Terminology in the IDPro Body of Knowledge

Heather Flanagan, editor - @ 2022 IDPro

Editor's Note: *This is a consolidated list of the terminology highlighted in each of the articles published in the Body of Knowledge (BoK). It is not, by any means, a definitive or even broadly supported set of definitions; the context an individual reader brings to the table will influence how accurate the terminology for their use case. We offer the consolidated list here as a touchpoint for discussion. Article authors are encouraged to review and use existing definitions before offering new ones for terms already described in the BoK.*

Please consider offering feedback to the articles that use these terms via the IDPro GitHub repository: https://github.com/IDPros/bok.

Term	Definition	Source
Abstraction	the practice of identifying and isolating repeated aspects of operations or business logic so that they can be maintained in one place and referenced in many places.	Introduction to Policy-Based Access Controls (v2)
Access Certification	Certification is the ongoing review of who has which accesses (i.e., the business process to verify that access rights are correct).	Introduction to Identity - Part 1: Admin-time (v2), Techniques To Approach Least Privilege
Access Control	Controlling who can have access to data, systems, services, resources, locations. The 'Who' can be a user, a device or thing, a service	Introduction to Access Control
Access Control	Various methods to limit access to data, systems, services, resources, locations by a user, a device or thing, or a service.	IAM Reference Architecture

Access Control Lists	Access Control Lists are definitions around who or what are allowed or denied access to a resource. For example, a file share may have an Access Control List that allows Marketing Department users to read and write, IT Department users to read-only, and denies all other users' access.	Authentication and Authorization
Access Control System	a structure that manages and helps enforce decisions about access within an organization.	Introduction to Policy-Based Access Controls (v2)
Access Governance	The assurance that all access has been given based on the correct decision criteria and parameters	Introduction to Access Control
Access Governance	Access Governance provides oversight and control over access rights implemented in multiple local or shared authorization systems. These rights may be controlled in a variety of ways, starting with the existence and validity of the digital identity. Other controls include various mechanisms such as policies, the mapping of roles, permissions, and identities. The abbreviation used is for Identity Governance and Administration and is commonly used in the commercial sector. This roughly corresponds to the Access Certification section of the first-class component Governance Systems in the FICAM model. IGA is not specifically addressed in the ISO/IEC model.	IAM Reference Architecture
Access Management	Use of identity information to provide access control to protected resources such as computer systems, databases, or physical spaces.	Introduction to IAM Architecture

Access Management	The process and techniques used to control access to resources. This capability works together with identity management and the Relying Party to achieve this goal. The model shows access management as a conceptual grouping consisting of the Access Governance function and the shared authorization component. However, access management impacts local authorization as well (through the governance function).	IAM Reference Architecture
Access Policy	Definition of the rules to allow or disallow access to secured objects.	Introduction to Access Control
Access Requester	The person, process, system, or thing that seeks to access a protected resource.	Introduction to Access Control
Access Supplier	The component granting access to data, systems, services after the access policy requirements (set in the Policy Administration Point) have been met by the Access Requester.	Introduction to Access Control
Account Owner	An entity that "owns" or claims responsibility for an account. Generally, an account is issued in the name of the owner(s) or their delegate(s) in the case of enterprises.	Account Recovery (v2)
Account Recovery	The process of returning account access to an account owner when they lose, forget, or cannot otherwise produce the account's nominal credentials. This may be accomplished in person, remote, or in a hybrid format.	Account Recovery (v2)
Account Recovery	The process of updating a user's credentials within a scenario where the user cannot validate those credentials	Managing Identity in Customer Service Operations

Account Takeover	Account takeover is a form of identity theft and fraud, where a malicious third party successfully gains access to a user's account credentials.	Account Recovery (v2), Designing MFA for Humans, Techniques To Approach Least Privilege
Accountability	The obligation of a person to accept the results of one's actions, be they positive or negative. This person is probably also a species of an owner.	Introduction to Access Control
Action	a protected operation available for a resource, such as "view", "edit", or "submit".	Introduction to Policy-Based Access Controls (v2)
Adaptive Authentication	Adaptive authentication aims to determine and enforce the authentication level required at any time during a user session - when the session is commenced, during the session when access requirements force a re-evaluation, or when the session token expires. The factors to be used in achieving that authentication level are determined dynamically based on the access control policy governing the resources being accessed, and a variety of environmental conditions and risk factors in effect at that time for that user.	Designing MFA for Humans
Agent (also "Customer Service Agent")	The person responsible for communicating with and solving problems on behalf of customers or end-users.	Account Recovery (v2), Managing Identity in Customer Service Operations
Agile Project Management	A framework that uses a continuous, iterative process to deliver a defined piece of functionality, typically a component of a product or service. Scrum is a popular framework	Introduction to IAM Project Management

	(https://www.scrumalliance.org/about-scrum/overview)	
Architecture	Framework for the design, deployment, and operation of an information technology infrastructure. It provides a structure whereby an organization can standardize the technology it uses and align its IT infrastructure with digital transformation policy, IT development plans, and business goals.	Introduction to IAM Architecture
Architecture Overview	Describes the architecture components required for supporting IAM across the enterprise.	Introduction to IAM Architecture
Architecture Patterns	Identifies the essential patterns that categorize the IT infrastructure architecture in an organization and will guide the deployment choices for IAM solutions.	Introduction to IAM Architecture
Assertion	A formal message or token that conveys information about a principal, typically including a level of assurance about an authentication event and sometimes additional attribute information. Sometimes this is called a Security Token.	IAM Reference Architecture
Assurance Level	A category describing the strength of the identity proofing process and/or the authentication process. See NIST SP.800-63-3 for further information.	IAM Reference Architecture
Asymmetric Cryptography	Any cryptographic algorithm which depends on pairs of keys for encryption and decryption. They are referred to as asymmetric because one key encrypts, and the other decrypts. And the keys are not shared between parties.	Practical Implications of Public Key Infrastructure for Identity Professionals

