Identity and Access Management (IAM) Glossary

Identity and Access Management Working Group
https://cloudsecurityalliance.org/research/working-groups/identity-and-access-management/

Acknowledgments

Lead Authors

Alon Nachmany
Ansuman Mishra
Ramesh Gupta
Ravi Erukulla
Shruti Kulkarni

Contributors

Faye Dixon
Heinrich Smit
Paul Mezzera
Venkat Raghavan

Reviewers

Andrews Antwi
Arun Dhanaraj
Chandrasekaran Rajagopalan
Erik Johnson
Kapil Bareja
Michael Roza
Rajat Dubey
Senthilkumar Chandrasekaran
Shraddha Patil

CSA Global

Ryan Gifford

CSA Global Staff

Stephen Lumpe
Stephen Smith

Table of Contents

Glossary

Term	Definition
Active Directory Federation Services (ADFS)	ADFS provides simplified, secured identity federation, and Web Single Sign-On (SSO) capabilities.
Source:	https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/how-to-connect-fed-azure-adfs
Adaptive Authentication	Risk-based or adaptive authentication systems evaluate a host of user, system, and environmental attributes; other such signals; and behavioral profiles to make an authentication decision. IP address, geolocation, time of day, transaction type, mouse movements, keystroke, and variances from typical usage norms are some of the signals used in these systems. These solutions do not currently count as a valid authenticator in and of themselves, as this information does not necessarily constitute a "secret", and most solutions leverage proprietary ways of making an authentication decision.
Source:	https://pages.nist.gov/800-63-FAQ/
Adaptive Multi-Factor Authentication (MFA)	Adaptive MFA, otherwise known as risk-based MFA, provides users with authentication factors that adapt each time a user logs in depending on the calculated risk level of the user based on contextual information. Some examples of contextual information include: • The number of consecutive login failures • The physical location (geolocation) of the user requesting access • The type of device • The day of the week and the time of the day • The IP address
Source:	https://www.manageengine.com/products/self-service-password/adaptive-multi-factor-authentication.html
Application / System Owner	Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system
Source:	https://csrc.nist.gov/glossary/term/system_owner#:~:text=NISTIR%208011%20Vol.,disposition%20of%20an%20information%20system

Assertion	Assertions are statements from an Identity Provider (IdP) to a relying party (RP) that contain information about a subscriber. Federation technology is generally used when the IdP and the RP are not a single entity or are not under common administration. The RP uses the information in the assertion to identify the subscriber and make authorization decisions about their access to resources controlled by the RP. An assertion typically includes an identifier for the subscriber, allowing association of the subscriber with their previous interactions with the RP. Assertions may additionally include attribute values or attribute references that further characterize the subscriber and support the authorization decision at the RP. Additional attributes may also be available outside of the assertion as part of the larger federation protocol. These attribute values and attribute references are often used in determining access privileges for Attribute Based Access Control (ABAC) or facilitating a transaction (e.g., shipping address).
Source:	https://pages.nist.gov/800-63-3/sp800-63c.html
Attack Surface	The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment.
Source:	https://csrc.nist.gov/glossary/term/attack_surface
Attributes	An attribute or set of attributes that uniquely describe a subject within a given context. The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.
Source:	https://csrc.nist.gov/glossary/term/identity#:~:text=An%20attribute%20or%20set%20of,subject%20within%20a%20given%20context.&text=The%20set%20of%20attribute%20values,entity%20from%20any%20other%20entity
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
Source:	https://csrc.nist.gov/glossary/term/authentication
Authentication Factors	Authentication using two or more factors to achieve authentication. Factors include: (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).
Source:	https://csrc.nist.gov/glossary/term/mfa#:~:text=Authentication%20using%20two%20or%20more,are%20(e.g.%2C%20biometric)

