Self-Sovereign ID Glossary

A

Access Management – Access management is the process of managing a user's login and access across a wide range of applications, systems, and resources belonging to an organization. Most IAM solutions manage user access to resources but leave access authorization decisions to the application owners.

Affiliation – Affiliation is the combination of one's relationship with an organization and some form of trusted identity (which may not be from within the organization).

Attribute – Small pieces of information that make up a digital identity. Attributes may include name, phone number, group affiliation, etc. (there are a whole different range of attributes - different attributes and claims have different qualities. A phone number and a self-asserted name are different - https://identitywoman.net/identifiers-a-field-guide/)

Audit – See security entitlement audit

Authentication (AuthN) – Authentication is the process of validating an identity, whether it be the identity of a user or, as in the Identity of Things, a device. The classic method of validation is the username/password combination.

Authorization (AuthZ) – Authorization is the process of determining if a user has the right to access a service or resource, or perform an action.

Authorization Audit – An authorization audit is a process that gives a detailed overview of the access capabilities of an entire organization.

Authorizer – An individual responsible for approving changes in user authorizations and privileges.

B

C

Central Authentication Service (CAS) – A single sign-on web protocol which allows a user to access multiple services while providing login credentials only once.

Chief Information Officer (CIO) – A senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals.

Chief Information Security Officer (CISO) – A senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure that information assets and technology are protected.

Chief Trust Officer (CTRO) – A senior-level executive within an organization responsible for establishing, maintaining, and enforcing the identity, security, and privacy policies within the organization.

Claim – A statement made by an entity about a subject (including itself). A verifiable claim is a claim that is effectively tamper-proof and whose authorship can be cryptographically verified.

Compliance – In IT and data storage terminology, compliance refers to organizational compliance with government regulations regarding data storage and management and other IT processes.

Credential – (this definition is contested - different meanings of it circulate and they are all "right") A credential is an item, such as an ID card, or a username/password combination, used by persons or entities to prove themselves.

Customer Identity and Access Management (CIAM) – Customer, or Consumer Identity and Access Managment (CIAM) is an IAM solution that is specifically tailored to meet the needs of organizations handling large volumes of consumer identity information. Though superficially similar to traditional IAM, CIAM solutions must provide smooth, yet secure customer experience, with the ability to scale quickly to handle large volumes of customer data.

D

Data Minimization – This is the act of limiting the amount of shared data strictly to the minimum necessary in order to successfully accomplish a task or goal. it has three parts: content minimization – the amount of data should be strictly the minimum necessary; temporal minimization – the data should be stored by the receiver strictly during the minimum amount of time necessary to execute the task; and scope minimization – the data should only be used for the strict purpose of the active task.

Decentralized Identifier (DIDs) – A globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology or other form of decentralized network. The generic format of a DID is defined in this specification. A specific DID scheme is defined in a DID method specification.

Decentralized Identity Management – Identity Management based on decentralized identifiers. Decentralized Identity Management extends the identifier creation authority beyond the traditional roots of trust required by X.500 directory services, the Domain Name System, and most national ID systems.

Decentralized Public Key Infrastructure (DPKI) - that is able to preserve the integrity of identifiers by protecting organizations or individuals from private key loss or compromise.

De-provisioning – The removal of an individual's organizational digital identity, access, and privileges.

DID-Auth - A blockchain based authentication method that uses DIDs for interoperability and standardization. And sometimes referred to as *"super sign on"*.

DID Document – A set of data that describes a DID, including mechanisms, such as public keys and pseudonymous biometrics, that an entity can use to authenticate itself as the DID. A DID Document may also contain other attributes or claims describing the entity. These documents are graph-based data structures that are typically expressed using [JSON-LD], but may be expressed using other compatible graph-based data formats.

DID Fragment – The portion of a DID reference that follows the first hash sign character ("#"). A DID fragment uses the same syntax as a URI fragment. See section 5.5. Note that a DID fragment MUST immediately follow a DID. If a DID reference includes a DID path followed by a fragment, that fragment is NOT a DID fragment.

DID Method – A definition of how a specific DID scheme can be implemented on a specific distributed ledger or network, including the precise method(s) by which DIDs and DID Documents can be read, written, and revoked.

DID Path – The portion of a DID reference that follows the first forward slash character. A DID path uses the identical syntax as a URI path. See section 5.4. Note that if a DID path is followed by a fragment, that fragment is NOT a DID fragment.

DID Reference – A DID plus an optional DID path or DID fragment.

DID Scheme – The formal syntax of a Decentralized Identifier. The generic DID scheme is defined in this specification. A DID method specification defines a specific DID scheme that works with a specific DID method.

Digital Identity – A digital identity is a set of information (attributes and credentials) about an individual that is maintained in order to associate them with an organization.

