

CSIS Digital Identity Management Project Authentication Lexicon

Attributes properties of an individual of interest to and knowable by other entities; for example, {first name, age, blood type}. Attributes are associated with a particular individual.

Authentication is the process whereby a degree of confidence is established about the truth of an assertion about identity. Authentication is the process by which a party tests a claimed mapping between a principal and a credential, by checking the correlation between credentials.

For example, the physical person John Smith wishes to log onto a system using the userID = johnsmith (principal is John Smith; userID is an attribute with value johnsmith). During the logon he provides the credential {userID = johnsmith, password = 1234}. The authentication service compares this credential with one it has on file; the authentication service may have been the issuer of this credential, or it may check with the issuer using federated authentication. If there is a match, it will assert that the principal who is using userID = johnsmith is the same principal to whom the johnsmith credential was issued.

Authorization The provision of services or activities based on an authenticated identity.

Birth certificate is a document issued by governments to persons that establishes legal identity.

Central Register network accessible database or directory where credentials are stored and can be accessed for authentication.

Core identity documents Government-issued documents that provide the basis for issuing all other identity documents, usually a birth certificate and a national identity number. Governments regard the issuance core identities as a crucial function closely tied to both security and access to benefits.

Credential a collection of attribute values for an identity. Since it is typically a sub-set of all attribute values, an identifier is not the same as an identity. (To reduce potential confusion between identities and identifiers - both are referred to as IDs - we may choose to use the term credential instead of identifier). These credentials are used by hosts, resource, or the individual itself to provide and manage services.

Digital identities. There are four classes of digital identities: legal, government issued identities; derivative identities, persistent pseudonyms; and temporary pseudonyms. The degree of trust that can be assigned to each class depend n the strength of its linkage to the government issued identity. Close linkages imply high responsibility (or liability) for acts taken with the digital token in the name of that identity).

- **Government issued identities.** For all practical purposes, a person is “stateless” and without identity until they receive valid, government issued documents. Use of these identities in a transaction makes them legally binding.
- **Derivative identities** Most of the identity tokens people use are derived from government issued identities, but these derivative identities can carry high degrees of trustworthiness. Their trustworthiness come form the strength of the linkage to the legally binding identity and to the degree of liability associated with them for actions taken. Use of these identities can also be legally binding in certain circumstances.
- **Persistent pseudonyms** Pseudonym means ‘false name.’ These are identities created by an individual and used repeatedly for a particular set of transactions. These are not binding and any trustworthiness associated with them is intuited from their pattern of behavior.
- **Temporary pseudonyms** are identities generated for a single transaction or event and not re-used. Anonymity is a decision not to provide a permanent identity (logging in as ‘guest’ or ‘anonymous’ or creating a temporary pseudonym).

Devices are machines containing microprocessors or software agents capable of engaging in transactions with others on their own, without direct human guidance. Devices will increasingly populate the Internet. Digital tokens for devices will be based either on the devices legal identity or on a legal identity derived from a person or firm.

Federation federated systems are autonomous, possibly heterogeneous information systems, which interoperate and cooperate to perform common tasks or to achieve common goals. For digital identities, federation is a cooperative arrangement among systems that uses common sets of rules to allow identities or credentials issued by one domain to be recognized and treated equally by other federated domains.

Federated or cross-domain authentication occurs when a principal in a domain presents a credential issued by another domain. The credential is passed to another domain, typically the issuing domain, which asserts that it is valid. If the receiving domain accepts assertions made by the second, a trust relationship is established between them. For example: assume that web site A has issued a credential to a user, which is used to access information (say, mail messages). If there is a trust relationship between site A and site B, the user can use the credential issued by site A to log into site B.

Firms groups of persons who have been issued a separate legal identity by a government (incorporate means ‘to be given a body’) to pursue commercial activities.

Governance describes the processes for the development, implementation and enforcement of rules.

Governments The formal political and administrative structure of societies, which are

the source of binding identities. For purposes of digital identities, governments are the issuers of primary identity documents; enforcers of rules governing identity, and negotiators (with other governments) of common approaches to managing digital identity.

Identity is the full set of all attribute values for a principal. It can be used to differentiate one principal from another.

Identity Services centralized provision by government agencies or firms of authorizations, application settings and credentials.

Incorporation The process by which a government recognizes the creation of an artificial legal entity (a corporation). A corporation has its own life separate from its owners and is liable for its own actions.

Issuer a principal who provides credentials.

Mediator a party external to an authentication transaction who can independently verify credentials. These can include Trusted Third Parties.

National Identity Number Numbers issued to persons by governments to allow them to access social services or to identify them for tax purposes. The General Accounting Office says that the U.S. Social Security Numbers says that it has become “the identifier of choice for government agencies and business” in the U.S. Practices in other countries vary but some use identification numbers, such as the UK’s National Insurance number (NI number) while others issue general purpose identity cards.

Participants there are four classes of participants in digital identity system: devices, persons, firms and governments.

Persons human beings with government-issued identities.

Principal an actor in an information transaction; it may be a person, machine or program.

Revocation the process of ending the validity of a digital identity, credential or token.

Token a physical representation (including software) that stores an individual's credentials that provide digital identity. These can include smart cards, biometrics or stored software (certificates). The differing levels of liability and trust they provide can also differentiate tokens.

Verification the process of a receiving party using information, a token or a credential provided by a sending party to verify an assertion about identity. These can include passwords, Personal Identification Numbers, biometric features, question-and-answer process