracker” application. In line with the terms of Executive Order 13681 requiring “...that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate.”, the agency could select LOA3 such that an AAL2 authenticator is required. However, in this example, there may be no need for the agency system to know the true identity of the user. In the past, the LOA3 assessment of data sensitivity would also require the agency to identity proof the user. This is no longer necessary and the agency is encouraged in this case to not perform any identity proofing and allow the user of the health tracker system to be pseudonymous at IAL1. The MFA authenticator at AAL2 or AAL3 will not leak any personal information because it is bound to an IAL 1 identity.

In this case of federal employees, bound by HSPD-12 and required to obtain a Personal Identity Verification (PIV) smart card, the requirement is that agencies meet LOA4. The HSPD-12 use case requires an authenticator at AAL3 **and** identity proofing at IAL 3.

Important 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 RP’s that have lower authenticator requirements. However, RPs will ensure that these scenarios only occur in federated scenarios with appropriate privacy protections by the CSP to ensure that only the requested attributes are provided to the RP and that no personal information leaks from the authenticator or the assertion. See privacy requirements (..sp800-63c/sec8_privacy.md) in SP 800-63C for more details.

Acceptable IAL and AAL Combinations

The following table details valid combinations of IAL and AAL that may be established during the enrollment process:

	IAL 1	IAL 2	IAL 3
AAL 1	Allowed	NO	NO
AAL 2	Allowed	Allowed	See Note
AAL 3	Allowed	Allowed	Allowed

Note: AAL 2 capable authenticators MUST be bound to credentials at IAL 2 enrollment since management (and often use) of those credentials is a release of personal data requiring multi-factor authentication. AAL 3 authenticators SHOULD be bound to IAL 3 credentials since they are frequently required for the high-sensitivity applications that require in-person identity proofing.

In limited situations, a given transaction requiring IAL 2 MAY be able to authenticate at AAL 1 when personal data is not made accessible to the subscriber (per Executive Order 13681) and the other risk and sensitivity requirements of M-04-04 are satisfied.

Table of Contents

1. Purpose
2. Introduction
3. Definitions and Abbreviations
4. Digital Authentication Model
5. References

1. Purpose

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

2. Introduction

Digital authentication is the process of establishing confidence in user identities presented to an information system. Digital authentication presents a technical challenge when this process involves the remote authentication of individual people over a network. This recommendation provides technical guidelines to agencies to allow an individual person to remotely authenticate his/her identity to a Federal Information Technology (IT) system. This recommendation also provides guidelines for credential service providers (CSPs), verifiers, and relying parties (RPs).

Current government systems do not separate the functions of authentication and attribute providers. However, in some applications, these functions are provided by different parties. This document suite describes authenticator assurance and identity assurance as separate metrics, and provides a mapping between these metrics and overall level of assurance. These technical guidelines supplement OMB guidance, *E-Authentication Guidance for Federal Agencies* [OMB M-04-04] and supersede NIST SP 800-63-1 and SP 800-63-2. OMB M-04-04 defines four levels of assurance, Levels 1 to 4, in terms of the consequences of authentication errors and misuse of credentials. Level 1 is the lowest assurance level and Level 4 is the highest. The guidance defines the required level of identity assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides agencies with criteria for determining the level of assurance required for specific digital transactions and systems, based on the risks and their likelihood of occurrence.

SP 800-63 is organized as a family of documents as follows:

- SP 800-63A *Enrollment and Identity Proofing* - Deals with the processes by which a credential, and authenticator(s) associated with that credential can be bound to a specific individual. This typically happens when that individual is enrolled in an identity system, through the identity proofing process.
- SP 800-63B *Authentication and Lifecycle Management* - provides guidance on the selection, use, and management of authenticators (formerly called *tokens*) to authenticate a remote subscriber to an identity system at specified authenticator assurance levels.
- SP 800-63C *Federation and Assertions* - Provides guidance on the use of assertions to convey the results of authentication processes to a relying party.

It is anticipated that SP 800-63A, SP 800-63B, and SP 800-63C will be revised asynchronously with each other and with this document. The latest revision of each should be used for guidance.

