Fri, 29 Jul 2016 16:15:26 -0400

DRAFT NIST Special Publication 800-63B

Digital Authentication Guideline

Authentication and Lifecycle Management

Paul A. Grassi

Elaine M. Newton

Ray A. Perlner

Andrew R. Regenscheid

William E. Burr

James L. Fenton

Justin P. Richer

COMPUTER SECURITY

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

DRAFT NIST Special Publication 800-63B

Digital Authentication Guideline

Authentication and Lifecycle Management

Paul A. Grassi

Applied Cybersecurity Division

Information Technology Laboratory

Elaine M. Newton

Office of the Director

Information Technology Laboratory

Ray A. Perlner

Computer Security Division

Information Technology Laboratory

Andrew R. Regenscheid

Computer Security Division

Information Technology Laboratory

William E. Burr

Dakota Consulting, Inc.

Silver Spring, MD

James L. Fenton

Altmode Networks

Los Altos, CA

Justin P. Richer

Bespoke Engineering

Billerica, MA

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 800-63B
Natl. Inst. Stand. Technol. Spec. Publ. 800-63B, 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 document and its companion documents, SP 800-63-3, SP 800-63A, and SP 800-63C, provide technical and procedural guidelines to agencies implementing electronic authentication to choose and implement effective authentication processes based on risk. 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 the three authenticator assurance levels. This publication supersedes corresponding sections of NIST SP 800-63-1 and SP 800-63-2.

Keywords

authentication; credential service provider; digital authentication; digital credentials; electronic authentication; electronic credentials.

Acknowledgements

The authors would like to acknowledge the thought leadership and innovation of the original authors: Donna F. Dodson, 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 that a given claimant is the same as a subscriber that has previously authenticated. The robustness of this confidence is described by categorization known as the Authenticator Assurance Level (AAL). The separation of AAL from Identity Assurance Level (IAL), described in SP 800-63A, better supports applications requiring strong authentication that may be pseudonomymous. The separation of authenticator issuance from the establishment of credentials binding those authenticators to individuals provides additional flexibility in the enrollment and identity proofing process.

This guideline addresses how an individual, known as a claimant, can securely authenticate to a Credential Service Provider to establish the context for a remote digital interaction.

The three AALs reflect the options agencies will select based on their risk profile and the potential harm caused by an invalid or fraudulent user accessing their systems. The AALs are as follows:

AAL 1: AAL 1 requires single factor authentication, giving some assurance that the same claimant who participated in previous transactions is accessing the protected transaction or data.

AAL 2: AAL 2 requires two different authentication factors, providing higher assurance that the same claimaint who participated in previous transactions is accessing the protected transaction or data.

AAL 3: AAL 3 provides the highest practical remote digital authentication assurance. It requires proof of possession of a key in a physical multifactor authenticator through a cryptographic protocol.

Table of Contents

1. Purpose

This recommendation and its companion documents, SP 800-63-3 (sp800-63-3.html), SP 800-63A (sp800-63a.html), and SP 800-63C (sp800-63c.html), provide technical guidelines to credential service providers for the implementation of digital authentication.

2. Introduction

Digital authentication is the process of establishing confidence in user identities electronically presented to an information system. E-authentication presents a technical challenge when this process involves the digital authentication of individual people over a network.

The ongoing authentication of subscribers is central to this process. Subscriber authentication is performed by verifying that the claimant controls one or more *authenticators* (called *tokens* in earlier editions of SP 800-63) associated with a given subscriber. A successful authentication results in the assertion of an identifier, either pseudonymous or non-pseudonymous, and optionally other identity information, to the relying party (RP).

This document provides guidance on types of authentication processes, including choices of authenticators, that may be used at various *Authenticator Assurance Levels* (AAL). It also provides guidance on the lifecycle of authenticators, including revocation in the event of loss or theft.

These technical guidelines apply to digital authentication of human users to IT systems over a network. They do not primarily address the authentication of a person who is physically present, for example, for access to buildings, although some credentials that are used remotely may also be used in local authentication. These technical guidelines also 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 to machines and servers when they are used in e-authentication protocols with people.

The strength of an authentication transaction is characterized by a categorization known as the AAL. A high-level summary of the technical requirements for each of the authenticator assurance levels is provided below; see Section 4 and 5 of this document for specific normative requirements.

Authenticator Assurance Level 1 - AAL 1 provides single factor 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, therefore allowing CSPs to allow users to use a higher AAL authenticator to be at AAL 1. 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. At least two different authentication factors SHALL be used. AAL 2 also permits any of the authentication methods of AAL 3 for the same reasons as AAL 1. 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 SHALL be used at AAL 2 and above.

Authentication Assurance Level 3 – AAL 3 is intended to provide the highest practical remote network authentication assurance. Authentication at AAL 3 is based on proof of possession of a key in a physical authenticator through a cryptographic protocol. AAL 3 is similar to AAL 2 except that only multifactor hardware cryptographic authenticators are allowed. The authenticator SHALL 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.

3. Definitions and Abbreviations

There is a variety of terms used in the area of authentication. While the definitions of many terms are consistent with the original version 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.

Active Attack

An attack on the authentication protocol 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.

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.

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 defeat security controls. For example, 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.)

Authenticated Protected Channel

A communication channel that uses approved encryption where the initiator of the connection (client) has authenticated the recipient (server). Authenticated protected channels provide confidentiality and man-in-the-middle protection and are frequently used in the user authentication process. TLS [BCP 195] is an example of an authenticated protected channel when the certificate presented by the recipient is verified by the initiator.

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. Secure authentication protocols also demonstrate 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.

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.

Biometrics

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

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

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.

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.

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 their identity.

Credential Service Provider (CSP)

A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. The CSP may encompass 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 one or more authenticators 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.

Equal Error Rate (EER)

The value where the false match rate (FMR) and false non-match rate (FNMR) of a sensor are equal. EER is a figure of merit for the sensor; the lower the EER is, the more certain the sensor’s decision is likely to be.

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.

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 offline 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 SHALL 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.

Offline 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).

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 an 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*.

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 the CSP validates the identity of the Applicant.

Relying Party (RP)

An entity that relies upon the subscriber's authenticator 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)

See *Transport Layer Security (TLS)*.

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

A persistent interaction between a subscriber and an endpoint, either an RP or a CSP. A session begins with an authentication event and ends with a session termination event. A session is bound by use of a session secret that the subscriber's software (a browser, application, or OS) can present to the RP or CSP in lieu of the subscriber's authentication credentials.

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.

Side Channel Attack

An attack enabled by leakage of information from a physical cryptosystem. Timing, power consumption, electromagnetic and acoustic emissions are examples of characteristics that could be exploited in a side-channel attack.

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 are bound to a subscriber in a tamper-evident fashion.

Subscriber

A party who has received a credential bound to an 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).

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 subscriber to the real verifier.

Weakly Bound Credentials

Credentials that are bound to a subscriber 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. Authenticator Assurance Levels

In order to satisfy the requirements of a given Authenticator Assurance Level (AAL), a claimant SHALL authenticate themselves with at least a given level of strength to be recognized as a subscriber. The result of an authentication process is an identifier, that MAY be pseudonymous, that SHALL be used each time that subscriber authenticates to that relying party. Optionally, other attributes that identify the subscriber as a unique person may also be provided.

Detailed normative requirements for authenticators and verifiers at each AAL are provided in Section 5.

FIPS 140 requirements are satisfied by [FIPS 140-2] or newer revisions.

The following table shows the required AAL per M-04-04 Level of Assurance. Agencies SHALL select the corresponding AAL based on the assessed M-04-04 LOA.

Level of Assurance	Authenticator Assurance Level
1	1, 2 or 3
2	2 or 3
3	2 or 3
4	3

4.1. Authenticator Assurance Level 1

AAL 1 provides single factor remote network 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.

4.1.1. Permitted Authenticator Types

Authenticator Assurance Level 1 permits the use of any of the following authenticator types, defined in Section 5:

- Memorized Secret
- Look-up Secret
- Out of Band (Partially deprecated; see Section 5.1.3 for more details)
- Single Factor OTP Device
- Multi-Factor OTP Device
- Single Factor Cryptographic Device
- Multi-Factor Software Cryptographic Authenticator
- Multi-Factor Cryptographic Device

4.1.2. Authenticator and Verifier Requirements

Cryptographic authenticators used at AAL 1 SHALL use approved cryptography.