Attribute Provider	Sometimes the authority for attributes is distinguished from the authority for identities. In this case, the term Attribute Provider is sometimes used. It is a subset or type of an Identity Information Authority.	IAM Reference Architecture
Attribute-Based Access Control (“ABAC”) / Claims-Based Access Control (“CBAC”)	a pattern of access control system involving dynamic definitions of permissions based on information (“attributes”, or “claims”), such as job code, department, or group membership.	Introduction to Policy-Based Access Controls (v2)
Attributes	Key/value pairs relevant for the digital identity (username, first name, last name, etc.).	An Overview of the Digital Identity Lifecycle (v2)
Audit Repository	A component that stores records about all sorts of events that may be useful later to determine if operations are according to policy, support forensic investigations, and allow for pattern analysis. Typically, this is highly controlled to prevent tampering. Audit Repository is the ISO name for this concept and is localized to the IDM. In this model, the term is generalized to indicate a service that supports event records from any part of the ecosystem.	IAM Reference Architecture
Authentication	Authentication is the process of proving that the user with a digital identity who is requesting access is the rightful owner of that identity. Depending on the use-case, an ‘identity’ may represent a human or a non-human entity; may be either individual or organizational; and may be verified in the real world to a varying degree, including not at all.	Introduction to Access Control (v3), Authentication and Authorization

Authentication (AuthN)	The act of determining that to a level of assurance, the principal/subject is authentic.	IAM Reference Architecture
Authenticator	The means used to confirm the identity of a user, processor, or device, such as a username and password, a one-time pin, or a smart card.	Identity and Access Management Workforce Planning
AuthN Assertion	A security token whereby the IDP provides identity and authentication information securely to the RP.	IAM Reference Architecture
Authoritative Source	The system of record (SOR) for identity data; an organization may have more than one authoritative source of data in their environment.	User Provisioning in the Enterprise
Authorization	Determining a user's rights to access functionality with a computer application and the level at which that access should be granted. In most cases, an 'authority' defines and grants access, but in some cases, access is granted because of inherent rights (like patient access to his/her own medical data)	Introduction to Access Control, Authentication and Authorization
Authorization (AuthZ)	Authorization is how a decision is made at run-time to allow access to a resource. We break this down into two types: shared and local. The FICAM framework includes this as a subcomponent of the Access Management System. AuthZ is not included in the ISO or Internet2 models.	IAM Reference Architecture
Automatic Certificate Management Environment (ACME)	A communication protocol for automating interactions between Private Key Holders and Certificate Authorities. Based on JSON and HTTP, it is widely deployed to support the	Practical Implications of Public Key Infrastructure for Identity Professionals

	issuance of TLS certificates for web servers.	
Bilateral Federation	A bilateral federation is one that consists of only two entities: one Identity Provider (IdP) and one Service Provider (SP). This is the most common model for an enterprise identity federation.	Federation Simplified (v2)
Binding	Associating an authenticator with an identity.	Identity and Access Management Workforce Planning
Bot	Sometimes called an Internet bot, short for 'robot' but referring to a software routine that performs automated tasks over the Internet or a web robot referring to an autonomous network application, or simply a 'bot' referring to an automated, typically repetitive, task used for a specific purpose.	Non-Human Account Management (v2)
Ceremonies	Predictable interactions that users can infrequently navigate in a well-watched place	Introduction to Identity – Part 2: Access Management
Certificate Authority Trust List (CTL)	A list of Trusted Certificate Authorities maintained by a client.	Practical Implications of Public Key Infrastructure for Identity Professionals
Certificate Management System (CMS)	A system that provides a management and reporting layer around certificate issuance and revocation. They can integrate with CA products from multiple vendors, as well as IGA and Service Desk systems.	Practical Implications of Public Key Infrastructure for Identity Professionals
Certificate Policy (CP)	A document that defines the high-level policy requirement for a PKI. The outline for a CP is described RFC 3647, which identifies the policy framework	Practical Implications of Public Key Infrastructure for Identity Professionals

	for PKI. A certificate policy is typically published to external parties so that they can determine whether to trust certificates issued by the CA publishing the CP	
Certificate Practices Statement (CPS)	A document using the RFC 3647 format which identifies the Practices which implement the requirements documented in the CP. Unlike the CP, the CPS is rarely published in unredacted form.	Practical Implications of Public Key Infrastructure for Identity Professionals
Certificate Revocation List (CRL)	A list of revoked certificates published by a Certificate Authority	Practical Implications of Public Key Infrastructure for Identity Professionals
Certificate Signing Request (CSR)	When requesting a certificate, the requesting entity provides a copy of the public key along with their name and other information in a specially formatted binary object called a CSR.	Practical Implications of Public Key Infrastructure for Identity Professionals
Channel	The communication avenue between you and your end-user, or your agent and their customer. This could be phone, chat, social media, or others.	Managing Identity in Customer Service Operations
CIA Triad	The fundamental Information security concepts of risk classification of resources from the perspectives of Confidentiality, Integrity, and Availability.	Non-Human Account Management (v2)
Claims-Based Access Control (CBAC)	See Attribute-Based Access Control (ABAC)	Introduction to Policy-Based Access Controls (v2)
Classical Computer	A computer that uses binary encoding and Boolean logic to make calculations in a deterministic way. Classical Computers are usually contrasted with Quantum Computers.	Practical Implications of Public Key Infrastructure for Identity Professionals