OMB guidance outlines a five-step process by which agencies should meet their authentication assurance requirements:

1. *Conduct a risk assessment of the government system* – No specific risk assessment methodology is prescribed for this purpose; however, NIST Special Publication (SP) 800-30 [SP 800-30] offers a general process for risk assessment and risk mitigation, and NIST Special Publication (SP) 800-37 Revision 1 [SP 800-37] provides guidelines on the selection and specification of security controls for an information system as part of an organization-wide information security program. This guidance supports the identification of risk to the organization or to individuals associated with the operation of an information system.
2. *Map identified risks to the appropriate assurance level* – Section 2.2 of OMB M-04-04 provides the guidance necessary for agencies to perform this mapping.
3. *Select technology based on digital authentication technical guidance* – After the appropriate assurance level has been determined, OMB guidance states that agencies should select technologies that meet the corresponding technical requirements, as specified by this document suite. Some agencies may possess existing digital authentication technology. Agencies should verify that any existing technology meets the requirements specified in this document suite.
4. *Validate that the implemented system has met the required assurance level* – As some implementations may create or compound particular risks, agencies should conduct a final validation to confirm that the system achieves the required assurance level for the user-to-agency process. NIST SP 800-53A [SP 800-53A] provides guidelines for the assessment of the implemented system during the validation process. Validation should be performed as part of a security authorization process as described in NIST SP 800-37, Revision 1 [SP 800-37].
5. *Periodically reassess the information system to determine technology refresh requirements* – The agency shall periodically reassess the information system to ensure that the identity authentication requirements continue to be satisfied. NIST SP 800-37, Revision 1 [SP 800-37] provides guidelines on the frequency,

depth and breadth of periodic reassessments. As with the initial validation process, agencies should follow the assessment guidelines specified in SP 800-53A [SP 800-53A] for conducting the security assessment.

This family of documents provides guidelines for implementing the third step of the above process. In particular, this document maps the four (4) Levels of Assurance defined in OMB M-04-04 into corresponding authenticator assurance and identity assurance levels. Other documents in the family state specific technical requirements for identity assurance and authenticator assurance in the following areas:

- Identity proofing and registration of applicants (covered in SP 800-63A)
- Credential lifecycle and management mechanisms (covered in SP 800-63A)
- Authenticators (typically a cryptographic key or password) for authentication (covered in SP 800-63B)
- Authenticator lifecycle and management mechanisms (covered in SP 800-63B)
- Protocols used to support the authentication mechanism between the claimant and the verifier (covered in SP 800-63B)
- Assertion mechanisms used to communicate the results of a remote authentication if these results are sent to other parties (covered in SP 800-63C).

The overall authentication assurance level is determined by the lowest identity assurance and authenticator assurance level achieved in any of the areas listed above, and then by mapping the result to the corresponding Level of Assurance.

Agencies may adjust the level of assurance using additional risk mitigation measures. Easing credential assurance level requirements may increase the size of the enabled customer pool, but agencies shall ensure that this does not corrupt the system's choice of the appropriate assurance level. Alternatively, agencies may consider partitioning the functionality of an digital authentication enabled application to allow less sensitive functions to be available at a lower level of authentication and attribute assurance, while more sensitive functions are available only at a higher level of assurance.

These technical guidelines cover remote digital authentication of human users to IT systems over a network. They do not address the authentication of a person who is physically present, for example, for access to buildings, although some credentials and authenticators that are used remotely may also be used for local authentication.

These technical guidelines establish requirements that Federal IT systems and service providers participating in authentication protocols be authenticated to subscribers. However, these guidelines do not specifically address machine-to-machine (such as router-to-router) authentication, or establish specific requirements for issuing authentication credentials and authenticators to machines and servers when they are used in authentication protocols with people.

The paradigm of this document suite is that individuals are enrolled, issued an authenticator, and undergo a registration process in which their identity is bound to that authenticator. Thereafter, the individuals are remotely authenticated to systems and applications over a network, using the authenticator in an authentication protocol. The authentication protocol allows an individual to demonstrate to a Verifier that he or she has possession and control of the authenticator, in a manner that protects the authenticator secret from compromise by different kinds of attacks. Higher authenticator assurance levels require use of stronger authenticators, better protection of the authenticator(s) and related secrets from attacks. Higher identity assurance levels require stronger registration procedures.

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. Certain authentication technologies, particularly biometrics and knowledge based authentication, use information that is private rather than secret. While they are discussed to a limited degree, they are largely avoided because their security is often weak or difficult to quantify, especially in the remote situations that are the primary scope of this document suite.