Authorization	The decision to permit or deny a subject access to system objects (network, data, application, service, etc.)
Source:	https://csrc.nist.gov/glossary/term/authorization
Brute Force	A method of accessing an obstructed device by attempting multiple combinations of numeric/alphanumeric passwords
Source:	https://csrc.nist.gov/glossary/term/brute_force_password_attack
Central Authentication Service (CAS)	CAS is a single sign-on (SSO) protocol that allows users to access multiple applications with one set of login credentials. This approach eliminates the need for users to remember multiple login credentials for different applications, reducing the risk of weak or reused passwords. CAS acts as a trusted intermediary between the user's identity provider and the service providers that the user wishes to access. It helps to enhance security by ensuring that users are authenticated only once and are then granted access to all applications that they are authorized to use. For example, a university may use CAS to provide access to various campus services, such as email, course management systems, and library resources, with one set of credentials.
Cloud Identity Management	Cloud identity management is the management of user identities and their access to resources that are stored and accessed in the cloud. It enables organizations to control user access to cloud-based applications and data through a central console. Cloud identity management provides authentication, authorization, and access management to cloud-based resources. It can be used to manage both employee and customer identities, with the aim of improving security, reducing administrative costs, and enhancing user experience. For example, an organization may use cloud identity management to manage access to cloud-based applications like Salesforce, Google Workspace, or Microsoft 365, ensuring that only authorized users have access to these applications.
Continuous Authentication	Continuous authentication is a security approach that verifies a user's identity on an ongoing basis, rather than just during the initial login. It helps to prevent unauthorized access by continuously monitoring user behavior, such as typing speed, mouse movements, and location, and comparing it to established patterns. Continuous authentication can help to detect and prevent account takeovers by identifying suspicious behavior in real-time. For example, a bank may use continuous authentication to monitor a customer's behavior while they are accessing their account, ensuring that any unusual activity is detected and addressed promptly.

Credential	A credential is a set of login credentials, such as a username and password, that a user provides to authenticate themselves to access a system or application. Credentials are used to verify a user's identity and ensure that only authorized individuals can access resources. The security of credentials is critical in protecting against unauthorized access to systems and data. For example, a user's credentials may include a username and password that they use to log in to their email account.
Customer Identity Access Management (CIAM)	Customer Identity Access Management (CIAM) is a subcategory of Identity Access Management (IAM) that focuses on managing and securing customer identities and their access to resources. CIAM solutions enable organizations to provide customers with seamless and secure access to digital services and applications, such as online shopping or banking, across multiple channels and devices. CIAM solutions typically include features such as identity verification, registration, authentication, authorization, and consent management. For example, a retailer may use CIAM to manage customer identities and access to their online store, ensuring that only authorized customers can make purchases.
Data Breach	A data breach occurs when unauthorized individuals gain access to sensitive or confidential information, such as personal information or financial data. Data breaches can occur due to a variety of reasons, such as cyber attacks, employee negligence, or physical theft. The consequences of a data breach can be severe, including financial loss, damage to reputation, and legal penalties. For example, a data breach at a healthcare organization may result in the theft of patient records, including medical history and personal information, which can be used for identity theft or sold on the dark web.
Data Breach Prevention	Data Breach Prevention is the practice of implementing security measures and strategies to avoid unauthorized access or disclosure of sensitive information. This is important in the IAM domain to protect the confidentiality, integrity, and availability of data. Data Breach Prevention includes implementing access controls, monitoring user activities, regularly updating security policies, and ensuring that all security systems are up to date. For example, an organization may deploy multifactor authentication and data encryption to protect data from unauthorized access.
Deprovisioning	Deprovisioning refers to the process of revoking access to resources when an employee or contractor leaves an organization or their role changes. This is a critical component of the IAM domain, as it ensures that former employees do not have access to sensitive information. Deprovisioning may involve disabling accounts, revoking permissions, and removing any associated digital certificates or keys. For instance, when an employee leaves an organization, their account should be deactivated, and access to their credentials should be revoked to prevent unauthorized access.