Cloud Infrastructure Entitlement Management (CIEM)	a categorization of technologies focused on managing the granting, verification, and refinement of permissions for cloud and hybrid technologies. CIEM is often seen as a component of Identity Governance and Administration (IGA)	Techniques To Approach Least Privilege
Competency Model	A collection of tasks, knowledge, and skills (TKS) needed for effective job performance. A competency model is part of a workforce framework.	Identity and Access Management Workforce Planning
Consent	Permission for something to happen or agreement to do something.	Introduction to Privacy and Compliance for Consumers
Consumer Protection Law	Laws and regulations that are designed to protect the rights of individual consumers and to stop unfair, deceptive, and fraudulent business practices.	Laws Governing Identity Systems
Context	conditions under which an action on a resource is authorized for a subject, such as time of access, location of access, or a compliance state.	Introduction to Policy-Based Access Controls (v2)
Continuous Authentication	Continuous authentication is a mechanism that uses a variety of signals and measurements to determine during a user session if there is any change in the confidence that it is still the same user that authenticated at the beginning of the session, and trigger an authentication action if there is a drop in confidence.	Designing MFA for Humans
Contract Law	Laws that relate to making and enforcing agreements between or among separate parties.	Laws Governing Identity Systems

Credential	A credential allows for authentication of an entity by binding an identity to an authenticator.	IAM Reference Architecture
Credential Management	How to issue, manage, and revoke authenticators bound to identities. Credential Management roughly corresponds to the IDPro term for Credential Services; we use the term Credential Management here to correlate to the Federal Identity, Credential, and Access Management (FICAM) initiative's terms.	Identity and Access Management Workforce Planning
Credential Service Provider	Following the guidance included in NIST 800-63-3, we include both the enrollment function and credential services together under the name Credential Services Provider.	IAM Reference Architecture
Credential Services	Credential Services issue or register the subscriber authenticators, deliver the credential for use, and subsequently manage the credentials. We include PKI information for IAM architectures that must include system components that need certificates and private keys. This roughly corresponds to the FICAM component called Credential Management Systems.	IAM Reference Architecture
Credentials	Any attribute or shared secret that can be used to authenticate a user.	Account Recovery (v2)
Cryptographic Module Validation Program (CMVP)	A program allowing cryptographic module developers to test their modules against the requirements defined in FIPS-140. Compliant modules are listed on a US government-run website	Practical Implications of Public Key Infrastructure for Identity Professionals
Data Controller	Defined in Article 4(7) of the GDPR: "'controller' means the natural or legal person, public authority, agency or	An Introduction to the GDPR

	other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;". This article uses the term "organisation" as a synonym for "data controller", since organisations involved in IAM will normally be data controllers.	
Data Mapping	"a system of cataloguing what data you collect, how it's used, where it's stored, and how it travels throughout your organization and beyond."	Impact of GDPR on Identity and Access Management
Data Processor	Defined in Article 4(8) of the GDPR for situations where an organisation processes personal data solely on the instructions of others. A Data Processor must not determine the purposes of processing, for example by processing in its own interests, or, beyond limited technical choices, the means of doing so. Data Processors are regulated by Article 28: in particular they must have a contract with the Data Controller that covers all the subjects listed in Article 28(3). Data Processors are excluded from some, but not all, of the liabilities and duties of Data Controllers.	An Introduction to the GDPR
Data Protection by Design	Data protection through technology design. See GDPR Article 25 for more detail	Impact of GDPR on Identity and Access Management
Data Protection Officer	An individual who must be appointed in any organization that processes any data defined by the GDPR as sensitive. The DPO is responsible for "Working towards the compliance with all relevant data protection laws, monitoring specific processes, such as	Impact of GDPR on Identity and Access Management

	data protection impact assessments, increasing employee awareness for data protection and training them accordingly, as well as collaborating with the supervisory authorities."(See GDPR Articles 35, 37, 38, and 39 for more detail)	
Data Subject	Defined in Article 4(1) of the GDPR (see "Personal Data" above) as the formal term for the human to whom personal data relates. This article uses the term "individual" as a synonym for "data subject".	An Introduction to the GDPR
Decentralized Identifier (DID)	An identifier that is created and anchored in a decentralized system such as a blockchain or ledger and can represent any entity in the ecosystem – an issuer, a holder, a verifier, and even an identity hub.	A Peek into the Future of Decentralized Identity
Delegated Authorization Framework	An access control framework that decouples authentication from authorization, allowing the password to stay local and protected	Introduction to Identity – Part 2: Access Management
Digital Cards	Represent verifiable credentials that users collect over time and are stored as part of the user agent or the identity hub of the user. It's somewhat simpler to refer to them as digital cards rather than verifiable credentials when speaking about them.	A Peek into the Future of Decentralized Identity
Digital Identity	the combination of a unique identifier together with relevant attributes that uniquely identifies an entity..	An Overview of the Digital Identity Lifecycle (v2)
Digital Wallet	represents a digital metaphor for a physical wallet and is generally represented by the combination of the user agent and the underlying capabilities of the computing device,	A Peek into the Future of Decentralized Identity

	such as secure storage and secure enclaves on a mobile phone. The digital wallet contains digital cards.	
Directory	A directory is a central repository for user identities and the attributes that make up those identities. A user identity might be John Smith with firstName attribute as John, lastName attribute as Smith, title attribute as Director, and Department attribute as Marketing. The attributes in the directory can be used to make authorization decisions about what this user should have access to in applications.	Authentication and Authorization
Discretionary Access Control	a pattern of access control system involving static, manual definitions of permissions assigned directly to users.	Introduction to Policy-Based Access Controls (v2)
dPKI	A decentralized public key infrastructure and is usually implemented via an immutable blockchain or ledger – a place where DIDs can be registered and looked up alongside the associated public keys of the DID and its metadata. dPKI can be described more generally as the *verifiable data registry*, as the dPKI is just one of many possible implementations for a verifiable data registry. While this paper refers to dPKI, the reader should be aware that a verifiable data registry need not necessarily be “decentralized”.	A Peek into the Future of Decentralized Identity
Electronic Identification, Authentication and Trust Services (eIDAS)	European legislation that gives legal standing to electronic signatures. This legislation also documents how to provide legally binding digital signatures with X.509 certificates to comply with Qualified Signature.	Practical Implications of Public Key Infrastructure for Identity Professionals