Knowledge based authentication achieves authentication by testing the personal knowledge of the individual against information obtained from public databases. As this information is considered private but not actually secret, confidence in the identity of an individual can be hard to achieve. In addition, the complexity and interdependencies of knowledge based authentication systems are difficult to quantify. However, knowledge based verification techniques are included as part of registration in this document suite.

Biometric characteristics do not constitute secrets suitable for use in the conventional remote authentication protocols addressed in this document suite either. In the local authentication case (which is outside the scope of this document suite), where the

claimant is observed by an attendant and uses a capture device controlled by the Verifier, authentication does not require that biometrics be kept secret. This document suite supports the use of biometrics to “unlock” multifactor authentication authenticators, to prevent repudiation of registration, and to verify that the same individual participates in all phases of the registration process.

This document suite identifies minimum technical requirements for remotely authenticating users. 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* [OMB M-03-22]. See the *Guide to Federal Agencies on Implementing Electronic Processes* [DOJ 2000] for additional information on legal risks, especially those that are related to the need to satisfy legal standards of proof and prevent repudiation, as well as *Use of Electronic Signatures in Federal Organization Transactions* [GSA ESIG].

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 the 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 information systems that support the operations and assets of the agency. This includes the security authorization of IT systems that 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.

2.1. How to Use this Suite of Special Publications

The business model, marketplace, and the composition of the way identity services are delivered has drastically changed since initial versions of Special Publication 800-63 were released. Notably, CSPs can be componentized and composed of multiple independently operated and owned business entities. In addition, there is a significant benefit to provide strong authenticators even if no identity proofing is required.

Therefore, a suite of special publications 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 guidelines 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 preferred over a standalone CSP, meeting the requirements of SP 800-63C (sp800-63c.html) will apply.

2.2. 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, it is intended to achieve alignment to national and international standards that describe levels of identity assurance. 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.

SP 800-63	[GPG 45]	[RSDOPS]	STORK 2.0	29115:2011	ISO 29003	Government of Canada
N/A	N/A	Level 01	N/A	N/A	N/A	N/A
AAL/IAL 1	Level 1	Level 1	QAA Level 1	LoA 1	LoA 1	IAL/CAL 1
AAL/IAL 1	Level 2	Level 2	QAA Level 2	LoA 2	LoA 2	IAL/CAL 2
AAL/IAL 2	Level 3	Level 3	QAA Level 3	LoA 3	LoA 3	IAL/CAL 3
AAL/IAL 3	Level 4	N/A2	QAA Level 4	LoA 4	LoA 4	IAL/CAL 4

2.2. Change History

2.2.1. 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 level of assurance 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.

2.2.2. SP 800-63-2

NIST SP 800-63-2 was a limited update of Special Publication 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.

2.2.3. SP 800-63-3

NIST SP 800-63-3 is a substantial update and restructuring of Special Publication 800-63-2. It introduces the concepts of authenticator assurance level and identity assurance level to support the growing need for independent treatment of authentication strength and confidence in the claimant's identity (for example, in strong pseudonymous authentication). It also moves from a single document describing authentication to a family of four documents, of which SP 800-63-3 is the top-level document.

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

- 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

There is a wide variety of terms used in the area of authentication. 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 of 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 family for additional definitions and abbreviations specific to their content.

To Be Done: Remove words/definitions only applicable to the sub-documents.

Active Attack

An online attack where the attacker transmits data to the claimant, credential service provider, verifier, or relying party. Examples of active attacks include man-in-the-middle, impersonation, and session hijacking.

Address of Record

The official location where an individual can be found. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual. In very limited circumstances, an Army Post Office

box number, Fleet Post Office box number or the street address of next of kin or of another contact individual can be used when a residential street address for the individual is not available.

Approved

Federal Information Processing Standard (FIPS) approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation.

Applicant

A party undergoing the processes of registration and identity proofing.

Assertion

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

Assertion Reference

A data object, created in conjunction with an assertion, which identifies the verifier and includes a pointer to the full assertion held by the verifier.

Assurance

In the context of [OMB M-04-04] and this document, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Asymmetric Keys

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

Attack

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

Attacker

A party who acts with malicious intent to compromise an information system.