Digital Certificate	A Digital Certificate is an electronic document that verifies the identity of an entity and is used to establish secure communication between parties. In the IAM domain, digital certificates are commonly used for authentication and encryption purposes. They are issued by a trusted third party called a Certificate Authority (CA). For example, an organization may use digital certificates to authenticate the identity of employees accessing the network remotely or to encrypt sensitive data transmitted over the internet.
Directory Service	A Directory Service is a centralized database that stores and manages user and device identities and their attributes, such as access permissions, roles, and credentials. It is used to simplify and streamline user authentication and authorization in the IAM domain. For example, an organization may use a directory service such as Microsoft Active Directory to manage user identities and access permissions across multiple systems.
Employee Identity Management	Encryption is the process of converting plaintext into ciphertext using an algorithm and a key. It is used to protect the confidentiality of data in transit or at rest. Encryption is an essential component of the IAM domain, as it helps to prevent unauthorized access to sensitive information. For example, an organization may use encryption to protect sensitive data transmitted over the internet or stored on a device.
Encryption	Encryption is the process of converting plain text into an unreadable format using a cryptographic algorithm to protect the confidentiality, integrity and availability of data. In the context of IAM within Information Security, encryption is commonly used to protect sensitive data such as passwords, authentication tokens, and personal information stored in databases or transmitted over networks. Encryption helps to prevent unauthorized access, interception, or modification of the data by attackers or eavesdroppers. There are various encryption techniques and algorithms available, such as symmetric key encryption, asymmetric key encryption, and hashing. An example of encryption in IAM is the use of encrypted passwords. When users create an account, they are prompted to create a password. The password is then encrypted and stored in a database in an unreadable format using a strong encryption algorithm. When the user logs in, the password they enter is also encrypted and compared to the stored encrypted password. If the two encrypted values match, the user is granted access. This way, even if an attacker gains access to the database, they will not be able to read the passwords in plain text and use them to gain unauthorized access to the system.

Entity	An entity refers to a unique, identifiable actor in a computer system. In the context of cybersecurity, an entity can be a user, a device, an application, or a system that is identified and authenticated by an IAM system. Entities can have different roles and permissions within the system, and their actions and access to resources are typically logged for auditing and security purposes. An individual (person), organization, device, or process. Used interchangeably with "party". (Ref: NIST SP 800-102, NIST SP 800-89, NIST SP 800-152, NIST SP 800-175B Rev. 1, NIST SP 800-56B Rev. 2, NIST SP 800-57 Part 1 Rev. 5) A person, device, service, network, domain, manufacturer, or other party who might interact with an IoT device. (Ref: NIST SP 800-213, NISTIR 8259A, NISTIR 8259B)
Federated Identity	Federated Identity allows users to access multiple systems or applications using a single set of credentials, often provided by an Identity Provider (IdP).
Source:	https://www.gartner.com/en/information-technology/glossary/federated-identity-management#:~:text=Federated%20identity%20management%20enables%20identity,entities%20and%20across%20trust%20domains
Identity	An attribute or set of attributes that uniquely describe a subject within a given context.
Source:	https://csrc.nist.gov/glossary/term/identity
Identity as a Service (IDaaS)	Identity as a Service (IDaaS) is a cloud-based delivery model for IAM services. It allows organizations a secure way to manage and control identities, access, and privileges across multiple applications and platforms. IDaaS providers offer a range of services including user provisioning, authentication, single sign-on, and multifactor authentication. IDaaS enables businesses to reduce the complexity and cost of managing IAM systems in-house and to provide secure access to employees, partners, and customers from anywhere and on any device. For example, Okta is an IDaaS provider that offers a cloud-based platform for managing user identities and access to applications and data.