Verifiers operated by government agencies at AAL 1 SHALL be validated to meet the requirements of [FIPS 140] Level 1.

4.1.3. Assertion Requirements

In order to be valid at AAL 1, authentication assertions SHALL meet the requirements defined in SP 800-63C (sp800-63c.html). Bearer assertions MAY be used.

4.1.4. Reauthentication

At AAL 1, reauthentication of the subscriber SHOULD be repeated at least once per 30 days, regardless of user activity.

4.1.5. Security Controls

The CSP SHOULD employ appropriately tailored security controls from the low baseline of security controls defined in [SP 800-53] or equivalent industry standard and SHOULD ensure that the minimum assurance requirements associated with the *low* baseline are satisfied.

4.1.6. Records Retention

The CSP shall comply with their respective records retention policies in accordance with whatever laws and/or regulations apply. Otherwise, no retention period is required.

4.2. 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. At least two different authentication factors are required. Various types of authenticators, including multi-factor software cryptographic authenticators, may be used as described below. 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 against verifier impersonation attacks. Approved cryptographic techniques are required at AAL 2 and above.

4.2.1. Permitted Authenticator Types

At AAL 2, it is required to have (a) a multi-factor authenticator, or (b) a combination of two single-factor authenticators. Authenticator requirements are specified in Section 5.

When a multi-factor authenticator is used, any of the following may be used:

- Multi-Factor OTP Device
- Multi-Factor Software Cryptographic Authenticator
- Multi-Factor Cryptographic Device

When a combination of two single-factor authenticators is used, it SHALL include a Memorized Secret authenticator and one possession-based (“something you have”) authenticator from the following list:

- Look-up Secret
- Out of Band
- Single Factor OTP Device
- Single Factor Cryptographic Device

> Note: The requirement for a memorized secret authenticator above derives from the need for two different types of authentication factors to be used. All biometric authenticators compliant with this specification are multi-factor, so something you know (a memorized secret) is the remaining possibility.

4.2.2. Authenticator and Verifier Requirements

Cryptographic authenticators used at AAL 2 SHALL use approved cryptography. Authenticators developed by government agencies SHALL be validated to meet the requirements of [FIPS 140] Level 1.

Verifiers operated by government agencies at AAL 2 SHALL be validated to meet the requirements of [FIPS 140] Level 1.

4.2.3. Assertion Requirements

In order to be valid at AAL 2, authentication assertions SHALL meet the requirements defined in SP 800-63C (sp800-63c.html). Bearer assertions MAY be used.

4.2.4. Reauthentication

At AAL 2, authentication of the subscriber SHALL be repeated at least once per 12 hours, regardless of user activity. Reauthentication of the subscriber SHALL be repeated following no more than 30 minutes of user inactivity. The CSP MAY prompt the user to cause activity just before the inactivity timeout, if desired. Reauthentication MAY use a single authentication factor.

4.2.5. Security Controls

The CSP SHOULD employ appropriately tailored security controls from the moderate baseline of security controls defined in [SP 800-53] or equivalent industry standard and SHOULD ensure that the minimum assurance requirements associated with the *moderate* baseline are satisfied.

4.2.6. Records Retention

CSPs shall comply with their respective records retention policies in accordance with whatever laws and/or regulations apply to those entities. Otherwise, retention of records is required for seven years and 6 months.

4.3. Authenticator Assurance Level 3

AAL 3 is intended to provide the highest practical remote network 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.

4.3.1. Permitted Authenticator Types

Authentication Assurance Level 3 requires the use of one of three kinds of hardware devices:

- Multi-Factor OTP Device
- Multi-Factor Cryptographic Device
- Single-Factor Cryptographic Device used in conjunction with Memorized Secret

4.3.2. Authenticator and Verifier Requirements

Multi-factor authenticators used at AAL 3 SHALL be hardware cryptographic modules validated at [FIPS 140] Level 2 or higher overall with at least [FIPS 140] Level 3 physical security. Single-factor cryptographic devices used at AAL 3 SHALL be validated at [FIPS 140] Level 1 or higher overall with at least [FIPS 140] Level 3 physical security. These requirements CAN be met by using the PIV authentication key of a [FIPS 201] compliant Personal Identity Verification (PIV) Card.

Verifiers at AAL 3 SHALL be validated at [FIPS 140] Level 1 or higher.

4.3.3. Assertion Requirements

In order to be valid at AAL 3, authentication assertions SHALL meet the requirements of proof-of-possession assertions as defined in SP 800-63C (sp800-63c.html).

4.3.4. Reauthentication

At AAL 3, authentication of the subscriber SHALL be repeated at least once per 12 hours, regardless of user activity. Reauthentication of the subscriber SHALL be repeated following a period of no more than 15 minutes of user inactivity. Reauthentication SHALL use both factors. The verifier MAY prompt the user to cause activity just before the inactivity timeout.

4.3.5. Security Controls

The CSP SHOULD employ appropriately tailored security controls from the high baseline of security controls defined in [SP 800-53] or an equivalent industry standard and SHOULD ensure that the minimum assurance requirements associated with the *high* baseline are satisfied.

4.3.6. Records Retention

The CSP shall comply with their respective records retention policies in accordance with whatever laws and/or regulations apply to those entities. Otherwise, retention of records is required for ten years and 6 months.

4.4. Summary of Requirements

(Non-normative; refer to preceding sections for normative requirements)

The following table summarizes the requirements for each of the authenticator assurance levels:

Requirement	AAL 1	AAL 2	AAL 3
Permitted authenticator types	Memorized Secret Look-up Secret Out of Band SF OTP Device MF OTP Device SF Cryptographic Device MF Software Cryptographic Authenticator MF Cryptographic Device	MF OTP Device MF Software Cryptographic Authenticator MF Cryptographic Device or memorized secret plus: Look-up Secret Out of Band SF OTP Device SF Cryptographic Device	MF OTP Device MF Cryptographic Device SF Cryptographic Device plus Memorized Secret

FIPS 140 verification	Level 1 (Government agency verifiers)	Level 1 (Government agency authenticators and verifiers)	Level 2 overall (MF authenticators) Level 1 overall (verifiers and SF Crypto Devices) Level 3 physical security (all authenticators)
Assertions	Bearer or proof of possession	Bearer or proof of possession	Proof of possession only
Reauthentication	30 days	12 hours or 30 minutes inactivity; may use one authentication factor	12 hours or 15 minutes inactivity; shall use both authentication factors
Security Controls	[SP 800-53] Low Baseline (or equivalent)	[SP 800-53] Moderate Baseline (or equivalent)	[SP 800-53] High Baseline (or equivalent)
Records Retention	Not required	7 years, 6 months	10 years, 6 months

5. Authenticator and Verifier Requirements

This section provides the detailed requirements specific for each of the authenticator types. With the exception of validation requirements specified in Section 4, the technical requirements for each of the authenticator types is the same regardless of the AAL at which it is used.

5.1. Requirements by Authenticator Type

5.1.1. Memorized Secrets

A Memorized Secret authenticator (commonly referred to as a *password* or *PIN* if it is numeric) is a secret value that is intended to be chosen and memorizable by the user. Memorized secrets need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value.

5.1.1.1. Memorized Secret Authenticators

Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber; memorized secrets chosen randomly by the CSP or verifier SHALL be at least 6 characters in length and MAY be entirely numeric. Some values for user-chosen memorized secrets may be disallowed based on their appearance on a blacklist of compromised values. No other complexity requirements for memorized secrets are imposed; a rationale for this is presented in Appendix A.

5.1.1.2. Memorized Secret Verifiers

Verifiers SHALL require subscriber-chosen memorized secrets to be at least 8 characters in length. Verifiers SHALL permit user-chosen memorized secrets to be at least 64 characters in length. All printing ASCII [RFC 20] characters as well as the space character SHALL be acceptable in memorized secrets; Unicode [ISO/ISC 10646:2014] characters SHOULD be accepted as well. Verifiers MAY remove space characters prior to verification; all other characters SHALL be considered significant. Truncation of the secret SHALL NOT be performed. For purposes of the above length requirements, each Unicode code point SHALL be counted as a single character.