Attribute

A claim of a named quality or characteristic inherent in or ascribed to someone or something. (See term in [ICAM] for more information.)

Authentication

The process of establishing confidence in the identity of users or information systems.

Authentication Protocol

A defined sequence of messages between a claimant and a verifier that demonstrates that the claimant has possession and control of a valid authenticator to establish his/her identity, and optionally, demonstrates to the claimant that he or she is communicating with the intended verifier.

Authentication Protocol Run

An exchange of messages between a claimant and a verifier that results in authentication (or authentication failure) between the two parties.

Authentication Secret

A generic term for any secret value that could be used by an attacker to impersonate the subscriber in an authentication protocol.

These are further divided into *short-term authentication secrets*, which are only useful to an attacker for a limited period of time, and *long-term authentication secrets*, which allow an attacker to impersonate the subscriber until they are manually reset. The authenticator secret is the canonical example of a long term authentication secret, while the authenticator output, if it is different from the authenticator secret, is usually a short term authentication secret.

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 versions of this guideline, this was referred to as a *token*.

Authenticator Assurance Level (AAL)

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

Authenticator Output

The output value generated by an authenticator. The ability to generate valid authenticator outputs on demand proves that the claimant possesses and controls the authenticator. Protocol messages sent to the verifier are dependent upon the authenticator output, but they may or may not explicitly contain it.

Authenticator Secret

The secret value contained within an authenticator.

Authenticity

The property that data originated from its purported source.

Bearer Assertion

An assertion that does not provide a mechanism for the subscriber to prove that he or she is the rightful owner of the assertion. The RP has to assume that the assertion was issued to the subscriber who presents the assertion or the corresponding assertion reference to the RP.

Bit

A binary digit: 0 or 1.

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.

Certificate Authority (CA)

A trusted entity that issues and revokes public key certificates.

Certificate Revocation List (CRL)

A list of revoked public key certificates created and digitally signed by a Certificate Authority. See [RFC 5280].

Challenge-Response Protocol

An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a secret (such as by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the verifier. The verifier can independently verify the response generated by the claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the claimant possesses and controls the secret.

Claimant

A party whose identity is to be verified using an authentication protocol.

Claimed Address

The physical location asserted by an individual (e.g. an applicant) where he/she can be reached. It includes the residential street address of an individual and may also include the mailing address of the individual.

For example, a person with a foreign passport, living in the U.S., will need to give an address when going through the identity proofing process. This address would not be an “address of record” but a “claimed address.”

Claimed Identity

A declaration by the applicant of their current Personal Name, date of birth and address. [GPG45]

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)

An interactive feature added to web-forms to distinguish use of the form by humans as opposed to automated agents. Typically, it requires entering text corresponding to a distorted image or from a sound stream.

Cookie

A character string, placed in a web browser's memory, which is available to websites within the same Internet domain as the server that placed them in the web browser.

Credential

An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to an 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.

Cross Site Request Forgery (CSRF)

An attack in which a subscriber who is currently authenticated to an RP and connected through a secure session, browses to an attacker's website which causes the subscriber to unknowingly invoke unwanted actions at the RP.

For example, if a bank website is vulnerable to a CSRF attack, it may be possible for a subscriber to unintentionally authorize a large money transfer, merely by viewing a malicious link in a webmail message while a connection to the bank is open in another browser window.

Cross Site Scripting (XSS)

A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user supplied data from requests or forms without sanitizing the data so that it is not executable.

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.

Data Integrity

The property that data has not been altered by an unauthorized entity.

Derived Credential

A credential issued based on proof of possession and control of an authenticator associated with a previously issued credential, so as not to duplicate the identity proofing process.

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.

Eavesdropping Attack

An attack in which an attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the claimant.

Electronic Authentication (E-Authentication)

The process of establishing confidence in user identities electronically presented to an information system.

Entropy

A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits.

Extensible Mark-up Language (XML)

Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them.

Federal Bridge Certification Authority (FBCA)

The FBCA is the entity operated by the Federal Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI Policy Authority to create, sign, and issue public key certificates to Principal CAs.

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 information 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>)

Hash Function

A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:

1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and
2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.

Holder-of-Key Assertion

An assertion that contains a reference to a symmetric key or a public key (corresponding to a private key) held by the subscriber. The RP may authenticate the subscriber by verifying that he or she can indeed prove possession and control of the referenced key.