Elliptic Curve Cryptography (ECC)	An asymmetric cryptosystem based on calculations of points along elliptic curves.	Practical Implications of Public Key Infrastructure for Identity Professionals
Encryption	Processing data using a cryptographic algorithm to provide confidentiality assurance.	Practical Implications of Public Key Infrastructure for Identity Professionals
Enforcement	The mechanism that ensures an individual cannot perform an action or access a system when prohibited by policy.	IAM Reference Architecture
Enrollment	Also known as Registration. Enrollment is concerned with the proofing and lifecycle aspects of the principal (or subject). The entity that performs enrollment has sometimes been known as a Registration Authority, but we (following NIST SP.800-63-3) will use the term Credential Service Provider.	IAM Reference Architecture
Enterprise Architecture	An architecture covering all components of the information technology (IT) environment	Introduction to IAM Architecture
Entitlement	The artifact that allows access to a resource by a principal. This artifact is also known as a privilege, access right, permission, or an authorization. An entitlement can be implemented in a variety of ways.	IAM Reference Architecture
Entitlement Catalog	A database of entitlements and their related metadata. The catalog includes an index of entitlement data pulled from business systems, applications, and platforms, as well as technical and business descriptions of the entitlements or their use	User Provisioning in the Enterprise

Entitlement Management	Cataloging and managing all the accesses an account may have. This is the business process to provision access.	Introduction to Identity - Part 1: Admin-time (v2)
External identifier	The means by which a person in control of a digital identity refers to that identity when interacting with a system	Identifiers and Usernames
Federal Agency Smart Credential Number (FASC-N)	A unique identifier associated with a smart card. Used in the US Federal Government PIV standard to support Physical Access.	Practical Implications of Public Key Infrastructure for Identity Professionals
Federal Information Processing Standard **(“**FIPS”) 140	A NIST standard defining “Security Requirements for Cryptographic Modules.	Practical Implications of Public Key Infrastructure for Identity Professionals
Federated Access Controls	an access control architecture that accommodates separation of user/subject authority and resource/object authority.	Introduction to Policy-Based Access Controls (v2)
Federated Identity	The means of linking a person’s electronic identity and attributes, stored across multiple distinct identity management systems	Introduction to Identity – Part 2: Access Management
Fractured Identity	A case where a single end-user has multiple disparate digital identities.	Managing Identity in Customer Service Operations
Fraud Law	Laws that protect against the intentional misrepresentation of information made by one person to another, with knowledge of its falsity and for the purpose of inducing the other person to act, and upon which the other person relies with resulting injury or damage.	Laws Governing Identity Systems

Gantt Chart	A popular schedule format that displays both activity and timeframes in a single chart	Introduction to Project Management for IAM Projects
General Data Protection Act (GDPR)	Formally, Regulation 2016/679 of the European Union, in force May 25, 2018. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679	An Introduction to the GDPR
Groups	A set of identities with defined permissions. In this specific context, a group contains many individuals, but the group identity is opaque, and no information is available regarding which group member took an individual action.	Practical Implications of Public Key Infrastructure for Identity Professionals
Hardware Security Module (HSM)	A hardware device that generates and protects cryptographic keys.	Practical Implications of Public Key Infrastructure for Identity Professionals
Holder	The entity that holds verifiable credentials. Holders are typically users but can also be organizations or devices.	A Peek into the Future of Decentralized Identity
Identification	Uniquely establish a user of a system or application.	Introduction to Access Control
Identifier	The way a system refers to a digital identity. PKI Certificates support both internal and external identifiers. See Ian Glazer's article, "Identifiers and Usernames," for a generic overview of identifiers.	Practical Implications of Public Key Infrastructure for Identity Professionals
Identity	Defining attributes for a human user that may vary across domains, e.g., a user's digital identity will have a different definition in a work environment as opposed to the user's	Non-Human Account Management (v2)

	bank. A device identifier is sometimes referred to as its identity.	
Identity Analytics and Intelligence (IdA)	Identity analytics and intelligence mean looking at entitlement data, looking at the assignment of that, and trying to figure out and define what risk looks like. IdA provides a risk-based approach for managing system identities and access, with the intention of centralizing governance, visibility, and reporting for access-based risk.	Introduction to Identity - Part 1: Admin-time (v2)
Identity and Access Management (IAM)	Identity and Access Management (IAM) is the discipline used to ensure the correct access is defined for the correct users to the correct resources for the correct reasons.	Authentication and Authorization
Identity and Access Management (IAM)	The discipline that enables the right individuals to access the right resources at the right times for the right reasons.	Identity and Access Management Workforce Planning
Identity and Access Management Workforce Planning	Activities involved in ensuring an enterprise identity and access management team are staffed with the right talent to execute business and technical objectives.	Identity and Access Management Workforce Planning
Identity, Credential, and Access Management (ICAM)	Programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and non-person entities, bind those identities to credentials that may serve as a proxy in access transactions, and leverage the credentials to provide authorized access to an organization's resources.	Identity and Access Management Workforce Planning
Identity Federation	An identity federation is a group of computing or network providers that agree to operate using standard	Federation Simplified (v2)