Distributed Ledger (aka DLT, blockchain) – A distributed database in which the various nodes use a consensus protocol to maintain a shared ledger in which each transaction is cryptographically signed and chained to the previous transaction

E

Entity – A thing with distinct and independent existence such as a person, organization, concept, or device.

Entity credential – A set of one or more claims made by the same entity about a subject.

Entity profile – A set of entity credentials related to the same subject. An entity may have multiple entity profiles and each entity profile may contain claims issued by multiple entities.

Event – An action or the result of an action. Events are often logged and monitored for security purposes.

Extensible Data Interchange (aka XDI) – A semantic graph format and semantic data interchange protocol defined by the OASIS XDI Technical Committee.

F

Federated Identity – A federated identity is the product of linking all of an individual's disparate electronic identities and attributes, which may be stored across multiple identity management solutions.

Federated Identity Management – A Federated Identity Management (FIM) Solution is a technical implementation that allows identity information to be developed and shared among multiple identity management entities, and across trust domains.

FIDO Alliance – The FIDO (Fast IDentity Online) Alliance is a non-profit group formed to address a lack of interoperability between authentication devices, and the challenges that users face in maintaining multiple usernames, passwords, and authentication methods.

G

Group – In identity management, a group allows the management of multiple entities (I.e. employees or customers) within a single category. Groups are used to define roles and simplify access control.

H

Hashgraph – This is a technology that can offer many of the same solutions as blockchain, but which uses different mechanisms to transmit information and confirm transactions within the network. It is essentially a graph in the mathematical sense of the word, held together by simple, regular hashes with no high-level cryptographic implementations, like zero-knowledge proofs, for example.

Holder – An entity that is in control of one or more verifiable claims. Examples of holders include students, employees, and customers.

I

Identity Hubs – an encrypted identity datastore that features message/intent relay, attestation handling, and identity-specific compute endpoints.

Inspector-verifier – An entity that receives one or more verifiable claims for processing. Examples of inspector-verifiers include employers, security personnel, and websites.

Identifier registry – Mediates the creation and verification of subject identifiers. Examples of identifier registries include corporate employee databases, government ID databases, and distributed ledgers.

Identification – Identification is the process by which an entity's information is gathered and verified for accuracy.

Identity Access Governance – Identity and Access Governance (IGA) solutions establish an identity lifecycle process that gives managers the ability to have comprehensive governance of identities and access requests.

Identity and Access Management – Identity and Access Management (IAM) is a system, solution, or service that addresses an organizational need for a system-wide solution that manages user's access and authentication into external and internal applications, databases, or networks.

Identity Governance and Administration (IGA) – Similar to IAM, IGA is a set of processes used to manage identity and access controls across systems. IGA differs from IAM in that it allows organizations to not only define and enforce IAM policy but also connect IAM functions to meet audit and compliance requirements.

Identity Management (IdM) – Identity Management (IdM) is the act of using processes and solutions for the creation and management of user or connected device information.

Identity Management as a Service – Identity and access management as service, or IDaaS, is an IAM solution delivered as a service. IDaaS solutions are predominately cloud-based and are hosted and sometimes managed by the service provider.

Identity Trust Fabric – This is a term that describes the storage of proof of decentralized identities and information about their profile cryptographically. This enables service providers to access and use such records to check the authenticity of customer identity.

Identity Custodian – This is an entity that can collaborate with organizations, manage regulations, but ultimately remain neutral. The entity should be ideally be decentralized and resilient to attack, and the individual user should be the ultimate owner and sovereign controller of their own identity.

Issuer – An entity that creates a verifiable claim, associates it with a particular subject, and transmits it to a holder. Examples of issuers include corporations, governments, and individuals.

J

K

L

Level of Assurance (LoA) – The Level of Assurance (LoA) is the degree of confidence achieved by the vetting and proofing process used to establish the identity of a user. There are four levels of assurance, ranking from zero (no confidence existing in the asserted identity) to four (very high confidence in the asserted identity's accuracy).

Log Files – Log files are files that record either events that occur in an operating system or software, or messages occurring on communication software. For example, when a failed login to an E-mail system occurs, a log file is created to record that event.

Logging – the act of keeping a log for an extended period of time.

M

Management Chain – In an organization, users usually have managers, who in turn may have their own managers. This sequence of managers, which starts with the user and ends with the highest manager in that organization, is known as the management chain. In the context of identity management, management chains are often used to authorized security changes.

Multifactor Authentication – Multifactor authentication adds an additional step (or factor) to the authentication process, typically by pairing something the user knows, such as username and password, with an action, or something the user has, such as an SMS message to their phone, an email, or a token.

N

NetID – An electronic identifier created specifically for use with online applications.

O

OAuth – OAuth is an open authorization standard that allows applications to autonomously access resources on behalf of a user. iOS and Android, for example, use this kind of authorization to let users choose whether or not an app can have access to certain functions and parts of the phone.