Identity

A set of attributes that uniquely describe a person within a given context.

Identity Assurance Level (IAL)

A metric describing degree of confidence that the applicant's claimed identity is their real identity.

Identity Proofing

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

Kerberos

A widely used authentication protocol developed at MIT. In “classic” Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by the KDC to use to authenticate with Bob.

When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to-KDC exchange. Longer password length and complexity provide some mitigation to this vulnerability, although sufficiently long passwords tend to be cumbersome for users.

Knowledge Based Authentication

Authentication of an individual based on knowledge of information associated with his or her claimed identity in public databases. Knowledge of such information is considered to be private rather than secret, because it may be used in contexts other than authentication to a verifier, thereby reducing the overall assurance associated with the authentication process.

Man-in-the-Middle Attack (MitM)

An attack on the authentication protocol run in which the attacker positions himself or herself in between the claimant and verifier so that he can intercept and alter data traveling between them.

Message Authentication Code (MAC)

A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non-repudiation protection.

Multi-Factor

A characteristic of an authentication system or an authenticator that uses more than one authentication factor.

The three types of 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 (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e., eavesdropping) attack at any point between the parties (e.g., claimant, verifier, CSP or RP).

Nonce

A value used in security protocols that is never repeated with the same key. For example, nonces used as challenges in challenge-response authentication protocols must not be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable.

Off-line Attack

An attack where the attacker obtains some data (typically by eavesdropping on an authentication protocol run or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing.

Online Attack

An attack against an authentication protocol where the attacker either assumes the role of a claimant with a genuine verifier or actively alters the authentication channel.

Online Guessing Attack

An attack in which an attacker performs repeated logon trials by guessing possible values of the authenticator output.

Passive Attack

An attack against an authentication protocol where the attacker intercepts data traveling along the network between the claimant and verifier, but does not alter the data (i.e., eavesdropping).

Password

A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings.

Personal Identification Number (PIN)

A password consisting only of decimal digits.

Personal Identity Verification (PIV) Card

Defined by [FIPS 201] as a physical artifact (e.g., identity card, smart card) issued to federal employees and contractors that contains stored credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

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.

Pharming

An attack in which an attacker corrupts an infrastructure service such as DNS (Domain Name Service) causing the subscriber to be misdirected to a forged verifier/RP, which could cause the subscriber to reveal sensitive information, download harmful software or contribute to a fraudulent act.

Phishing

An attack in which the subscriber is lured (usually through an email) to interact with a counterfeit verifier/RP and tricked into revealing information that can be used to masquerade as that subscriber to the real verifier/RP.

Possession and control of an authenticator

The ability to activate and use the authenticator in an authentication protocol.

Practice Statement

A formal statement of the practices followed by the parties to an authentication process (i.e., RA, CSP, or verifier). It usually describes the policies and practices of the parties and can become legally binding.

Private Credentials

Credentials that cannot be disclosed by the CSP because the contents can be used to compromise the authenticator.

Private Key

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

Protected Session

A session wherein messages between two participants are encrypted and integrity is protected using a set of shared secrets called session keys.

A participant is said to be *authenticated* if, during the session, he, she or it proves possession of a long term authenticator in addition to the session keys, and if the other party can verify the identity associated with that authenticator. If both participants are authenticated, the protected session is said to be *mutually authenticated*.

Pseudonym

A false name.

In this document, all unverified names are assumed to be pseudonyms.

Public Credentials

Credentials that describe the binding in a way that does not compromise the authenticator.

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 the name of 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].

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 an RA validates the identity of the applicant on behalf of the CSP.

Registration Authority (RA)

A trusted entity that establishes and vouches for the identity or attributes of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).

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

(As in *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.

Replay Attack

An attack in which the attacker is able to replay previously captured messages (between a legitimate claimant and a verifier) to masquerade as that claimant to the verifier or vice versa.

Risk Assessment

The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.

Salt

A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.

Secondary Authenticator

A temporary secret, issued by the verifier to a successfully authenticated subscriber as part of an assertion protocol. This secret is subsequently used, by the subscriber, to authenticate to the RP.

Examples of secondary authenticators include bearer assertions, assertion references, and Kerberos session keys.