	protocols and trust agreements. In a Single Sign-On (SSO) scenario, identity federation occurs when an Identity Provider (IdP) and Service Provider (SP) agree to communicate via a specific, standard protocol. The enterprise user will log into the application using their credentials from the enterprise rather than creating new, specific credentials within the application. By using one set of credentials, users need to manage only one credential, credential issues (such as password resets) can be managed in one location, and applications can rely on the appropriate enterprise systems (such as the HR system) to be the source of truth for a user's status and affiliation. Identity federations can take several forms. In academia, multilateral federations, where a trusted third party manages the metadata of multiple IdPs and SPs, are fairly common. [1]This article focuses, however, on the enterprise use case where **bilateral federation** arrangements, where the agreements are one-to-one between an IdP and an SP, are the most common form of identity federation in use today.	
Identity Governance and Administration (IGA)	a discipline that focuses on identity life cycle management and access control from an administrative perspective.	Introduction to Identity - Part 1: Admin-time (v2)
Identity Governance and Administration (IGA)	Includes the collection and use of identity information as well as the governance processes that ensure the right person has the right access to the right systems at the right time.	Introduction to IAM Architecture

Identity Hub or Repository	The place where users can store their encrypted identity-related information. An identity hub can be anywhere – on the edge, on the cloud, or on your own server. Its purpose is to store personal data. Some implementations may allow other entities to access the identity hub of the user if the user specifically grants such access. You can think of an identity hub as the individual's personal data store.	A Peek into the Future of Decentralized Identity
Identity Information Authority (IIA)	This represents one or more data sources used by the IDM as the basis for the master set of principal/subject identity records. Each IIA may supply a subset of records and a subset of attributes. Sometimes the IIA is distinguished from the Identity Information Provider or IIP. We use IIA to include the service that actually provides the information as well as the root authority. This corresponds to Identity Information Source in ISO/IEC 24760-2 and Identity Sources in Internet2.	IAM Reference Architecture
Identity Lifecycle Management	A process that detects changes in authoritative systems of record and updates identity records based on policies.	User Provisioning in the Enterprise
Identity Management (IDM)	A set of policies, procedures, technology, and other resources for maintaining identity information. The IDM contains information about principals/subjects, including credentials. It also includes other data such as metadata to enable interoperability with other components. The IDM is shown with a dotted line to indicate that it is a	IAM Reference Architecture

	conceptual grouping of components, not a full-fledged system in itself.	
Identity Proofing	accruing evidence to support "who this is." Identity proofing is the last, but not the least, important part of this admin-time section. This is the process of collecting and verifying information about a person for the purpose of providing an account or a corresponding credential. This is typically performed before an account is created or the credential is issued, or a special privilege is granted.	Introduction to Identity - Part 1: Admin-time (v2)
Identity Provider (IdP)	An Identity Provider (IdP) performs a service that sends information about a user to an application. This information is typically held in a user store, so an identity provider will often take that information and transform it to be able to be passed to the service providers, AKA apps. The OASIS organization, which is responsible for the SAML specifications, defines an IdP as "A kind of SP that creates, maintains, and manages identity information for principals and provides principal authentication to other SPs within a federation, such as with web browser profiles."	Federation Simplified (v2), Authentication and Authorization
Identity Provider (IDP)	Identity Provider or IDP is a common term. We treat this as a subset of Identity Management. It consists of the service interfaces: AuthN/Assertion, Service Provisioning Agent, Session Management, Discovery Services, and Metadata Management.	IAM Reference Architecture
Identity Register	This is the datastore that contains the enrolled entities and their attributes,	IAM Reference Architecture

	including credentials. See the IDM section for elaboration. The terms Directory, Identity Repository, and Attribute Store are sometimes used as synonyms.	
Identity Repository	The identity repository is a directory or a database that can be referenced by external systems and services (such as authentication or authorization services).	User Provisioning in the Enterprise
Identity Theft Law	Laws governing crimes in which the perpetrator gains access to sensitive personal information belonging to the victim (such as birth dates, passwords, email addresses, driver's license numbers, social security numbers, financial records, etc.), and then uses this information to impersonate the victim for personal gain, such as to commit fraud, establish credit in the victim's name, or access the victim's accounts.	Laws Governing Identity Systems
Impersonation	A scenario where a user is able to perform actions as though they are a known user other than themself.	Managing Identity in Customer Service Operations
Infrastructure-as-code	the process of managing and provisioning computer data centers through machine-readable definition files rather than physical hardware configuration or interactive configuration tools.	Techniques To Approach Least Privilege
Internet Key Exchange (IKE)	A subordinate standard under IPsec which specifies how to use X.509 certificates to establish symmetric keys for an IPsec tunnel.	Practical Implications of Public Key Infrastructure for Identity Professionals
Internet Protocol Security (IPsec)	A standard for communication between two machines providing	Practical Implications of Public Key Infrastructure for Identity Professionals