Identity and Access Management (IAM)	Identity and Access Management (IAM) refers to the policies, technologies, and processes that enable organizations to manage and control user identities, access, and privileges to systems and applications. IAM solutions typically include user provisioning, authentication, authorization, and auditing capabilities. IAM helps organizations to ensure that only authorized users can access sensitive data and applications and that access is granted based on the principle of least privilege. IAM also enables organizations to streamline user management processes and reduce the risk of insider threats. For example, a bank may use an IAM solution to manage the access of its employees and customers to its online banking platform, ensuring that only authorized users can perform transactions and access account information.
Identity Management	Identity Management (IM) is the process of managing and controlling user identities and access to systems, applications, and data. IM includes tasks such as user registration, authentication, authorization, and password management. The goal of IM is to ensure that only authorized users can access resources and that access is granted based on the principle of least privilege. IM is a critical component of information security and helps organizations to protect against unauthorized access and data breaches. For example, an organization may use an IM system to manage the identities and access of its employees and partners to its network and applications.
Identity Provider	An Identity Provider (IdP) is a service that manages and controls user identities and authentication in a federated identity environment. An IdP is responsible for verifying the identity of users and providing authentication tokens that enable users to access resources on behalf of an identity provider. IdPs are commonly used in single sign-on (SSO) scenarios, where users can access multiple applications and services using a single set of credentials. For example, Google provides an IdP service that enables users to use their Google accounts to access a range of third-party applications and services.
Identity Stores	Identity stores refer to databases or directories that store information about user identities and attributes. Identity stores are a critical component of IAM systems and enable organizations to manage user identities and access to systems and applications. Identity stores typically include information such as user names, passwords, email addresses, and access privileges. For example, Microsoft Active Directory is a popular identity store that is used by many organizations to manage user identities and access to resources.

Incident Response Planning	Incident Response Planning (IRP) is a process that organizations use to prepare for and respond to security incidents. IRP involves creating a plan that outlines the steps that will be taken in the event of a security incident, including identifying the incident, containing the damage, and restoring normal operations. IRP also involves training employees on how to respond to security incidents and conducting regular testing to ensure that the plan is effective. For example, an organization may have an IRP in place that outlines the steps that will be taken in the event of a data breach, such as notifying affected parties, conducting a forensic investigation, and implementing measures to prevent future incidents.
JSON Web Token (JWT)	JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA or ECDSA. Although JWTs can be encrypted to also provide secrecy between parties, we will focus on signed tokens. Signed tokens can verify the integrity of the claims contained within it, while encrypted tokens hide those claims from other parties. When tokens are signed using public/private key pairs, the signature also certifies that only the party holding the private key is the one that signed it.
Source:	https://jwt.io/introduction
Just in Time Access (JIT)	JIT access is a process of granting a level of access as fast as possible, at the time it is needed, and removed as soon as possible, after the access is no longer needed.
Source:	https://www.cyberark.com/what-is/just-in-time-access/
Least Privileged Access Control	Least Privilege Access Control is a mechanism through which an identity is provided just enough access to a resource to carry out the work - not more / not less. For example, if a Developer needs to create resources in Development Env for his application development work, he / she will be provided to create resources only in development env (and not in test / production env). This concept is very important for enhancing the security of a system and is critical for implementing Zero Trust principles.
Source:	https://csrc.nist.gov/glossary/term/least_privilege

Lightweight Directory Access Protocol (LDAP)	LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate data about organizations, individuals, and other resources such as files and devices in a network -- whether on the public internet or a corporate intranet. LDAP is a "lightweight" version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network. LDAP is considered lightweight because it uses a smaller amount of code than other protocols. A directory tells the user where in the network something is located. On TCP/IP networks -- including the internet -- the domain name system (DNS) is the directory system used to relate the domain name to a specific network address, which is a unique location on the network. However, the user may not know the domain name. LDAP allows a user to search for an individual without knowing where they're located, although additional information will help with the search.
Source:	https://www.techtarget.com/searchmobilecomputing/definition/LDAP#:~:text=LDAP%20(Lightweight%20Directory%20Access%20Protocol)%20is%20a%20software%20protocol%20for,internet%20or%20a%20corporate%20intranet
Lifecycle Management	Lifecycle Management is a process through which identities are managed throughout its lifecycle such as from creation to deletion. For example, in the Joiner - Mover - Leaver (JML) case, an employee joins an organization, his / her / their identity is created / granted certain access to systems / resources needed for their job execution. Later on, they move to a different department, their access to systems / resources are modified (added / deleted) to make sure they can do their job for his / her / their new department. Once that employee leaves the organization, his / her / their accesses are removed and ultimately, identities are deleted as per the corporate policy.
Machine Identity	A machine identity is a digital identity associated with a device or machine, such as a server, a computer, or a mobile device. Machine identities are used to authenticate and authorize devices and systems that access network resources. Examples of machine identities include a digital certificate or a security token that is used to establish trust between the device and the network.
Source:	https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8320C.ipd.pdf