Memorized secrets that are randomly chosen by the CSP (e.g., at enrollment) or by the verifier (e.g., when a user requests a new PIN) SHALL be at least 6 characters in length and SHALL be generated using an approved random number generator.

Memorized secret verifiers SHALL NOT permit the subscriber to store a “hint” that is accessible to an unauthenticated claimant. Verifiers also SHALL NOT prompt subscribers to use specific types of information (e.g., “What was the name of your first pet?”) when choosing memorized secrets.

When processing requests to establish and change memorized secrets, verifiers SHOULD compare the prospective secrets against a dictionary of known commonly-used and/or compromised values. This list SHOULD include passwords from previous breach corpuses, as well as dictionary words and specific words (such as the name of the service itself) that users are likely to choose. If the chosen secret is found in the dictionary, the subscriber SHOULD be required to choose a different value. The subscriber SHOULD be advised that they need to select a different secret because their previous choice was commonly used.

Verifiers SHALL implement a throttling mechanism that effectively limits the number of failed authentication attempts an attacker can make on the subscriber’s account as described in Section 5.2.2.

Verifiers SHOULD NOT impose other composition rules (mixtures of different character types, for example) on memorized secrets. Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically) unless there is evidence of compromise of the authenticator or a subscriber requests a change.

In order to assist the claimant in entering a memorized secret successfully, the verifier SHOULD offer an option to display the secret (rather than a series of dots or asterisks, typically) as it is typed. The verifier SHALL hide the character after it is displayed for a time sufficient for the claimant to see the character. This allows the claimant to verify their entry if they are in a location where their screen is unlikely to be observed.

Verifiers SHALL use approved encryption and SHALL authenticate themselves to the claimant (e.g., through the use of a X.509 certificate using approved encryption that is acceptable to the claimant) when requesting memorized secrets in order to provide resistance to eavesdropping and phishing attacks.

Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks. Secrets SHALL be hashed with a *salt* value using an approved hash function such as PBKDF2 as described in [SP800-132]. The salt value SHALL be a 32 bit (or longer) random value generated by an approved random number generator and is stored along with the hash result. At least 10,000 iterations of the hash function SHOULD be performed. A keyed hash function (e.g., HMAC), with the key stored separately from the hashed authenticators (e.g., in a hardware security module) SHOULD be used to further resist dictionary attacks against the stored hashed authenticators.

5.1.2. Look-up Secrets

A look-up secret authenticator is a physical or electronic record that stores a set of secrets shared between the claimant and the CSP. The claimant uses the authenticator to look up the appropriate secret(s) needed to respond to a prompt from the verifier. For example, a claimant may be asked by the verifier to provide a specific subset of the numeric or character strings printed on a card in table format.

5.1.2.1 Look-up Secret Authenticators

CSPs creating look-up secret authenticators SHALL use an approved random number generator to generate the list of secrets, and SHALL deliver the authenticator securely to the subscriber. Look-up secrets SHALL have at least 64 bits of entropy, or SHALL have at least 20 bits of entropy if the number of failed authentication attempts is limited as described in Section 5.2.2.

If the authenticator uses look-up secrets sequentially from a list, the subscriber MAY dispose of used secrets, but only after a successful authentication.

5.1.2.2. Look-up Secret Verifiers

Verifiers of look-up secrets SHALL prompt the claimant for the next secret from their authenticator or for a specific (i.e., numbered) secret. A given secret from an authenticator SHALL be used successfully only once; therefore, a given authenticator can only be used for a finite number of successful authentications. If the look-up secret is derived from a grid card, each cell of the grid SHALL be used only once.

Verifiers SHALL store look-up secrets in a form that is resistant to offline attacks. Secrets SHALL be hashed with a “salt” value using an approved hash function as described in [SP 800-132]. The “salt” value SHALL be a 32 bit (or longer) random value generated by an approved random number generator that is stored along with the hash result. A keyed hash function (e.g., HMAC [FIPS198-1]), with the key stored separately from the hashed authenticators (e.g., in a hardware security module) SHOULD be used to further resist dictionary attacks against the stored hashed authenticators.

Look-up secrets SHALL be generated using an approved random number generator and SHALL have at least 20 bits of entropy. When look-up secrets have less than 64 bits of entropy, the verifier SHALL implement a throttling mechanism that effectively limits the number of failed authentication attempts an attacker can make on the subscriber’s account as described in Section 5.2.2.

Verifiers SHALL use approved encryption and SHALL authenticate themselves to the claimant (e.g., through the use of a X.509 certificate using approved encryption that is acceptable to the claimant) when requesting look-up secrets in order to provide resistance to eavesdropping and phishing attacks.

5.1.3. Out of Band

> An Out of Band authenticator is a physical device that is uniquely addressable and can receive a verifier-selected secret for one-time use. The device is possessed and controlled by the claimant and supports private communication over a secondary channel that is separate from the primary channel for e-authentication. The out-of-band authenticator can operate in one of two ways:
>
> - The claimant presents the secret that was received by the out-of-band authenticator to the verifier using the primary channel for e-authentication.
>
> - The claimant sends a response to the verifier from the out-of-band authenticator via the secondary communications channel
>
> Two key requirements are that the device be uniquely addressable and that communication over the secondary channel be private. Some voice-over-IP

telephone services can deliver text messages and voice calls without the need for possession of a physical device; these SHALL NOT be used for out of band authentication. Mechanisms such as smartphone applications employing secure communications protocols are preferred for out-of-band authentication.

If the authenticator responds directly to the verifier via the secondary communications channel, the verifier SHALL send and the authenticator SHALL display information, such as a transaction ID or description, allowing the claimant to uniquely associate the authentication operation on the primary channel with the request on the secondary channel.

Ability to receive email messages or other types of instant message does not generally prove the possession of a specific device, so they SHALL NOT be used as out of band authentication methods.

5.1.3.1. Out of Band Authenticators

The out of band authenticator SHALL establish an authenticated protected channel in order to retrieve the out of band secret or authentication request. This channel is considered to be out of band with respect to the primary communication channel, even if it terminates on the same device, provided the device does not leak information from one to the other.

The out of band authenticator SHALL uniquely authenticate itself in one of the following ways in order to receive the authentication secret:

- Authentication to the verifier using approved cryptography. The key SHOULD be stored in the most secure storage available on the device (e.g., keychain storage, trusted platform module, or trusted execution environment if available).
- Authentication to a public mobile telephone network using a SIM card or equivalent that uniquely identifies the device

Out of band authenticators SHOULD NOT display the authentication secret on a device that is locked by the owner (i.e., requires an entry of a PIN or passcode). However, authenticators MAY indicate the receipt of an authentication secret on a locked device.

If the out of band authenticator sends an approval message over the secondary communication channel (rather than by the claimant transferring a received secret to the primary communication channel):

- The authenticator SHALL display identifying information about the authentication transaction to the claimant prior to their approval.

- The secondary communication channel SHALL be an authenticated protected channel.

5.1.3.2. Out of Band Verifiers

Out of band verifiers SHALL generate a random authentication secret with at least 20 bits of entropy using an approved random number generator. They then optionally signal the device containing the subscriber's authenticator to indicate readiness to authenticate.

Due to the risk that SMS messages may be intercepted or redirected, implementers of new systems SHOULD carefully consider alternative authenticators. If the out of band verification is to be made using a SMS message on a public mobile telephone network, the verifier SHALL verify that the pre-registered telephone number being used is actually associated with a mobile network and not with a VoIP (or other software-based) service. It then sends the SMS message to the pre-registered telephone number. Changing the pre-registered telephone number SHALL NOT be possible without two-factor authentication at the time of the change. **OOB using SMS is deprecated**, and may no longer be allowed in future releases of this guidance.