	confidentiality and integrity over the Internet Protocol.	
Intra-organizational (Single Sign-On):	A central digital identity, such as an account in a directory, is linked by downstream systems as authoritative for authentication.	An Overview of the Digital Identity Lifecycle (v2)
Inter-organizational (Federation)	An organization relies on another organization's digital identity and lifecycle management processes.	An Overview of the Digital Identity Lifecycle (v2)
Internal identifier	The way an identity management system refers to a digital identity	Identifiers and Usernames
Issuer	The entity that issues verifiable credentials about subjects to holders. Issuers are typically a government entity or corporation, but an issuer can also be a person or device.	A Peek into the Future of Decentralized Identity
Joiner/Mover/Leaver	The joiner/mover/leaver lifecycle of an employee identity considers three stages in the life cycle: joining the organization, moving within the organization, and leaving the organization.	Introduction to Identity - Part 1: Admin-time (v2)
Journey-based Creation	The process that guides a customer through a series of interactions prior to establishing a digital identity. For example, capturing the minimum basic information needed from a customer to enable creation of an identity.	An Overview of the Digital Identity Lifecycle (v2)
Just-in-time (JIT) Access	a technique where a credential or a permission is granted to a principal for a temporary timeframe when they need the permission to perform an activity. Access is revoked once the activity is complete, limiting its usage.	Techniques To Approach Least Privilege

Key	In a cryptosystem, a Key is a piece of information used to encrypt or decrypt data in a cryptographic algorithm.	Practical Implications of Public Key Infrastructure for Identity Professionals
Knowledge-Based Authentication (KBA)	A method of authentication that uses information known by both the end-user and the authentication service but is not necessarily a secret.	Account Recovery (v2), Managing Identity in Customer Service Operations
Least Privilege	Also known as the Principle of Least Privilege; a resource, such as a user, must only be able to access the resources (e.g., applications, data) that are necessary for it to function.	Introduction to Identity – Part 2: Access Management
Least Privilege	The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. (NIST Information Technology Laboratory)	Techniques To Approach Least Privilege
Local Authorization	Local authorization is handled by the RP.	IAM Reference Architecture
Metadata Management	The processes and techniques that allow the collection, use, and eventual deletion of control data used by the IDM to recognize and trust the Relying Party. This corresponds to Relying Party data in the Internet2 model.	IAM Reference Architecture
Multi-Factor Authentication (MFA)	An approach whereby a user's identity is validated to the trust level required according to a security policy for a resource being accessed using more than one factor (something you know (e.g., password), something you have (e.g., smartphone), something you are (e.g., fingerprint).	Account Recovery (v2), Introduction to Access Control

Multilateral Federation	A federation that consists of multiple entities that have agreed to a specific trust framework. There are several forms of multilateral federations, including hub-and-spoke and mesh. Multilateral federations are the most common model for academic identity federations.	Federation Simplified (v2)
National Institute of Standards and Technology (NIST)	A US Government agency that defines and publishes standards. One department within NIST, the Computer Security Resource Center ("CSRC"), publishes the Federal Information Processing Standards ("FIPS") series. While these standards are only mandatory for US Government Agencies, they are widely recognized as de-facto standards globally.	Practical Implications of Public Key Infrastructure for Identity Professionals
Non-Human/Person Account	Any account not used by a person, such as accounts used for devices, services, and servers.	Non-Human Account Management (v2)
Non-Person Entities	Any unique combination of hardware, software firmware (e.g., device) that utilizes the capabilities of other programs, devices, or services to perform a function. Non-person entities may either act independently or on behalf of an authenticated individual or NPE	Practical Implications of Public Key Infrastructure for Identity Professionals
OAuth 2.0	OAuth 2.0 is an open-source protocol that allows Resource Owners such as applications to share data with clients by facilitating communication with an Authorization Server. That data takes the form of credentials given to applications to obtain information/data from other applications. The Authorization Server is usually the Identity Provider (IdP).	Federation Simplified (v2)

	The Authorization Server (AS) may provide authorization directly or indirectly. For example, the AS may supply attributes or profile data of the Resource Owner or provide access to data that can later be used for authorization purposes, such as entitlements from an Identity Management or Governance Solution.	
Online Certificate Status Protocol (OCSP)	A protocol that allows a client to query the Certificate Authority or a Validation Authority for the status of an individual certificate rather than downloading a CRL.	
OpenID Connect (OIDC)	OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol. It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.	Federation Simplified (v2)
Path Discovery and Validation (PDVal)	The process to determine whether a certificate is valid and trusted by the validator.	Practical Implications of Public Key Infrastructure for Identity Professionals
Permission	a statement of authorization for one or more subjects to perform one or more actions on one or more objects.	Introduction to Policy-Based Access Controls (v2)
Personal Data	Defined in Article 4(1) of the GDPR: "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a	An Introduction to the GDPR

	name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;". Note: "natural person" (human) is used to distinguish from companies and other corporate entities that are "legal persons".	
Personal Data	Personal data are any information which are related to an identified or identifiable natural person.	Account Recovery (v2), Impact of GDPR on Identity and Access Management
Personal Identification Number (PIN)	A numeric secret commonly used to unlock a private key container in software or hardware	Practical Implications of Public Key Infrastructure for Identity Professionals
Personal Identity Verification (PIV)	A US Government program designed to enable strong authentication for all government employees and contractors, based on Public Key Infrastructure.	Practical Implications of Public Key Infrastructure for Identity Professionals
Policy Access Point (PAP)	The location where the different types of owners define the access policy.	Introduction to Access Control
Policy Decision Point (PDP)	The policy engine validating Access requests and provided attributed against the Access Policy (as defined in the Policy Administration Point).	Introduction to Access Control
Policy Enforcement Point (PEP)	The authority that will only let an Access Requester connect to the Access Supplier if the Policy Decision Point allows it.	Introduction to Access Control
Policy Engine	It is a security component that validates whether an actor is allowed to access a protected resource, following the requirements in an access policy.	Introduction to Access Control