Multifactor Authentication (MFA)	Multifactor Authentication is a mechanism through which an identity is authenticated through additional factors such as something you know, something you have or something you are. This is a very important technique in containing identity based attacks such as stolen user id / password etc. It is commonly used in authenticating identities before access is granted to critical systems such as finance, health etc. For example, someone logs onto his / her / their bank account through a web browser. After using the login / password, the system sends a message to the person's phone or any authenticator app to confirm the person's identities. This technique is also used in conditional access such as logging from an unknown device, unknown place / country (impossible travel) etc.
Non-Human Identity	A non-human identity refers to an identity that is not associated with a human user. This could include an identity associated with an automated process or service, such as a script or an application. Non-human identities are often used to perform tasks that are not performed by human users, such as running a scheduled task or accessing a web service. They also can be used in cases like Internet of Things devices or other machines that can interact with systems with certain permissions.
Source:	https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63a.pdf
Non-Person Entity	An entity with a digital identity that acts in cyberspace, but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts.
Source:	https://csrc.nist.gov/glossary/term/non_person_entity#:~:text=CNSSI%20 4009%2D2015%2C%20NIST%20SP,software%20applications%2C%20 and%20information%20artifacts
OAuth 2.0	OAuth 2.0 is a flexible framework for securing application access to protected resources through APIs. OAuth allows you to decouple clients and resources from the business processes and policy decisions used to authorize access. It's truly a framework, though, which means that it gives you a structure, but you ultimately must make the decisions about how to authorize access.
Source:	https://www.pingidentity.com/en/resources/blog/post/setting-oauth-security-policies-secure-access.html
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Source:	https://csrc.nist.gov/glossary/term/password#:~:text=memorized%20 secret%20show%20sources,or%20to%20verify%20access%20 authorization

Password Spray	Password spraying is a type of brute force attack. In this attack, an attacker will brute force logins based on a list of usernames with default passwords on the application. For example, an attacker will use one password (say, Secure@123) against many different accounts on the application to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. This attack can be found commonly where the application or admin sets a default password for the new users.
Source:	https://owasp.org/www-community/attacks/Password_Spraying_Attack#:~:text=Password%20spraying%20is%20a%20type,default%20passwords%20on%20the%20application
Passwordless Authentication	Passwordless authentication is signing into a service without using a password. This is often done with certificates, security tokens, one-time passwords (OTPs), or biometrics. Passwordless authentication is generally considered more secure than using passwords.
Source:	https://www.techtarget.com/searchsecurity/definition/passwordless-authentication
Phishing	A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information.
Source:	https://csrc.nist.gov/glossary/term/phishing#:~:text=NIST%20SP%20800%2D83%20Rev,Web%20site%20that%20requests%20information
Public-Key Infrastructure	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates.
Source:	https://csrc.nist.gov/glossary/term/pki#:~:text=Definition(s)%3A,and%20revoke%20public%20key%20certificates
Secure Socket Layer (SSL)	A popular implementation of public-key encryption, is an internet security protocol used by web browsers and servers to transmit sensitive information. SSL has become part of an overall security protocol known as Transport Layer Security (TLS). You can look in your browser to determine when a website is using a secure protocol such as TLS; locations of websites that use SSL begin with the prefix "https" rather than "http," and you will often see the icon of a closed padlock or a solid, unbroken key in your browser's address bar to indicate that SSL is enabled.
Source:	https://iam.harvard.edu/glossary

