GEORGETOWN UNIVERSITY | beeckcenter social impact + innovation | Digital Benefits NETWORK

DECEMBER 2022

Digital Identity Glossary

This glossary provides definitions for some of the key terms related to digital identity topics, such as identity proofing and authentication. Some of these terms are directly applicable to the processes benefits agencies might deploy, while other definitions help explain topics that may affect future digital identity work.

Where relevant, definitions are drawn directly from the National Institute of Standards and Technology (NIST) Computer Security Resource Center Glossary and other NIST guidance. We use hyperlinks to cite to NIST definitions as well as other outside sources. This is a living document and we will add new entries and update terms as the Digital Benefits Network (DBN) continues our digital identity research.

Terms

+ **Attribute**: A quality or characteristic ascribed to someone or something. An identity is composed of an attribute or set of attributes (e.g., name, date of birth, address, fingerprints, etc.) that uniquely describe a subject within a given context.
+ **Authentication**: The verification of the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources. For example, a user is asked to present something they know (e.g., a password), something they have (e.g., a security key or ID badge), or something they inherently possess (e.g., fingerprint or other biometric data) to gain access to a system.
+ **Authenticator Assurance Levels (AAL)**: NIST category describing the strength of an authentication process.
+ **Claimed Identity**: An applicant's declaration of unvalidated and unverified personal attributes.
+ **Credential Service Provider (CSP) or Identity Provider (IdP)**: A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or issue credentials for its own use.

+ **Digital Identity**: As noted in our overview, *What is Digital Identity*, NIST points out that "a single definition of [digital identity] is widely debated." For the purposes of their digital identity guidelines, NIST defines digital identity as, "the unique representation of a subject engaged in an online transaction." The publication goes on to clarify that "a digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known."
    - As we explain further in our introductory resource on digital identity, digital identity as a topic encompasses distinct processes such as authentication and identity proofing, which are used to confirm and verify identities, as well as digital identification credentials.
    - For more on digital identity as an evolving concept, we suggest Dr. Clare Sullivan's article, "Digital identity – From emergent legal concept to new reality."
+ **Facial Recognition Technology**: A set of digital tools that can be used to perform different tasks on instances, images, or videos of human faces, including determining if there is a face in a given image, deciding what kind of face is presented, and whose face is present.
    - **Face verification, 1-1 comparison**: When an entity wants to confirm the identity of a face, they may compare a faceprint (an image or recording of a face) to an existing faceprint of the expected individual. This process can be used to verify a person's claim about who they are.
    - **Face identification: 1-to-many comparison**: When someone wants to identify a face, for example, from surveillance footage, and does not know the expected identity of the individual, they may compare one faceprint to a set of faceprints in a gallery to find a match.
+ **Federation Assurance Levels (FAL)**: NIST category describing the strength of the assertion protocol used by a federated identity management system to communicate authentication and attribute information (if applicable) to a relying party. (Relying Party (RP) is the entity that relies on results of an authentication protocol to establish confidence in the identity or attributes of a subscriber for the purpose of conducting an online transaction.) If federated identity management trusts credentials from one provider across other systems, the FAL describes the protocols used to assert authentication and attribute information across systems.
+ **Federated Identity Management**: A process that allows for the conveyance of identity and authentication information across a set of networked systems. Federated identity management can allow users to use one set of credentials to log into multiple separate systems.
+ **Identity Assurance Levels (IAL)**: Currently ranging from IAL1 to IAL3, this category conveys the degree of confidence that a person's claimed identity is their real identity.
+ **Identity Evidence**: Information or documentation provided by an individual to support their claimed identity. Identity evidence may be physical such as a driver license or digital. Digital identity evidence can be in the form of an assertion generated and issued by a credential service provider (CSP) based on the applicant successfully authenticating to the CSP.
+ **Identity proofing**: The process by which a credential service provider collects, validates, and verifies information about a person. Identity proofing is the more official term for what is often informally referred to as identity verification. Identity proofing encompasses multiple distinct steps or types of processes, including:
    - **Identity resolution**: According to NIST guidelines, identity resolution aims "to uniquely distinguish an individual within a given population or context." Resolution describes the processes used to confirm that whatever personally identifiable information (PII) a user shares belongs to a single, real person. This can be accomplished by comparing self-asserted PII to information in publicly available databases.
    - **Identity validation**: As defined in NIST guidelines, "the goal of identity validation is to collect the most appropriate identity evidence (e.g., a passport or driver's license) from the applicant and determine its authenticity, validity, and accuracy." NIST breaks this process out into three consecutive steps: collecting identity evidence, confirming that the identity evidence is genuine and authentic, and confirming that the data provided from the identity evidence is valid, current, and related to a real-life subject.

- **Identity verification**: NIST guidance explains the goal of identity verification is "to confirm and establish a linkage between the claimed identity and the real-life existence of the subject presenting the evidence." Identity verification "represents the highest degree of certainty that the user is who they say they are by establishing a physical connection between the applicant and the PII or evidence provided." It can be achieved through methods such as biometric verification, enrollment codes, or two-factor authentication.

+ **Knowledge-based verification (KBV)**: Identity verification method based on knowledge of private information associated with the claimed identity. This is also often referred to as knowledge-based authentication (KBA) or knowledge-based proofing (KBP).

+ **Personally identifiable information (PII)**: Personally Identifiable Information is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Examples include Social Security number, passport number, driver's license number, taxpayer identification number, credit card numbers, telephone numbers, address, etc.

+ **Remote identity proofing**: Describes identity proofing processes that take place remotely. (See NIST descriptions and requirements for conventional remote identity proofing and supervised remote identity proofing.) The phrase remote identity proofing or RIDP is sometimes also used to describe knowledge-based verification challenges that require users to correctly answer a series of questions about their credit history or other data. (For an example, see the CMS informational page.)

+ **Self-sovereign identity**: An identity management framework, independent of a third-party public or private actor, in which individual users have control over their identifying information.

+ **Single-sign-on (SSO)**: An authentication framework that allows the use of a single set of credentials to login to multiple related software systems. Authentication for one part of the system may automatically authenticate the user in other parts.

+ **Two-factor authentication (2FA)**: Authentication using two or more factors to achieve authentication. For example, using both a password and a PIN to log in to an application, or using a password then entering a one-time code sent to your mobile device via SMS. Multi-factor authentication, or MFA, may require users to employ more than two authentication factors.

+ **Zero-trust/zero-trust architecture (ZTA)**: Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. The zero trust security model eliminates implicit trust in any one element, component, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.

You can read more about digital identity on the Digital Benefits Hub, and find our other introductory resources including:

+ A primer, *What is Digital Identity?*

+ A short explainer on digital identity in public benefits

+ An overview of federal interest in digital identity

Agencies or individuals interested in our research on digital identity can subscribe to the DBN and follow updates. If you would like to discuss our research further or are interested in sharing your own experiences administering identification and authentication processes in a benefits program, we encourage you to reach out to us at digitalbenefits@georgetown.edu.