If out of band verification is to be made using a secure application (e.g., on a smart phone), the verifier MAY send a push notification to that device. The verifier then waits for a establishment of an authenticated protected channel and verifies the authenticator's identifying key. The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method such as hashing (using an approved hash function) or proof of possession of the identifying key to uniquely identify the authenticator. Once authenticated, the verifier transmits the authentication secret to the authenticator. Depending on the type of out-of-band authenticator, either: * The verifier waits for the secret to be returned on the primary communication channel.

- The verifier waits for the secret, or some type of approval message, to be returned over the secondary communication channel.

If approval is made over the secondary communication channel, the request to the verifier SHALL include a transaction identifier, such as a transaction ID or description, for display by the verifier.

In collecting the authentication secret from the claimant, the verifier SHALL use approved encryption and SHALL authenticate itself to the claimant. The authentication secret SHALL be considered invalid if not received within 5 minutes.

If the authentication secret has less than 64 bits of entropy, the verifier SHALL implement a throttling mechanism that effectively limits the number of failed authentication attempts an attacker can make on the subscriber's account as described in Section 5.2.2.

5.1.4. Single Factor OTP Device

A single factor OTP device is a hardware device that supports the time-based generation of one-time passwords. This includes software-based OTP generators installed on devices such as mobile phones. This device has an embedded secret that is used as the seed for generation of one-time passwords and does not require activation through a second factor. Authentication is accomplished by using the authenticator output (i.e., the one-time password) in an authentication protocol, thereby proving possession and control of the device. A one-time password device may, for example, display 6 characters at a time.

Single factor OTP devices are similar to look-up secret authenticators with the exception that the secrets are cryptographically generated by the authenticator and verifier and compared by the verifier. The secret is computed based on a nonce that may be time-based or from a counter on the authenticator and verifier.

5.1.4.1. Single Factor OTP Authenticators

Single factor OTP authenticators contain two persistent values. The first is a symmetric key that persists for the lifetime of the device. The second is a nonce that is changed each time the authenticator is used or is based on a real-time clock.

The secret key SHALL be of at least the minimum approved length as defined in the latest revision of [SP 800-131A] (currently 112 bits). The nonce SHALL be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.

The authenticator output is obtained by using an approved block cipher or hash function to combine the key and nonce in a secure manner. The authenticator output MAY be truncated to as few as 6 decimal digits (approximately 20 bits of entropy).

If the nonce used to generate the authenticator output is based on a real-time clock, the nonce SHALL be changed at least once every 2 minutes. The OTP value associated with a given nonce SHALL be accepted only once.

If the authenticator supplies its output via an electronic interface such as USB, it SHOULD require a physical input (e.g., pressing a button on the device) to cause a one-time password to be generated.

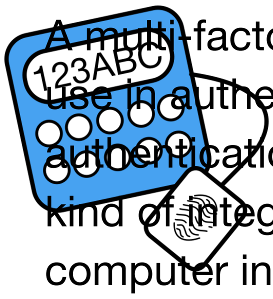
5.1.4.2. Single Factor OTP Verifiers

Single factor OTP verifiers effectively duplicate the process of generating the OTP used by the authenticator. As such, the symmetric keys used by authenticators are also present in the verifier, and SHALL be strongly protected against compromise.

In collecting the OTP from the claimant, the verifier SHALL use approved encryption and SHALL authenticate itself to the claimant.

If the authenticator output has less than 64 bits of entropy, the verifier SHALL implement a throttling mechanism that effectively limits the number of failed authentication attempts an attacker can make on the subscriber’s account as described in Section 5.2.2.

5.1.5. Multi-Factor OTP Devices



A multi-factor (MF) OTP device hardware device generates one-time passwords for use in authentication and requires activation through a second factor of authentication. The second factor of authentication may be achieved through some kind of integral entry pad, an integral biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port). The one-time password is typically displayed on the device and manually input to the verifier, although direct electronic output from the device as input to a computer is also allowed. For example, a one-time password device may display 6 characters at a time. The MF OTP device is *something you have*, and it may be activated by either *something you know* or *something you are*.

5.1.5.1. Multi-Factor OTP Authenticators

Multi-factor OTP authenticators operate in a similar manner to single-factor OTP authenticators (see Section 5.1.4.1), except that they require the entry of either a memorized secret or use of a biometric to obtain a password from the authenticator. Each use of the authenticator SHALL require the input of the additional factor.

The authenticator output SHALL have at least 6 decimal digits (approximately 20 bits) of entropy. The output SHALL be generated by using an approved block cipher or hash function to combine a symmetric key stored on a personal hardware device with a nonce to generate a one-time password. The nonce MAY be based on the date and time or on a counter generated on the device.

Any memorized secret used by the authenticator for activation SHALL be at least 6 decimal digits (approximately 20 bits) in length or of equivalent complexity. A biometric activation factor SHALL meet the requirements of Section 5.2.3, including limits on number of successive authentication failures.

The unencrypted key and activation secret or biometric sample (and any biometric data derived from the biometric sample such as a probe produced through signal processing) SHALL be immediately erased from storage immediately after a password has been generated.

5.1.5.2. Multi-Factor OTP Verifiers

Multi-factor OTP verifiers effectively duplicate the process of generating the OTP used by the authenticator, but without the requirement that a second factor be provided. As such, the symmetric keys used by authenticators SHALL be strongly protected against compromise.

In collecting the OTP from the claimant, the verifier SHALL use approved encryption and SHALL authenticate itself to the claimant. Time-based one-time passwords SHALL have a lifetime of less than 2 minutes.

If the authenticator output or activation secret has less than 64 bits of entropy, the verifier SHALL implement a throttling mechanism that effectively limits the number of failed authentication attempts an attacker can make on the subscriber's account as described in Section 5.2.2. A biometric activation factor SHALL meet the requirements of Section 5.2.3, including limits on number of successive authentication failures.

5.1.6. Single Factor Cryptographic Devices

> A single-factor cryptographic device is a hardware device that performs cryptographic operations on input provided to the device. This device does not require activation through a second factor of authentication. This device uses embedded symmetric or asymmetric cryptographic keys. Authentication is accomplished by proving possession of the device. The authenticator output is highly dependent on the specific cryptographic device and protocol, but it is generally some type of signed message.

5.1.6.1. Single Factor Cryptographic Device Authenticators

Single-factor cryptographic device authenticators encapsulate a secret key that is unique to the device and SHALL NOT be exportable (removed from the device). They operate by signing a challenge nonce, usually presented through a direct computer interface such as a USB port.

The secret key SHALL be of at least the minimum approved length as defined in the latest revision of [SP 800-131A] (currently 112 bits). The challenge nonce SHALL be at least 64 bits in length. The authenticator output is normally provided via a computer interface (usually the same one from which the challenge value was received).

Single-factor cryptographic device authenticators SHOULD require a physical input such as the pressing of a button in order to operate. This provides defense against unintended operation of the device, which might occur if the device to which it is connected is compromised.

5.1.6.2. Single Factor Cryptographic Device Verifiers

Single-factor cryptographic device verifiers generate a challenge nonce, send it to the corresponding authenticator, and use the authenticator output to verify possession of the device. The authenticator output is highly dependent on the specific cryptographic device and protocol, but it is generally some type of signed message.

The verifier contains either symmetric or asymmetric public keys corresponding to each authenticator. While both types of keys SHALL be protected against modification, symmetric keys SHALL additionally be strongly protected against unauthorized disclosure.

The challenge nonce SHALL be at least 64 bits in length, and SHALL either be unique over the lifetime of the authenticator or statistically unique (generated using an approved random number generator).

5.1.7. Multi-Factor Cryptographic Software

> A multi-factor software cryptographic authenticator is a cryptographic key is stored on disk or some other “soft” media that requires activation through a second factor of authentication. Authentication is accomplished by proving possession and control of the key. The authenticator output is highly dependent on the specific cryptographic protocol, but it is generally some type of signed message. The MF software cryptographic authenticator is *something you have*, and it may be activated by either *something you know* or *something you are*.

5.1.7.1. Multi-Factor Cryptographic Software Authenticators

Multi-factor software cryptographic authenticators encapsulate a secret key that is unique to the authenticator and is accessible only through the input of an additional factor, either a memorized secret or a biometric. The key SHOULD be stored in the most secure storage available on the device (e.g., keychain storage, trusted platform module, or trusted execution environment if available).