Secure Token Service (STS)	A Secure Token Service (STS) is a component that issues, validates, renews, and cancels security tokens for trusted systems, users, and resources requesting access within a federation.
Source:	https://docs.aws.amazon.com/STS/latest/APIReference/welcome.html
Secure Web Authentication (SWA)	A compatibility layer provided by Sign-On product, allowing the integration of legacy applications that don't support federated authentication and would not otherwise be able to take advantage of organization-wide single sign-on. The feature stores a unique password for each application, and securely posts the credentials directly to the application's authentication handler, resulting in a near-seamless SSO user experience.
Source:	https://www.okta.com/resources/identity-and-access-management-glossary/
Security Assertion Markup Language (SAML)	A language for exchanging authentication and authorization information. SAML standardizes the representation of credentials in an XML format called assertions, enhancing the interoperability between disparate applications.
Source:	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf/
Service Provider	A system that provides a generic service to the user in a federated system. To users, a service provider is the same thing as the application they are trying to use.
Source:	https://iam.harvard.edu/glossary
Shadow Access	Shadow Access is unauthorized, invisible, unsafe, and generally over permissioned access that has grown along with cloud identities, apps and data. Today, identities, human, and nonhuman are automatically created, along with access pathways to cloud data. Current tools are blind to many cloud identities and access pathways, creating vulnerabilities that are exploited to breach cloud data.
Source:	https://cloudsecurityalliance.org/blog/2023/03/16/shadow-access-in-your-cloud/
Single Sign-On (SSO)	SSO provides the capability to authenticate once, and be subsequently and automatically authenticated when accessing various target systems. It eliminates the need to separately authenticate and sign on to individual applications and systems, essentially serving as a user surrogate between client workstations and target systems. Target applications and systems still maintain their own credential stores and present sign-on prompts to client devices. Behind the scenes, SSO responds to those prompts and maps the credentials to a single login/password pair. SSO is commonly deployed in enterprise, Web, and federated models.
Source:	https://www.gartner.com/en/information-technology/glossary/

System for Cross-domain Identity Management (SCIM)	SCIM is a standard for modeling identity data through resources such as users and groups. It defines standard operations through a REST-based system for manipulating the resources as JSON objects.
Source:	https://www.okta.com/resources/identity-and-access-management-glossary/
Time-Based One-Time Password (TOTP)	An algorithmically-generated code that is deterministic based on the current date and time and a secret "seed" value. The server knows the seed, and can easily verify that a given code is valid for the current time period. TOTP can significantly increase security because even if a code is intercepted, it is worthless after the time window has passed (usually less than a minute). This makes the logistics of an attack much more difficult. TOTP can be implemented on a simple and inexpensive hardware device or on a smartphone. The seed is installed and is made difficult or impossible to recover or duplicate.
Source:	https://www.okta.com/resources/identity-and-access-management-glossary/
Token Authentication	A method of authenticating to an application using a signed cookie containing session state information. A more traditional authentication method is usually used to initially establish user identity, and then a token is generated for re-authentication when the user returns.
Source:	https://www.okta.com/resources/identity-and-access-management-glossary/
Two-Factor Authentication (2FA)	It requires two different proofs of identity to provide authentication.This authentication is a subset of multifactor authentication, and significantly increases security, because each authentication factor requires a different style of attack to compromise.
Source:	https://csrc.nist.gov/glossary/term/2fa
Universal Authentication Frameworks (UAF)	UAF is an open standard developed by the FIDO Alliance with the goal of enabling a secure passwordless experience for primary authentication, as opposed to a second factor as described in U2F. Under the spec, the user presents a local biometric or PIN and is authenticated into the service.
Source:	https://www.okta.com/resources/identity-and-access-management-glossary/
Universal 2nd Factor (U2F)	U2F is an open standard, whereby a hardware token device can attest the holder's identity through a challenge and response protocol. The token device is connected via USB or NFC (near-field communication). It is the standard maintained by the FIDO Alliance and is supported by Chrome, Firefox, and Opera.