Secure Sockets Layer (SSL)

An authentication and security protocol widely implemented in browsers and web servers. SSL has been superseded by the newer Transport Layer Security (TLS) protocol; TLS 1.0 is effectively SSL version 3.1.

Security Assertion Mark-up Language (SAML)

An XML-based security specification developed by the Organization for the Advancement of Structured Information Standards (OASIS) for exchanging authentication (and authorization) information between trusted entities over the Internet. See [SAML].

SAML Authentication Assertion

A SAML assertion that conveys information from a verifier to an RP about a successful act of authentication that took place between the verifier and a subscriber.

Session Hijack Attack

An attack in which the attacker is able to insert himself or herself between a claimant and a verifier subsequent to a successful authentication exchange between the latter two parties. The attacker is able to pose as a subscriber to the verifier or vice versa to control session data exchange. Sessions between the claimant and the relying party can also be similarly compromised.

Shared Secret

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

Social Engineering

The act of deceiving an individual into revealing sensitive information by associating with the individual to gain confidence and trust.

Special Publication (SP)

A type of publication issued by NIST. Specifically, the Special Publication 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.

Strongly Bound Credentials

Credentials that describe the binding between a user and authenticator in a tamper-evident fashion.

Subscriber

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

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.

Token

See *Authenticator*.

Token Authenticator

See *Authenticator Output*.

Token Secret

See *Authenticator Secret*.

Transport Layer Security (TLS)

An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by [RFC 5246]. TLS is similar to the older Secure Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST [SP 800-52], *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations* specifies how TLS is to be used in government applications.

Trust Anchor

A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g. in a public key certificate).

Unverified Name

A subscriber name that is not verified as meaningful by identity proofing.

Valid

In reference to an ID, the quality of not being expired or revoked.

Verified Name

A subscriber name that has been verified by identity proofing.

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) and identity and check their status.

Verifier Impersonation Attack

A scenario where the attacker impersonates the verifier in an authentication protocol, usually to capture information that can be used to masquerade as a claimant to the real verifier.

Weakly Bound Credentials

Credentials that describe the binding between a user and authenticator in a manner than can be modified without invalidating the credential.

Zeroize

Overwrite a memory location with data consisting entirely of bits with the value zero so that the data is destroyed and not recoverable. This is often contrasted with deletion methods that merely destroy reference to data within a file system rather than the data itself.

Zero-knowledge Password Protocol

A password based authentication protocol that allows a claimant to authenticate to a Verifier without revealing the password to the verifier. Examples of such protocols are EKE, SPEKE and SRP.

4. Digital Authentication Model

4.1. Overview

In accordance with OMB M-04-04, digital authentication is the process of establishing confidence in individual identities presented to a digital system. Systems can use the authenticated identity to determine if that individual 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 authentication model used in these guidelines reflects current technologies and architectures used in government. 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 credential service provider (CSP) are sometimes delegated to an entity known as the registration authority (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/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 an identifier, which can be pseudonymous, and possibly one or more attributes that the CSP has verified. The authenticators may be issued by the CSP, generated directly by the subscriber, or provided by a third party. The authenticator and credential may be used in subsequent authentication events.

The name specified in a credential may either be a verified name or pseudonym. If the CSP has determined that the name is officially associated with a real person and the subscriber is the person who is entitled to use that identity, the name is considered a verified name. If the CSP has not verified the subscriber's name, or the name is known to differ from the official name, the name is considered a pseudonym. The process used to verify a subscriber's association with a name is called *identity proofing*.

The strength of identity proofing is described by a categorization called the identity assurance level (IAL). At IAL 1, identity proofing is not required so names in credentials and assertions are considered to be pseudonyms. At IAL 2 and 3, identity proofing is required, but the CSP may assert verified attribute values, verified attribute claims, a pseudonym, or nothing. This information assists Relying Parties (RPs) in making access control or authorization decisions. RPs may decide that their required IAL is 2 or 3, but may only need specific attributes, and perhaps attributes that retain an individual's pseudonymity. This privacy enhancing approach is one of the benefits of separating the strength of the proofing process from that of the authentication process. A relying party 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, 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 the claimant's attributes (for example if the subscriber is a US 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 (e.g., government agencies) will use a subscriber's authenticated identity and attributes with other factors to make access control or authorization decisions. Nothing in this document precludes RPs from requesting additional information from a subscriber that has successfully authenticated.