Policy Information Point	The authority that refers to the (external) trusted providers of attributes that will be used in the Access Decision. An example is the myacclaim.com service that administers Open Badges of certifications, such as CISSP and MSCP.	Introduction to Access Control
Policy-Based Access Control (PBAC)	a pattern of access control system involving dynamic definitions of access permissions based on user attributes (as in ABAC) and context variables for permitting or denying access.	Introduction to Policy-Based Access Controls (v2)
Principle of Least Privilege	an information security best practice ensuring that users in an access control system do not have more access to resources than is necessary for their intended activities.	Introduction to Policy-Based Access Controls (v2)
Privacy	An abstract concept, with no single, common definition	Introduction to Privacy and Compliance for Consumers
Privacy Law	Laws that regulate the collection, use, storage, and transfer of personal data relating to identified or identifiable individuals.	Laws Governing Identity Systems
Private Key	A key that is exclusively and privately controlled by a single entity. It corresponds to a public key that the entity may share for data encryption or signature verification.	Practical Implications of Public Key Infrastructure for Identity Professionals
Privileged Access Management	A mechanism for managing temporary access for accounts with high-risk permissions. PAM often involves check-out and check-in of a credential generated for a single use.	Techniques To Approach Least Privilege
Privileged Account Management (PAM)	focusing on special control for risky high-level access. Privileged Account Management (PAM) is a mechanism	Introduction to Identity - Part 1: Admin-time (v2)

	for getting those special accounts under control.	
Processing	Defined in Article 4(2) of the GDPR: "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". Note that even this long list of activities is not exhaustive: other activities may also fall within the definition of "processing". Additional rules, in Article 22, apply to "automated individual decision-making, including profiling". These generally have the effect of strengthening the rights of information and objection described later and may limit the use of automation for some high-impact decisions.	An Introduction to the GDPR
Project	A time-limited activity to achieve a defined outcome(s)	Introduction to Project Management for IAM Projects
Project Charter	Documented authority for the project manager to proceed with a project; it will usually include a succinct statement of the project's purpose	Introduction to Project Management for IAM Projects
Project Plan	A document that describes a project; it will usually include a scope statement, schedule, resource plan, communications plan, and quality plan	Introduction to Project Management for IAM Projects

Public Key	A key that is publicly distributed by an entity that is used with the corresponding private key.	Practical Implications of Public Key Infrastructure for Identity Professionals
Public Key Certificate	A certificate containing a public key, one or more identifiers for the private key holder, an identifier for the Certificate Authority, and additional metadata to support security requirements.	Practical Implications of Public Key Infrastructure for Identity Professionals
Public Key Infrastructure	A set of tools, standards, and related policies designed to manage trust based on public/private key pairs and certificates.	Practical Implications of Public Key Infrastructure for Identity Professionals
Protected Resource	A system, a process, a service, an information object, or even a physical location that is subject to access control as defined by the owner of the resource and by other stakeholders, such as a business process owner or Risk manager.	Introduction to Access Control
Reconciliation	The process of identifying and processing changes to users and user access made directly on target systems.	User Provisioning in the Enterprise
Registration Authority (RA)	An individual, system, or business function which provides registration and identity proofing for entities receiving certificates and manages the certificate issuance and renewal process. The most important responsibilities of an RA include identity proofing and binding of the private key to the identity.	Practical Implications of Public Key Infrastructure for Identity Professionals
Relying Party (RP)	A component, system, or application that uses the IDP to identify its users. The RP has its own resources and logic. Note that the term 'relying	IAM Reference Architecture

	service' is used in the ISO/IEC standards to encompass all types of components that use identity services, including systems, sub-systems, and applications, independent of the domain or operator. We will use the more common Relying Party (or RP). An RP roughly corresponds to the Agency Endpoint in the FICAM model or to Identity Consumers in the Internet2 model.	
Resource or Object	an asset protected by access controls, such as an application, system, or door.	Introduction to Identity - Part 1: Admin-time (v2)
Revised Payment Systems Directive (PSD2)	PSD2 (the Revised Payment Services Directive, Directive (EU) 2015/2366) is an EU Directive, administered by the European Commission (Directorate General Internal Market) to regulate payment services and payment service providers throughout the European Union (EU) and European Economic Area (EEA). It contains many requirements specifically related to Strong Client Authentication.	Designing MFA for Humans
Risk Context (RCTX)	Risk Context consists of additional facts that can be brought to bear to improve the overall security of the ecosystem. Internal or external events and facts can be applied to enable, limit, or terminate access. This is similar to the section Monitors and Sensors under FICAM's Governance Systems and to many of the inputs of the Policy Decision Point in the NIST Special Publication 800-207, a paper on Zero Trust.	IAM Reference Architecture
Role Management	a way to group access rules to make them more manageable	Introduction to Identity - Part 1: Admin-time (v2)

Role-Based Access Control (RBAC)	the use of roles at run-time; a way to govern who gets access to what through the use of roles.	Introduction to Identity - Part 1: Admin-time (v2)
Role-Based Access Control (RBAC)	a pattern of access control system involving sets of static, manual definitions of permissions assigned to "roles", which can be consistently and repeatably associated with users with common access needs.	Introduction to Identity - Part 1: Admin-time (v2)
Roles	An entity that defines a set of permissions. A role must be associated with an individual user, and the user gains the associated authorization during the time that they are associated with the role.	Practical Implications of Public Key Infrastructure for Identity Professionals
RSA	An asymmetric cryptosystem based on large prime numbers. The acronym RSA stands for the three principal inventors, Ron Rivest, Adi Shamir, and Len Adleman.	Practical Implications of Public Key Infrastructure for Identity Professionals
S/MIME	A standard for constructing and sending digitally signed or encrypted messages using asymmetric cryptography	Practical Implications of Public Key Infrastructure for Identity Professionals
Schedule	A document that defines the activity and resources required to achieve the planned deliverable(s) and outcome(s)	Introduction to Project Management for IAM Projects
Secure Socket Layer (SSL)	A deprecated standard for encrypting data in transit; it has been superseded by TLS.	Practical Implications of Public Key Infrastructure for Identity Professionals
Security Assertion Markup Language (SAML)	SAML is an XML-based communication protocol between SPs and IdPs. Usually, the enterprise hosts the IdP, whereas applications (including cloud services) are the SPs.	Federation Simplified (v2)