Each authentication operation using the authenticator SHALL require the input of the additional factor.

Any memorized secret used by the authenticator for activation SHALL be at least 6 decimal digits (approximately 20 bits) in length or of equivalent complexity. A biometric activation factor SHALL meet the requirements of Section 5.2.3, including limits on number of successive authentication failures.

The unencrypted key and activation secret or biometric sample (and any biometric data derived from the biometric sample such as a probe produced through signal processing) SHALL be immediately erased from storage immediately after an authentication transaction has taken place.

5.1.7.2. Multi-Factor Cryptographic Software Verifiers

The requirements for a multi-factor cryptographic software verifier are identical to those for a multi-factor cryptographic device verifier, described in Section 5.1.8.2.

5.1.8. Multi-Factor Cryptographic Devices

> A multi-factor cryptographic device is a hardware device that contains a protected cryptographic key that requires activation through a second authentication factor. Authentication is accomplished by proving possession of the device and control of the key. The authenticator output is highly dependent on the specific cryptographic device and protocol, but it is generally some type of signed message. The MF Cryptographic device is *something you have*, and it may be activated by either *something you know* or *something you are*.

5.1.8.1. Multi-Factor Cryptographic Device Authenticators

Multi-factor cryptographic device authenticators use tamper-resistant hardware to encapsulate a secret key that is unique to the authenticator and is accessible only through the input of an additional factor, either a memorized secret or a biometric.

Each authentication operation using the authenticator SHOULD require the input of the additional factor. Input of the additional factor MAY be accomplished via either direct input on the device or via a hardware connection (e.g., USB or smartcard).

Any memorized secret used by the authenticator for activation SHALL be at least 6 decimal digits (approximately 20 bits) in length or of equivalent complexity. A biometric activation factor SHALL meet the requirements of Section 5.2.3, including limits on number of successive authentication failures.

The unencrypted key and activation secret or biometric sample (and any biometric data derived from the biometric sample such as a probe produced through signal processing) SHALL be immediately erased from storage immediately after an authentication transaction has taken place.

5.1.8.2 Multi-Factor Cryptographic Device Verifiers

Multi-factor cryptographic device verifiers generate a challenge nonce, send it to the corresponding authenticator, and use the authenticator output to verify possession of the device and activation factor. The authenticator output is highly dependent on the specific cryptographic device and protocol, but it is generally some type of signed message.

The verifier contains either symmetric or asymmetric public keys corresponding to each authenticator. While both types of keys SHALL be protected against modification, symmetric keys SHALL additionally be strongly protected against unauthorized disclosure.

The challenge nonce SHALL be at least 64 bits in length, and SHALL either be unique over the lifetime of the authenticator or statistically unique (generated using an approved random number generator). The verification operation SHALL use approved cryptography.

5.2. General Authenticator Requirements

5.2.1. Physical Authenticators

CSPs SHALL provide subscriber instructions on how to appropriately protect the authenticator against theft or loss. The CSP SHALL provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected.

5.2.2. Rate Limiting (Throttling)

cf. 800-63-2 sec 8.2.3, p.75

When the authenticator output or activation secret does not have sufficient entropy, the verifier SHALL implement controls to protect against online guessing attacks. Unless otherwise specified in the description of a given authenticator, the verifier SHALL effectively limit online attackers to 100 consecutive failed attempts on a single account in any 30 day period.

Additional techniques MAY be used to prioritize authentication attempts that are likely to come from the subscriber over those that are more likely to come from an attacker:

- Requiring the claimant to complete a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) before attempting authentication

- Requiring the claimant to wait for a short period of time (anything from 30 seconds to an hour, depending on how close the system is to its maximum allowance for failed attempts) before attempting Authentication following a failed attempt
- Only accepting authentication requests from a white list of IP addresses at which the subscriber has been successfully authenticated before
- Leveraging other risk-based or adaptive authentication techniques to identify user behavior that falls within, or out of, typical norms.

Since these measures often create user inconvenience, the verifier SHOULD allow a certain number of failed authentication attempts before employing the above techniques.

When the subscriber successfully authenticates, the verifier SHOULD disregard any previous failed attempts from the same IP address.

5.2.3. Use of Biometrics

For a variety of reasons, this document supports only limited use of biometrics for authentication. These include:

- Biometric False Match Rates (FMR) and False Non-Match Rates (FNMR) do not provide confidence in the authentication of the subscriber by themselves. In addition, FMR and FNMR do not account for spoofing attacks.
- Biometric matching is probabilistic, whereas the other authentication factors are deterministic.
- Biometric template protection schemes provide a method for revoking biometric credentials that are comparable to other authentication factors (e.g., PKI certificates and passwords). However, the availability of such solutions is limited, and standards for testing these methods are under development.
- Biometric characteristics do not constitute secrets. They can be obtained online or by taking a picture of someone with a camera phone (e.g. facial images) with or without their knowledge, lifted from through objects someone touches (e.g., latent fingerprints), or captured with high resolution images (e.g., iris patterns for blue eyes). While presentation attack detection (PAD) technologies such as liveness detection can mitigate the risk of these types of attacks, additional trust in the sensor is required to ensure that PAD is operating properly in accordance with the needs of the CSP and the subscriber.

Therefore, the use of biometrics for authentication is supported, with the following requirements and guidelines:

Biometrics SHALL be used with another authentication factor (something you know or something you have).

Testing of the biometric system to be deployed SHALL demonstrate an equal error rate of **1 in 1000** or better with respect to matching performance. The biometric system SHALL operate with a false match rate of **1 in 1000** or better.

When the biometric sensor and subsequent processing are not part of an integral unit that resists replacement of the sensor, the sensor SHALL demonstrate that it is a certified or qualified sensor meeting these requirements by authenticating itself to the processing element.

Testing of the biometric system to be deployed SHALL demonstrate at least 90% resistance to presentation attacks for each relevant attack type (aka species), where resistance is defined as the number of thwarted presentation attacks divided by the number of trial presentation attacks. The biometric system SHALL implement presentation attack protection (PAD).

The biometric system SHALL allow no more than 10 consecutive failed authentication attempts. Once that limit has been reached, the claimant SHALL be required to use a different authenticator or to activate their authenticator with a different factor such as a memorized secret.

Biometric matching SHOULD be performed locally on claimant’s device or MAY be performed at a central verifier.

If matching is performed centrally:

- Use of the biometric SHALL be bound tightly to a single, specific device that is identified using approved cryptography.
- Biometric revocation SHALL be implemented.
- An authenticated protected channel between sensor and central verifier SHALL be established, and the sensor authenticated, **prior** to capturing the biometric sample from the claimant.
- All transmission of biometrics shall be over the authenticated protected channel.

Biometric samples collected in the authentication process MAY be used to train matching algorithms or, with user consent, for other research purposes. Biometric samples (and any biometric data derived from the biometric sample such as a probe produced through signal processing) SHALL be immediately erased from storage immediately after a password has been generated.

Biometrics are also used in some cases to prevent repudiation of registration and to verify that the same individual participates in all phases of the registration process as described in SP 800-63A.

5.2.4 Attestation

Authenticators that are directly connected to or embedded in endpoints MAY convey attestation information such as the provenance or health and integrity of the authenticator (and possibly the endpoint as well) to the verifier as part of the authentication protocol. If this attestation is signed, the verifier SHOULD validate its signature. This information MAY be used as part of a risk-based authentication decision.

When federated authentication is being performed as described in SP 800-63C (sp800-63c.html), the verifier SHOULD include any such attestation information in the assertion it provides to the relying party.

6. Authenticator Lifecycle Management

During the lifecycle of an authenticator bound to a subscriber's identity, a number of events may occur that affect the use of that authenticator. These events include binding, loss, theft, unauthorized duplication, expiration, and revocation. This section describes the actions that SHALL be taken in response to those events.

6.1. Authenticator binding

Authenticators may be provided by a CSP as part of a process such as enrollment; in other cases, the subscriber may provide their own, such as software or hardware cryptographic modules. For this reason, we refer to the *binding* of an authenticator rather than the issuance, but this does not exclude the possibility that an authenticator is issued as well.