Offboarding – The process by which a user is removed (with access revoked) from an organization's IAM system.

OpenID – A standardized, open method of decentralized authentication.

OpenID Connect (OIDC) - OpenID Connect is an authentication layer on top of OAuth 2.0, an authorization framework. The standard is controlled by the OpenID Foundation.

Onboarding – The process of adding new users to an organization's IAM system.

One Time Password (OTP) – A password that is valid for use one use or session.

P

Password – A word or string of characters used to prove one's identity, or authorize access to a resource. Usually, but not always, paired with a username.

Password Reset – The process by which a user changes their own password.

PGP – Aka "Pretty Good Privacy", is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. Phil Zimmermann developed PGP in 1991.

Privilege – A privilege is a construct that allows certain users within an organization to have a number of powers based on their credentials and identity attributes.

Privileged Account Management (PAM) – See privileged identity management.

Privileged Identity Management (PIM) – Privileged identity management is a process or technology focused on managing, monitoring, and protecting powerful privileged user accounts within the IT infrastructure of an enterprise.

Privilege Management – Privilege Management is the process by which the owner of a network can modify or assign privileges for applications and resources.

Privileged User – A user possessing specific security privileges and entitlements.

Progressive Disclosure – The ability of an individual to gradually increase the amount of relevant data revealed as trust is built or value generated. See appendix for collected definitions of progressive disclosure.

Provisioning – A process that enables users to use their privileges to access applications and services.

Q

R

Requester – A person who requests a change in user profiles, privileges, or entitlements, either by an automated or manual process.

Role – An identity attribute that gives users automatic privileges when assigned. Roles make take the form of groups wherein all members of a group have the same set of privileges.

Role-Based Access Control (RBAC) – A model in which users are assigned “roles” that give them a certain level of access to resources and systems. Assigning a role to a user grants that user a certain set of privileges and entitlements.

S

Security Administrator – A person responsible for maintaining a list of users, their identity attributes, their passwords, security privileges, or other authentification factors.

Security Entitlement Audit – An official organizational review of security entitlements and user privileges. A periodical entitlement audit is a reliable method for finding and removing old, unneeded entitlements.

Selective Disclosure – The ability of an individual to granularly decide what information to share. Selective disclosure is a means by which data minimization can be achieved. See appendix for collected definitions of selective disclosure.

Self-Service Password Resets – A self-service password reset is a process that allows users that have forgotten their password to use an alternate process to authenticate themselves and thus reset their password without the assistance of help desk personnel.

Service Endpoint – A network address at which a service operates on behalf of an entity. Examples of specific services include discovery services, social networks, file storage services, and verifiable claim repository services. Service endpoints may also be provided by a generalized data interchange protocol such as Extensible Data Interchange.

Session – A session is an interaction between two or more entities on a network, generally consisting of an exchange of information. In the context of identity management, the most important information exchanged is the credentials of each entity and the time-out information for the session.

Single-Factor Authentication – A method of authentication that relies on a single factor, such as username and password, to verify a user's identity.

Single Sign-On (SSO) – In a single sign-on (SSO) service model users log onto a single platform which gives them automatic log-in access to multiple applications for a particular period of time. When utilizing SSO systems users only need to present one set of credentials, rather than learning or remembering separate credentials for each application.

Subject – An entity which may have multiple entity profiles and about which claims may be made.

Support Analyst – A support analyst, in an identity management context, is a user with special privileges that allow him or her to help other users, often by resetting their forgotten passwords or provisioning new privileges.

System for Cross-Domain Identity Management (SCIM) – A system for cross-domain identity management (SCIM) is an open standard for automating the exchange of user identity information between identity domains, or IT systems, designed to make user identity management in cloud-based applications easier.

System of Record (SoR) – A system of record (SoR) is a storage system designated as an authoritative source for a certain identity attribute. As the SoR is the direct line of access to the identity attribute that it controls, all modifications to those identity attributes should be brokered via the SoR.

T

Termination – The process by which user or customer credentials or privileges are de-provisioned and removed.

U

Universal DID Resolver – a server that resolves DIDs across blockchains

User – Users are people whose access to systems and identity information must me managed.

User Lifecycle Management (ULM) – User Lifecycle Management (ULM) is an Identity-based user management process library and framework designed to enable personalized digital user experiences across multiple services and devices.

User Provisioning – Technologies or processes that create, modify, and deactivate user accounts, privileges, and profiles across IT infrastructure and business apps.

V

Verifiable Credentials – These cryptographic objects consist of a set of attributes that have been digitally signed by an issuer. The signature of the issuer serves as an attestation that the attributes in the claim are true.

Vetting – The process of thoroughly investigating and validating information collected from or about an individual for the purpose of issuing credentials or privileges.

W

X

Y

Z

Zero Knowledge Proof – A cryptographic method by which one party can prove to another party that they know a value x, without conveying any information apart from the fact that they knows the value x.