The strength of the authentication process is described by a categorization called the authenticator assurance level (AAL). AAL 1 requires single-factor authentication is permitted with a variety of different authenticator types. At AAL 2, authentication

requires two authentication factors for additional security. Authentication at the highest level, AAL 3, 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 authenticator assurance level, they can enforce 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 authentication model used here are illustrated below in Figure 1. The shaded box on the left shows the enrollment, credential issuance, lifecycle management activities, and the interactions between the subscriber/claimant and the CSP. The usual sequence of interactions is as follows:

1. An individual applies to a CSP through an enrollment process.
2. The CSP identity proofs that applicant.
3. An authenticator and a corresponding credential are established between the CSP and the new 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.

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

The shaded box on the right side of Figure 1 shows the entities and the interactions related to using a 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 to the verifier that he or she possesses and controls the authenticator through an authentication protocol.
2. The verifier interacts with the CSP to validate the credential that binds the subscriber's identity to his or her authenticator.
3. If the verifier is separate from the RP (application), the 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 attribute 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 the CSP functions may be distributed and separated as shown in Figure 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, CSPs maintain status information about credentials they issue. 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/or 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.

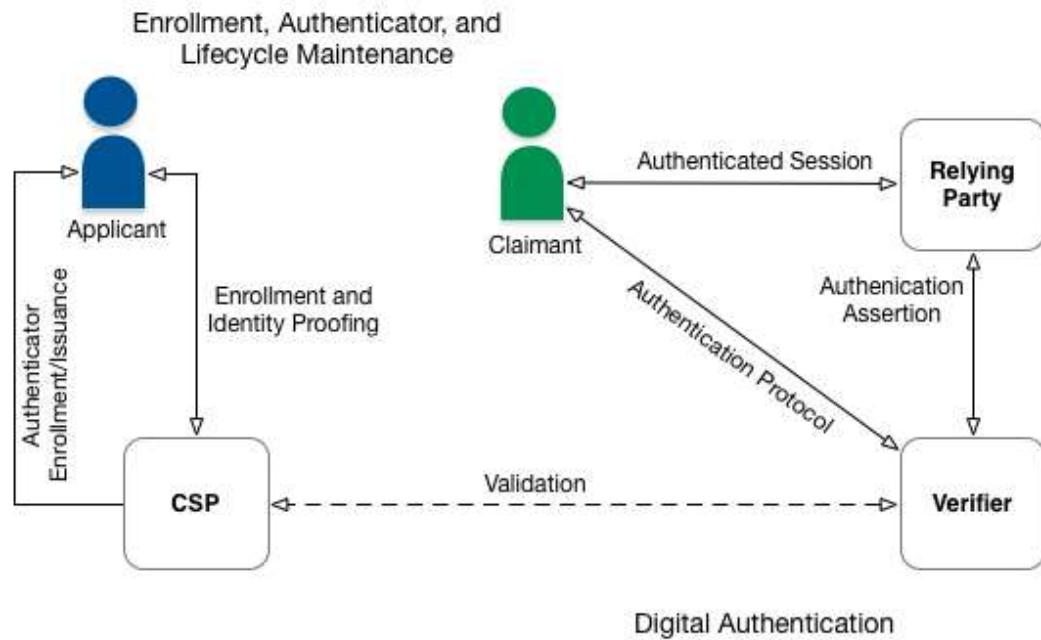


Figure 1 - Digital Authentication Model

4.2. Enrollment and Identity Proofing

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

The previous section introduced the different participants in the conceptual digital authentication 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 authenticators are issued by a CSP, 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 enrollment records.

4.3. Authentication and Lifecycle Management

Normative requirements can be found in Special Publication 800-63B, Authentication and Lifecycle Management (sp800-63b.html).

4.3.1. Authenticators

The classic paradigm for authentication systems identifies three factors as the cornerstone 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)

Multi-factor authentication 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 considered to be stronger than those that use only one factor; systems that incorporate all three factors are stronger than systems that only incorporate two of the factors. As discussed in Section 4.1, 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 a authenticator.