Throughout the online identity lifecycle, CSPs SHALL maintain a record of all authenticators that are or have been associated with the identity. It SHALL also maintain the information required for throttling authentication attempts when required, as described in section 5.2.2.

The record created by the CSP SHALL contain the date and time the authenticator was bound to the account and SHOULD include information about the binding, such as the IP address or other device identifier associated with the enrollment. It SHOULD also contain information about unsuccessful authentications attempted with the authenticator.

6.1.1. Enrollment

The following requirements apply when an authenticator is bound to an identity as a result of a successful identity proofing transaction, as described in 800-63-A.

At IAL 2, the CSP SHALL bind at least one, and SHOULD bind at least two, authenticators to the subscriber's online identity. Binding of multiple authenticators is preferred in order to recover from loss or theft of their primary authenticator. While at IAL 1 all identifying information is self-asserted, creation of online material or an online reputation makes it undesirable to lose control of an account as result of the loss of an authenticator. The second authenticator makes it possible to securely recover from that situation.

At IAL 2 and above, identifying information is associated with the online identity and the subscriber has undergone an identity proofing process as described in SP 800-63A. As a result, authenticators at the same AAL as the desired IAL SHALL be bound to the account. For example, if the subscriber has successfully completed proofing at IAL 2, AAL 2 or 3 authenticators are appropriate to bind to the IAL 2 identity. As above, the availability of additional authenticators provides backup methods of authentication if an authenticator is lost or stolen.

Enrollment and binding MAY be broken up into a number of separate physical encounters or electronic transactions. (Two electronic transactions are considered to be separate if they are not part of the same protected session.) In these cases, the following methods SHALL be used to ensure that the same party acts as Applicant throughout the processes:

1. For remote transactions:
    1. The applicant SHALL identify himself/herself in each new transaction by presenting a temporary secret which was established during a prior transaction or encounter, or sent to the Applicant's phone number, email address, or postal address of record.
    2. Permanent secrets shall only be issued to the Applicant within a protected session.

2. For physical transactions:
    1. The applicant SHALL identify himself/herself in person by either using a secret as described above, or through the use of a biometric that was recorded during a prior encounter.
    2. Temporary secrets SHALL not be reused.
    3. If the CSP issues permanent secrets during a physical transaction, then they SHALL be loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record.

6.1.2. Post-Enrollment Binding

Following enrollment, binding an additional authenticator to an account requires the use of an existing authenticator of the same type (or types). For example, binding a new single-factor OTP device requires the subscriber to authenticate with another *something you have* authentication factor. If the account has only one authentication factor bound to it (which is possible only at IAL 1/AAL 1), an additional authenticator of the same factor may be bound to it.

Binding an additional authenticator SHALL require the use of two different authentication factors, except as provided below.

If the subscriber has only one of the two authentication factors, they SHALL repeat the identity proofing process, using the remaining authentication and SHOULD verify knowledge of some information collected during the proofing process to bind to the existing identity. In order to reestablish authentication factors at IAL 3, they SHALL verify the biometric collected during the proofing process.

Consider what proofing information the CSP is allowed to maintain. Privacy impact here?

6.1.3. Binding Identity to a Subscriber Provided Authenticator

In some instances, a claimant may already possess authenticators at a suitable AAL without having been proofed at the equivalent IAL. For example, a user may have a two-factor authenticator from a social network provider, considered AAL2 and IAL1, and would like to use those credentials at a relying party that requires IAL2.

The following requirements apply when a claimant choses to increase IAL in order to bind to a suitable authenticator they already have.

1. The CSP MAY accept an existing authenticator at or above the desired IAL
2. The CSP SHALL require the user to authenticate using their existing authenticator
3. The CSP SHALL execute all required identity proofing processes for the desired IAL
4. If the user successfully completes identity proofing, the CSP MAY issue an enrollment code (temporary secret) that confirms address of record as per 800-63-A, Section 5.3.1, Address Confirmation Requirements (sp800-63a.html#address_confirmation), **OR** MAY request the claimant to register their own authenticator by proving proof of possession (for example, activating a private key by physically touching the token)

6.1.4. Renewal

The CSP SHOULD bind an updated authenticator an appropriate amount of time in advance of an existing authenticator's expiration. The process for this SHOULD conform closely to the initial authenticator issuance process (e.g., confirming address of record, etc.). Following successful use of the new authenticator, the CSP MAY revoke the authenticator that it is replacing.

6.2. Loss, Theft, and Unauthorized Duplication

Loss, theft, and unauthorized duplication of an authenticator are handled similarly, because in most cases one must assume that a lost authenticator has potentially been stolen or recovered by someone that is not the legitimate claimant of the authenticator. One notable exception is when a memorized secret is forgotten without other indication of having been compromised (duplicated by an attacker).

To facilitate secure reporting of loss or theft of an authenticator, the CSP SHOULD provide the subscriber a method to authenticate to the CSP using a backup authenticator; either a memorized secret or a physical authenticator MAY be used for this purpose (only one authentication factor is required for this purpose). Alternatively, the subscriber MAY establish an authenticated protected channel to the CSP and verify information collected during the proofing process. Alternatively, the CSP MAY verify an address of record (email, telephone, or postal) and suspend authenticator(s) reported to have been compromised. The suspension SHALL be reversible if the subscriber successfully authenticates to the CSP and requests reactivation of an authenticator suspended in this manner.

6.3. Expiration

CSP’s SHOULD issue authenticators that expire. When an authenticator expires, it SHALL NOT be usable for authentication. When an authentication is attempted, the CSP SHOULD give an indication to the subscriber that the authentication failure is due to expiration rather than some other cause.

The CSP SHALL require subscribers to surrender any physical authenticator containing trustable attributes as soon as practical after expiration or after receipt of a renewed authenticator.

6.4. Revocation

CSPs SHALL revoke the binding of authenticators promptly when an online identity ceases to exist or when requested by the subscriber.

7. Session Management

Once an authentication event has taken place, it is often desirable to allow the user to continue using the application across multiple subsequent interactions without requiring the user to repeat the authentication event every time. This requirement is particularly true for federation scenarios (described in volume C), where the authentication event necessarily involves several components and actors coordinating across a network.

To facilitate this behavior, a *session* MAY be started in response to an authentication event, and such a session SHALL continue until such time that it is terminated. The session MAY be terminated for any number of reasons, including but not limited to an inactivity timeout, an explicit logout event, or other means. The session MAY be continued through a reauthentication event (described in section 7.2), wherein the user repeats some or all of the initial authentication event, thereby asserting their presence again.

Session management is preferable over continuous presentation of credentials as the usability requirements of such continuous presentation would incentivize workarounds such as cached unlocking credentials, negating the freshness of the authentication event in the first place.

7.1. Session Bindings

A session occurs between the software that a subscriber is running, such as a browser, application, or operating system (the session subject), and the RP or CSP that the subscriber is accessing (the session host). A session secret is shared between the subscriber’s software and the service being accessed. This secret binds the two ends of the session, allowing the user to continue using the service over time. The secret MAY be presented directly by the user's software (a bearer secret) or MAY be proofed using a cryptographic mechanism (a proof of possession secret).

The secret used for session binding SHALL be generated by the session host in direct response to an authentication event. A session SHOULD inherit the AAL properties of the authentication event which triggered its creation; a session MAY be considered at a lower AAL than the authentication event and SHALL NOT be considered at a higher AAL than the authentication event.

Secrets used for session binding:

- SHALL be generated by the session host during an interaction, typically immediately following user authentication
- SHALL contain entropy of at least 64 bits in length generated using an approved random number generator
- SHALL be recorded along with the time of generation by the session subject
- SHALL be erased or invalidated by the session subject when the user logs out
- SHOULD be erased on the user endpoint when the user logs out or when the secret is deemed to have expired
- SHOULD not be placed in insecure locations such as HTML5 Local Storage
- SHALL be sent to and received from the device using an authenticated protected channel
- SHALL time out and not be accepted after the times specified in section 4.1.4, 4.2.4, and 4.3.4 (depending on AAL)

There are several different mechanisms for managing a session over time. The following sections give three examples, along with additional requirements and considerations particular to each example technology.