Source:	https://www.okta.com/resources/identity-and-access-management-glossary/
User	A person or entity with authorized access.
Source:	https://csrc.nist.gov/glossary/term/user
User Provisioning	User provisioning or account provisioning technology creates, modifies, disables, and deletes user accounts and their profiles across IT infrastructure and business applications. Provisioning tools use approaches such as cloning, roles, and business rules so that businesses can automate onboarding, offboarding, and other administration workforce processes (for example, new hires, transfers, promotions and terminations). Provisioning tools also automatically aggregate and correlate identity data from HR, CRM, email systems, and other "identity stores." Fulfillment is initiated via self-service, management request, or HR system changes. Regulatory compliance and security efficiencies continue to drive most user-provisioning implementations.
Source:	https://www.gartner.com/en/information-technology/glossary/
WebAuthn	An evolution of the FIDO, U2F, and UAF protocols. WebAuthn continues in the FIDO tradition of allowing for using credentials for step up authentication. However, its biggest innovation is in enabling users to authenticate to services without necessarily needing the user to identify themselves first (through the use of a username and password combination).
Source:	https://www.okta.com/resources/identity-and-access-management-glossary/

Reference

https://csrc.nist.gov/glossary

https://www.okta.com/resources/identity-and-access-management-glossary/

https://iam.harvard.edu/glossary

https://www.gartner.com/en/information-technology/glossary

Acronyms

Acronym	Term
ABAC	Attribute-based Access Control
ACM	Access Control Mechanism
AD	Active Directory
ADAM	Active Directory Application Mode
ADFS	Active Directory Federation Services
ADSI	Active Directory Service Interface
API	Application Programming Interface
AuthN	Authentication
AutZ	Authorization
Azure AD	Azure Active Directory (Cloud)
CA	Certificate Authority
CASB	Cloud Access Security Broker
CBAC	Claims based Access Control
CSV	Comma separated Value (File)
DAC	Discretionary Access Control
DB	Database
DDNS	Dynamic DNS
DLL	Dynamic Link Library
DNS	Domain name Service
ERP	Enterprise Resource Planning
FIDO2	Fast Identity Online
GUID	Global Unique Identifier
GBAC	Graph Based Access Control
IA	Identity Assurance
IAM	Identity and Access Management
IGA	Identity Governance and Administration

IDaaS	Identity as a Service
IdM	Identity Management
IdP	Identity Provider
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Directory Interface Format
MAC	Mandatory Access Control
MFA	Multifactor Authentication
MSP	Managed service Provider
MX Record	Mail eXchange Record
OID	Object Identifier
OAuth	Open Authorization
OrBAC	Organization Based Access Control
OTP	One time Password
PACS	Physical Access Control Systems
PAM	Privileged Access Management
PAP	Policy Administration Point
PAT	Port Address Translation
PBAC	Policy Based Access Control
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIM	Privileged Identity Management
PIP	Policy Inforcement Point
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PUM	Privileged User Management
RBAC	Role-Based Access Control
REST	Representational State Transfer
RFID	Radio-frequency Identification

RSBAC	Rule Set Based Access Control
RSO	Reduced Sign-On
SaaS	Software as a Service
SAM	Security Account Manager
SAML	Security Assertion Markup Language
SCIM	Simple Cloud Identity Management
SDK	Software Development Kit
SEM	Security Event Management
SIEM	Security Information Event Management
SIM	Security Information Management
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SoD	Segregation/Separation of Duties
SoR	System of Record
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSO	Single Sign-On
SSPR	Self-Service Password Reset
STS	Secure Token Service
TLS	Transport Layer Security
UI	User Interface
VDS	Virtual Directory Services
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language