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 passwords. While they 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. As such, keys are something the subscriber has, while passwords are something he or she knows. Since passwords are committed to memory, they usually do not have as many possible values as cryptographic keys, and, in many protocols, are severely vulnerable to network attacks that are more restricted for keys. Moreover the entry of passwords into systems (usually through a keyboard) presents the opportunity for very simple keyboard logging attacks, and may also allow those nearby to learn the password by watching it being entered. Therefore, keys and passwords demonstrate somewhat separate authentication properties (something you have rather than something you know). When using either public key pairs or shared secrets, the subscriber has a duty to maintain exclusive control of his or her authenticator, since possession and control of the authenticator is used to authenticate the claimant's identity.

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 is useful when authenticating to a human (e.g., a guard), but is not a 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, this recommendation does not permit the use of biometrics as a authenticator.

However, this recommendation does accept that authentication systems that incorporate all three factors offer better security than systems that only incorporate two of the factors. A digital authentication system may incorporate multiple factors in either of two ways. The system may be implemented so that multiple factors are presented to the verifier, or some factors may be used to protect a secret that will be presented to the verifier. If multiple factors are presented to the verifier, each will need to be a authenticator (and therefore contain a secret). If a single factor is presented to the verifier, the additional factors are used to protect the authenticator and need not themselves be authenticators.

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. Special Publication 800-63A, Enrollment and Identity Proofing (sp800-63a.html) recommends that biometrics be used in the enrollment process for higher levels of assurance 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, credentials bind an authenticator to the subscriber as part of the issuance process. Credentials are stored and maintained by the CSP. The claimant possesses a authenticator, but is not necessarily in possession of the electronic credentials. 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 a authenticator that is bound to the asserted identity through an authentication protocol. Once possession and control has 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 traffic between the claimant and the verifier both during and after the authentication exchange, 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 and/or the RP. 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 Special Publication 800-63C, Federation and Assertions (sp800-63c.html).

Overall, SP 800-63-3 does not presuppose a federated identity architecture; rather, the guidance is 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, consistent with the National Strategy for Trusted Identities in Cyberspace (NSTIC) [NSTIC], 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 (one authenticator) and the agency (reduction in IT infrastructure)
- Data minimization: agencies do not need to pay for collection, storage, disposal, and compliance activities related to storing personal information
- Privacy enhancing

- Pseudonymous attribute assertions. Agencies can request a minimized set of attributes, to include claims, to fulfill service delivery.
- Mission enablement. 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:

- SAML Assertions – 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 - OpenID Connect 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 – 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/or FAL (federation assurance level, 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.

4.5. Assurance Levels

The overall M-04-04 LOA is determined by combining the discrete assurance level for each of the components of the architecture. For instance, to achieve M-04-04 LOA3:

- The enrollment and identity proofing process shall, at a minimum, use IAL 1 or 2 processes.
- The authenticator (or combination of authenticators) used shall have an AAL of 2 or higher.
- Authentication assertions (if used) shall have an FAL of 2 or higher (under consideration as -C is finalized).

The overall level is determined by the lowest level because it will likely be the target of an attacker. For example, if a system uses an authenticator that has AAL 2 assurance, but uses assertion mechanisms at FAL 3, the attacker will likely focus on gaining access to the authenticator since it is easier to attack a system component meeting AAL 2 rather than attacking the assertion that meets FAL 3.

5. References

Under construction

[EO 13681] *Executive Order 13681, Improving the Security of Consumer Financial Transactions* (October 17, 201, 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.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
(https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf).

[DOJ 2000] *Guide to Federal Agencies on Implementing Electronic Processes* (November 2000), available at:
<http://www.usdoj.gov/criminal/cybercrime/ecommerce.html>
(<http://www.usdoj.gov/criminal/cybercrime/ecommerce.html>)

[GSA ESIG] *Use of Electronic Signatures in Federal Organization Transactions* (2011), available at: <http://www.gsa.gov/> (<http://www.gsa.gov/>)

[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>)

[OMB 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>).

[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>).

Privacy Policy (http://www.nist.gov/public_affairs/privacy.cfm#privpolicy) | Security Notice
(http://www.nist.gov/public_affairs/privacy.cfm#secnot) | Accessibility Statement
(http://www.nist.gov/public_affairs/privacy.cfm#accesstate) | Send feedback
(<https://github.com/usnistgov/800-63-3/issues/>)  (/800-63-3/comment_help.html)