

Authentication

[Go up to Terms and Definitions](#)

Discussion

Authentication evaluates evidence associated with a claimed [Identity](#) or another asserted attribute.

The subject of Authentication includes a person, organisation, process, device, service, [Node](#), system, message, or data source.

An authentication process evaluates one or more factors, including knowledge, possession, inherent characteristics, location, behaviour, cryptographic proof, or an assertion issued by a trusted authority.

A [Credential](#) supplies or references evidence used by the authentication process. Authentication remains distinct from [Access Control](#). Authentication evaluates a claim. Access Control determines whether the authenticated or otherwise identified subject receives access to a resource.

Definition

process that establishes confidence in the validity of a claimed identity or other asserted attribute

Source

Adapted from ISO/IEC 27000, Information security, cybersecurity and privacy protection — Vocabulary, and NIST terminology concerning digital identity.

Note

Authentication identifies the claim, subject, evidence, authentication method, applicable assurance criteria, result, and time of evaluation.

Authentication does not independently grant access or establish authority. An Access Control decision evaluates the authenticated identity or attribute together with the applicable [Policy](#) and request context.

Failed, expired, revoked, incomplete, or unverifiable authentication evidence produces an unsuccessful authentication result.

Example

A Node authenticates another Node by validating its certificate chain, verifying possession of the corresponding private key, and confirming the asserted Node identity.

© 2026 Dido Solutions, Inc. and Jackrabbit Consulting, Inc.

From:
<https://wiki.didosolutions.com/> - **Dido Solutions, Inc Wiki**

Permanent link:
https://wiki.didosolutions.com/dido/99_annexes/annex-b-terms-and-definitions/a/authentication

Last update: **2026/08/08 12:59**