7.1.1. Browser Cookies

Browser cookies are the predominant mechanism by which a session will be created and tracked for a user accessing a service.

Cookies:

- SHALL be tagged to be accessible on secure (HTTPS) sessions only
- SHALL be accessible to the minimum practical set of hostnames and paths
- SHOULD be tagged to be inaccessible via JavaScript

- SHOULD be tagged to expire at or soon after the validity period of the session (This requirement is intended to limit the accumulation of cookies, but SHALL NOT be depended upon to enforce session timeouts.)

7.1.2. OAuth Tokens

An OAuth access token is be used to allow an application to access a set of services on behalf of a user following an authentication event. The presence of an OAuth access token SHALL NOT be interpreted by the RP to indicate the presence of the user, in the absence of other signals. The OAuth access token (and any associated refresh tokens) MAY be valid long after the authentication session has ended and the user has left the application in question.

7.1.3. Device Identification

Other methods of secure device identification, including but not limited to mutual TLS, token binding, or other mechanisms, MAY be used to enact a session between a user and a service.

7.2. Reauthentication

A session SHALL NOT be extended past the guidelines in sections 4.1.4, 4.2.4, and 4.3.4 (depending on AAL) based on presentation of the session secret alone.

When a session is terminated due to a time-out or other action, the user MAY reauthenticate using their primary authentication mechanism or an appropriate subset thereof, depending on the AAL.

AAL	Requirement
1	Presentation of any one factor
2	Presentation of any one factor
3	Presentation of all factors

7.2.1 Reauthentication from a federation or assertion

When using a federation protocol (sp800-63c#sec4) to connect the CSP and RP, special consideration needs to be made for session management and reauthentication. Both the CSP and RP are likely to employ separate session management technologies, and there

SHALL NOT be any assumption of correlation between these sessions. Consequently, when a session expires at an RP and reauthentication is required by the RP, it is entirely possible that the session at the CSP is not expired and a new assertion could be generated from this session at the CSP without reauthenticating the user. Therefore, an RP requiring a reauthentication through a federation protocol SHALL indicate a minimum acceptable authentication age to the CSP (if possible within the protocol), and the CSP SHALL honor this request (if possible). The CSP in all cases SHALL communicate the primary authentication event time to the RP to allow the RP to decide if the assertion is sufficient for reauthentication or not.

8. Threats and Security Considerations

This section is non-normative.

8.1. Authenticator Threats

An attacker who can gain control of an authenticator will often be able to masquerade as the authenticator's owner. Threats to authenticators can be categorized based on attacks on the types of authentication factors that comprise the authenticator:

- *Something you have* may be lost, damaged, stolen from the owner or cloned by an attacker. For example, an attacker who gains access to the owner's computer might copy a software authenticator. A hardware authenticator might be stolen, tampered with, or duplicated.

- *Something you know* may be disclosed to an attacker. The attacker might guess a memorized secret. Where the authenticator is a shared secret, the attacker could gain access to the CSP or verifier and obtain the secret value or perform a dictionary attack on a hash of that value. An attacker may observe the entry of a PIN or passcode, find a written record or journal entry of a PIN or passcode, or may install malicious software (e.g., a keyboard logger) to capture the secret. Additionally, an attacker may determine the secret through offline attacks on a hashed password database maintained by the verifier.

- *Something you are* may be replicated. An attacker may obtain a copy of the subscriber's fingerprint and construct a replica - assuming that the biometric system(s) employed do not block such attacks by employing robust liveness detection techniques.

This document assumes that the subscriber is not colluding with the attacker who is attempting to falsely authenticate to the verifier. With this assumption in mind, the threats to the authenticator(s) used for e-authentication are listed in Table 4, along with some examples.

Table 4 – Authenticator Threats

Authenticator Threats/Attacks	Description	Examples
Theft	A physical authenticator is stolen by an Attacker.	A hardware cryptographic device is stolen.
		A One-Time Password device is stolen.
		A look-up secret authenticator is stolen.
		A cell phone is stolen.
Duplication	The subscriber's authenticator has been copied with or without their knowledge.	Passwords written on paper are disclosed.
		Passwords stored in an electronic file are copied.
		Software PKI authenticator (private key) copied.
		Look-up secret authenticator copied.
Eavesdropping	The authenticator secret or authenticator output is revealed to the attacker as the subscriber is authenticating.	Memorized secrets are obtained by watching keyboard entry.
		Memorized secrets or authenticator outputs are intercepted by keystroke logging software.
		A PIN is captured from PIN pad device.

Offline cracking	The authenticator is exposed using analytical methods outside the authentication mechanism.	A software PKI authenticator is subjected to dictionary attack to identify the correct password to use to decrypt the private key.
Side channel attack	The authenticator secret is exposed using physical characteristics of the authenticator.	A key is extracted by differential power analysis on a hardware cryptographic authenticator.
		A cryptographic authenticator secret is extracted by analysis of the response time of the authenticator over a number of attempts.
Phishing or pharming	The authenticator output is captured by fooling the subscriber into thinking the attacker is a verifier or RP.	A password is revealed by subscriber to a website impersonating the verifier.
		A memorized secret is revealed by a bank subscriber in response to an email inquiry from a phisher pretending to represent the bank.
		A memorized secret is revealed by the subscriber at a bogus verifier website reached through DNS spoofing.
Social engineering	The attacker establishes a level of trust with a subscriber in order to convince the subscriber to reveal his or her authenticator secret or authenticator output.	A memorized secret is revealed by the subscriber to an officemate asking for the password on behalf of the subscriber's boss.
		A memorized secret is revealed by a subscriber in a telephone inquiry from an attacker masquerading as a system administrator.
Online guessing	The attacker connects to the	Online dictionary attacks are

	verifier online and attempts to guess a valid authenticator output in the context of that verifier.	used to guess memorized secrets.
		Online guessing is used to guess authenticator outputs for a one-time password device registered to a legitimate claimant.
Endpoint compromise	Malicious code on the endpoint proxies remote access to a connected authenticator without user consent.	A cryptographic authenticator connected to the endpoint is used to authenticate remote attackers.
	Malicious code on the endpoint causes authentication to other than the intended verifier.	Authentication is performed on behalf of an attacker rather than the subscriber.
	Malicious code on the endpoint compromises a multi-factor software cryptographic authenticator.	Malicious code proxies authentication or exports authenticator keys from the endpoint.

8.2. Threat Mitigation Strategies

Related mechanisms that assist in mitigating the threats identified above are summarized in Table 5.

Table 5 - Mitigating Authenticator Threats

Authenticator Threat/Attack	Threat Mitigation Mechanisms
Theft	Use multi-factor authenticators which need to be activated through a PIN or biometric.
Duplication	Use authenticators that are difficult to duplicate, such as hardware cryptographic authenticators.
Discovery	Use methods in which the responses to prompts cannot be easily discovered.
Eavesdropping	Use authenticators with dynamic outputs where knowledge of one authenticator does not assist in deriving a subsequent authenticator.
	Use authenticators that generate authenticators based on an

	authenticator input value or challenge.
	Establish authenticators through a separate channel.
Offline cracking	Use an authenticator with a high entropy authenticator secret.
	Use an authenticator that locks up after a number of repeated failed activation attempts.
	Store memorized secrets in a salted, hashed form to raise the cost of dictionary attacks; use a keyed hash.
Side channel attack	Use authenticator algorithms that are designed to maintain constant power consumption and timing regardless of secret values.
Phishing or pharming	Use authenticators with dynamic outputs where knowledge of one output does not assist in deriving a subsequent output.
Social engineering	Use authenticators with dynamic outputs where knowledge of one output does not assist in deriving a subsequent output.
Online guessing	Use authenticators that generate high entropy output.
Endpoint compromise	Use hardware authenticators that require physical action by the subscriber.
	Provide secure display of identity of verifier and relying party.
	Maintain software-based keys in restricted-access storage.

There are several other strategies that may be applied to mitigate the threats described in Table 5:

- *Multiple factors* make successful attacks more difficult to accomplish. If an attacker needs to both steal a cryptographic authenticator and guess a memorized secret, then the work to discover both factors may be too high.
- *Physical security mechanisms* may be employed to protect a stolen authenticator from duplication. Physical security mechanisms can provide tamper evidence, detection, and response.
- *Requiring the use of long memorized secrets* that don’t appear in common dictionaries may force attackers to try every possible value.

