authentication - Glossary | CSRC

Archived: 2026-04-05 16:44:15 UTC

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Sources:

FIPS 200 under AUTHENTICATION

NIST SP 1800-10B under Authentication from FIPS 200

NIST SP 1800-21C under Authenticate

NIST SP 800-128 under Authentication from FIPS 200

NIST SP 800-137 under Authentication from FIPS 200

NIST SP 800-18 Rev. 1 under Authentication

NIST SP 800-30 Rev. 1 under Authentication from FIPS 200

NIST SP 800-39 under Authentication from FIPS 200

NIST SP 800-60 Vol. 1 Rev. 1 under Authentication from FIPS 200

NIST SP 800-60 Vol. 2 Rev. 1 under Authentication from FIPS 200

The process of establishing confidence of authenticity; in this case, the validity of a person’s identity and an authenticator (e.g., PIV Card or derived PIV credential).

Sources:

FIPS 201-3 under Authentication

A security measure designed to protect a communications system against acceptance of fraudulent transmission or simulation by establishing the validity of a transmission, message, originator, or a means of verifying an individual's eligibility to receive specific categories of information.

Sources:

CNSSI 4009-2015 from CNSSI 4005, NSA/CSS Manual Number 3-16 (COMSEC)

Security measures designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to receive specific categories of information.

Sources:

NIST SP 800-59 under Authentication from CNSSI 4009

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

Sources:

NIST SP 800-12 Rev. 1 under Authentication from FIPS 200

NIST SP 800-128 from FIPS 200

NIST SP 800-171r3 from FIPS 200 - adapted

NIST SP 800-172 from FIPS 200 - Adapted

NIST SP 800-172A from FIPS 200 - Adapted
NIST SP 800-37 Rev. 2 from FIPS 200
NIST SP 800-53 Rev. 5 from FIPS 200
NISTIR 7316 under Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Sources:
CNSSI 4009-2015 from FIPS 200
NIST SP 800-82r3 from FIPS 200

To confirm the identity of an entity when that identity is presented.

Sources:
CNSSI 4009-2015 under authenticate

The process a VPN uses to limit access to protected services by forcing users to identify themselves.

Sources:
NIST SP 800-113 under Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.

Sources:
NIST SP 1800-16B under Authentication
NIST SP 1800-16C under Authentication
NIST SP 1800-16D under Authentication
NIST SP 1800-17c under Authentication

Provides assurance of the authenticity and, therefore, the integrity of data.

Sources:
NIST SP 800-67 Rev. 2 under Authentication

A process that provides assurance of the source and integrity of information in communications sessions, messages, documents or stored data or that provides assurance of the identity of an entity interacting with a system.

Sources:
NIST SP 800-57 Part 2 Rev.1 under Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources

Sources:
NIST SP 1800-17b under Authentication

The process of establishing confidence of authenticity. In this case, it is the validity of a person’s identity and the PIV Card.

Sources:

NIST SP 1800-12b

A process that provides assurance of the source and integrity of information that is communicated or stored or the identity of an entity interacting with a system.

Sources:

NIST SP 800-175B Rev. 1 under Authentication

Note that in common practice, the term "authentication" is used to mean either source or identity authentication only. This document will differentiate the multiple uses of the word by the terms source authentication, identity authentication, or integrity authentication, where appropriate.

Sources:

NIST SP 800-175B Rev. 1 under Authentication

A process that provides assurance of the source and integrity of information in communications sessions, messages, documents or stored data or that provides assurance of the identity of an entity interacting with a system. See Source authentication, Identity authentication, and Integrity authentication.

Sources:

NIST SP 800-57 Part 1 Rev. 5 under Authentication

The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Sources:

NIST SP 1800-27B under Authentication from FIPS 200

NIST SP 1800-27C under Authentication from FIPS 200

The act of verifying that the subject has been authorized to use the presented identifier by a trusted identity provider organization.

Sources:

NIST SP 800-162

The corroboration that a person is the one claimed.

Sources:

NIST SP 800-66r2 from HIPAA Security Rule - §164.304

As used in this document, a process that provides assurance of the source and integrity of information that is communicated or stored, or that provides assurance of an entity’s identity.

Sources:

NIST SP 800-175A

The process by which a claimant proves possession and control of one or more authenticators bound to a subscriber account to demonstrate that they are the subscriber associated with that account.

Sources:

NIST SP 800-63-4 [

]

NIST SP 800-63A-4 []

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

Sources:

NISTIR 8149 under Authentication

The process of verifying a claimed identity of a user, device, or other entity in a computer system

Sources:

NISTIR 4734 under Authentication

the process of verifying the integrity of data that has been stored, transmitted, or otherwise exposed to possible unauthorized access.

Sources:

NISTIR 4734 under Authentication

The process of proving the claimed identity of an individual user, machine, software component or any other entity. Typical authentication mechanisms include conventional password schemes, biometrics devices, cryptographic methods, and onetime passwords (usually implemented with token based cards.)

Sources:

NISTIR 5153 under Authentication

The process of establishing confidence in the claimed identity of a user or system

Sources:

NISTIR 7682 under Authentication

Verifying the identity of a user, process, or device, often as a prerequisite for allowing access to resources in an information system.

Sources:

NISTIR 8301 under Authentication from FIPS 200

measures the number of times an attacker must authenticate to a target in order to exploit a vulnerability.

Sources:

NISTIR 7864 under Authentication

NISTIR 7946 under Authentication

The process by which a claimant proves possession and control of one or more authenticators bound to a subscriber account to demonstrate that they are the subscriber associated with that account and involves one or more of the following factors:

i. something you know (e.g., password/personal identification number (PIN));

ii. something you have (e.g., cryptographic identification device, token); or

iii. something you are (e.g., biometric).

Sources:
NIST IR 8523 from NIST SP 800-63-4 - adapted