- *System and network security controls* may be employed to prevent an attacker from gaining access to a system or installing malicious software.
- *Periodic training* may be performed to ensure subscribers understand when and how to report compromise (or suspicion of compromise) or otherwise recognize patterns of behavior that may signify an attacker attempting to compromise the authentication process.
- *Out of band techniques* may be employed to verify proof of possession of registered devices (e.g., cell phones).

8.3. Authenticator Recovery

The weak point in many authentication mechanisms is the process followed when a subscriber loses control of one or more authenticators and needs to replace them. In many cases, the options remaining available to authenticate the subscriber are limited, and economic concerns (cost of maintaining call centers, etc.) motivate the use of inexpensive, and frequently less secure, backup authentication methods. To the extent that authenticator recovery is human-assisted, there is also the risk of social engineering attacks.

In order to maintain the integrity of the authentication factors, it is essential that it not be possible to leverage an authentication involving one factor to obtain an authenticator of a different factor. For example, a memorized secret must not be usable to obtain a new list of look-up secrets.

Subscribers should be encouraged to maintain at least two valid authenticators of each factor they will be using. For example, a subscriber that usually uses a one-time OTP device as a physical authenticator should also be issued a number of look-up secret authenticators, or should register a device for out-of-band authentication, in case the physical authenticator is lost, stolen, or damaged.

9. Privacy Considerations

To be completed

When developing e-authentication processes and systems, agencies SHALL consult OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 OMB M-03-22

10. Usability Considerations

To be completed

11. References

To be completed

11.1. General References

[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.

[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.

[RFC 20] Cerf, V., *ASCII format for network interchange*, STD 80, RFC 20, DOI 10.17487/RFC0020, October 1969, http://www.rfc-editor.org/info/rfc20 (http://www.rfc-editor.org/info/rfc20).

[RFC 5246] IETF, *The Transport Layer Security (TLS) Protocol Version 1.2*, available at https://tools.ietf.org/html/rfc5246/.

[RFC 5280] IETF, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, available at https://tools.ietf.org/html/rfc5280/.

[BCP 195] Sheffer, Y., Holz, R., and P. Saint-Andre, *Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, BCP 195, RFC 7525, May 2015, http://www.rfc-editor.org/info/bcp195 (http://www.rfc-editor.org/info/bcp195).

[ICAM] National Security Systems and Identity, Credential and Access Management Sub-Committee Focus Group, Federal CIO Council, *ICAM Lexicon*, Version 0.5, March 2011.

[ISO/IEC 10646] International Standards Organization, *Universal Coded Character Set*, 2014, available at http://standards.iso.org/ittf/PubliclyAvailableStandards/c063182_ISO_IEC_10646_2014.zip

[SAML] OASIS, SAML, *Security Assertion Markup Language 2.0”, v2.0, March 2005, available at http://oasis-open.org/standards#samlv2.0

11.2. NIST Special Publications

NIST 800 Series Special Publications are available at: http://csrc.nist.gov/publications/nistpubs/index.html (http://csrc.nist.gov/publications/nistpubs/index.html). The following publications may be of particular interest to those implementing systems of applications requiring e-authentication.

[SP 800-52] NIST Special Publication 800-52, Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, April, 2014.

[SP 800-53] NIST Special Publication 800-53, Revision 4, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*, August 2013 and Errata as of January 2015.

[SP 800-63C] NIST Special Publication 800-63C, *Assertions and Federation*. ***To be updated at publication***

[SP 800-131A] NIST Special Publication 800-131A , *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Revision 1, November 2015.

[SP 800-132] NIST Special Publication 800-132, *Recommendation for Password-Based Key Derivation*, December 2010.

11.3. Federal Information Processing Standards

FIPS can be found at: http://csrc.nist.gov/publications/fips/

[FIPS 140-2] Federal Information Processing Standard Publication 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001.

[FIPS 198-1] Federal Information Processing Standard Publication 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*, July 2008.

[FIPS 201] Federal Information Processing Standard Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013, available at http://dx.doi.org/10.6028/NIST.FIPS.201-2 (http://dx.doi.org/10.6028/NIST.FIPS.201-2).

Appendix A: Strength of Memorized Secrets

This appendix is non-normative.

A.1 Introduction

Despite widespread frustration with the use of passwords from both a usability and security standpoint, they remain a very widely used form of authentication. Humans, however, have only a limited ability to memorize complex, arbitrary secrets, so they often choose passwords that can be easily guessed. To address the resultant security concerns, online services have introduced rules in an effort to increase the complexity of these memorized secrets. The most notable form of these is composition rules, which require the user to choose passwords constructed using a mix of character types, such as at least one digit, uppercase letter, and symbol. However, analyses of breached password databases reveals that the benefit of such rules is not nearly as significant as initially thought, although the impact on usability and memorability is severe.

Complexity of user-chosen passwords has often been characterized using the information theory concept of entropy[ref]. While entropy can be readily calculated for data having deterministic distribution functions, estimating the entropy for user-chosen passwords is difficult and past efforts to do so have not been particularly accurate. For this reason, a different and somewhat simpler approach, based primarily on password length, is presented herein.

It should be noted that there are many attacks associated with the use of passwords that are not affected by password complexity. Keystroke logging, phishing, and social engineering attacks are equally effective on complex passwords as simple ones. Observation, “shoulder-surfing” attacks are only slightly more difficult for complex passwords. These attacks are outside the scope of this Appendix.

A.2 Length

Password length has been found to be the primary factor in characterizing password strength. Passwords that are too short yield to brute force attacks as well as to dictionary attacks using words and commonly chosen passwords.

The minimum password length that should be required depends to a large extent on the threat model being addressed. Online attacks where the attacker attempts to log in by guessing the password can be readily addressed by throttling the rate of login attempts permitted. In order to prevent an attacker (or a claimant with poor typing skills) from easily inflicting a denial-of-service attack on the subscriber by making many incorrect guesses, passwords need to be complex enough that throttling does not occur after a modest number of erroneous attempts, but does occur before there is a significant chance of a successful guess.

Offline attacks are sometimes possible when one or more hashed passwords is obtained by the attacker through a database breach. The ability of the attacker to determine one or more users' passwords depends on the way in which the password is stored. Commonly, passwords are salted with a random value and hashed, preferably using a computationally expensive algorithm. Even with such measures, the current ability of attackers to compute many billions of hashes per second with no throttling requires passwords to be orders of magnitude more complex to resist such attacks.

Users should be encouraged to make their passwords as lengthy as they want. Since the size of a hashed password is independent of its length, there is no reason not to permit the use of lengthy passwords (or pass phrases) if the user wishes.

A.3 Complexity

As noted above, composition rules are commonly used in an attempt to decrease the guessability of user-chosen passwords. Research has shown, however, that users respond in very predictable ways to the requirements imposed by composition rules. For example, a user that might have chosen "password" as their password would be relatively likely to choose "Password1" if required to include an uppercase letter and a number, or "Password1!" if a symbol is also required.

Users also express frustration when attempts to create complex passwords are rejected by online services. Many services reject passwords with spaces and various special characters. In some cases the special characters that are not accepted might be an effort to avoid attacks like SQL Injection that depend on those characters. But a properly hashed password would not be sent intact to a database in any case, so such precautions are unnecessary. Users should also be able to include space characters to allow the use of phrases. Spaces themselves, however, add little to the complexity of passwords and may introduce usability issues (e.g., the undetected use of two spaces rather than one), so it may be beneficial to remove spaces in typed passwords prior to verification.

Users' password choices are very predictable, so attackers are likely to try guess passwords that have been successful in the past. These include dictionary words and passwords from previous breaches, such as the "Password1!" example above. For this reason, it is recommended that passwords chosen by users be compared against a "black list" of unacceptable passwords. This list should include passwords from previous breach corpuses, dictionary words, and specific words (such as the name of the service itself) that users are likely to choose. Since user choice of passwords will also be governed by a minimum length requirement, this dictionary need only include entries meeting that requirement.