Segment	a grouping of subjects that may be useful for authorizations, such as full-time employees, undergraduate students, IT administrators, or clinicians.	Introduction to Policy-Based Access Controls (v2)
Self-sovereign Identity	A term that describes a digital movement that is founded on the principle that an individual should own and control their identity without the intervening administrative authorities.	A Peek into the Future of Decentralized Identity
Server Account	An account with privileged access rights to a server's operation typically used for configuration purposes.	Non-Human Account Management (v2)
Server-based Certificate Validation Protocol (SCVP)	A protocol that allows a client to query a server to determine whether a certificate is valid and trusted. The server does not need to be associated with the issuing CA SCVP does two things; (1) it determines the path between the end-entity and the trusted root whereby the client doesn't need to trust any intermediate CAs. (2) it also performs delegated path validation according to policy.	Practical Implications of Public Key Infrastructure for Identity Professionals
Service Account	An account used by a computer application to access other applications or services for a specific purpose.	Non-Human Account Management (v2)
Service Provider (SP)	Defined by the OASIS organization, which is responsible for the SAML specification, as "A role donned by a system entity where the system entity provides services to principals or other system entities." This usually takes the form of an application that offers services requiring authentication and authorization to a user.	Federation Simplified (v2)

Session	A period of time after an authentication event when an RP grants access to resources for the principal/subject. The duration of the session and the mechanism for enforcement vary by implementation.	IAM Reference Architecture
Session Management	A coordinating function provided by an IDP to control sessions of subscribing RPs.	IAM Reference Architecture
Shared Authorization	Shared authorization is provided by a facility outside of the RP. It is shown here as part of the access management grouping.	IAM Reference Architecture
Signature	Processing data using a cryptographic algorithm to provide integrity assurance.	Practical Implications of Public Key Infrastructure for Identity Professionals
Single Sign-On	Single Sign-On is a service that enables SPs to verify the identities of End Users by facilitating communication with IdPs. SSO acts as a bridge to decouple SPs and IdPs. This can happen via numerous protocols such as agent-based integrations, direct LDAP integration, SAML, and OpenID Connect, to name a few.	Federation Simplified (v2)
Social Engineering	Social engineering is a method of manipulating people so they give up confidential information, such as passwords or bank information, or grant access to their computer to secretly install malicious software.	Account Recovery (v2), Designing MFA for Humans
Sources of "Truth"	where authoritative data about individuals live.	Introduction to Identity - Part 1: Admin-time (v2)
Special Category Data (SCD)	Categories of data that are regarded as particularly sensitive, so subject to additional regulation. Defined in	An Introduction to the GDPR

	Article 9(1) of the GDPR as “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”; Article 10’s “personal data relating to criminal convictions and offences” requires similar treatment, so is normally considered as another category of SCD.	
Step-Up Authentication	A method to increase the level of assurance (or confidence) the system has regarding a user’s authentication by issuing one or more additional authentication challenges, usually using factors different from the one(s) used to establish the initial authenticated session. The need for increasing the level of assurance is typically driven by the risk associated with the sensitive resource the user is attempting to access.	Designing MFA for Humans
Subject Alternative Name	One or more identifiers for a certificate subject that can be used to carry application-specific identifiers such as email address or User Principle Name (UPN).	Practical Implications of Public Key Infrastructure for Identity Professionals
Subject Distinguished Name (Subject DN)	A unique identifier for the Subject, within the scope of the Certificate Authority. Subject DN is structured like an LDAP entry name.	Practical Implications of Public Key Infrastructure for Identity Professionals
System Account	A generic term for a privileged account that has extensive permissions that enable system configuration changes.	Non-Human Account Management (v2)

Task	Lowest level of defined activity; multiple tasks will typically be grouped into stages of project phases	Introduction to Project Management for IAM Projects
Threat Modeling	Threat modeling is an analysis technique used to help identify threats, attacks, vulnerabilities, and countermeasures that could impact an application or process.	Account Recovery (v2), Designing MFA for Humans
Tort Law	The body of law that covers situations where one person's behavior causes injury, suffering, unfair loss, or harm to another person, giving the injured person (or the person suffering damages) a right to bring a civil lawsuit for compensation from the person who caused the injury. Examples include battery, fraud, defamation, negligence, and strict liability.	Laws Governing Identity Systems
Transport Layer Security ("TLS")	A cryptographic protocol designed to provide confidentiality and integrity of communications between two endpoints.	Practical Implications of Public Key Infrastructure for Identity Professionals
Trust Federation	a trust framework between multiple entities with the purpose of leveraging identity and access management information in a controlled fashion	Introduction to Identity – Part 2: Access Management
Trust Framework	This component represents the legal, organizational, and technical apparatus that enables trust between the IDM and the RPs.	IAM Reference Architecture
Trust Root	A technical structure that provides the IDP and RP the ability to recognize each other with a high degree of certainty. This is similar to the concept of Trust Anchor (NIST SP.800-63-3), but we allow for a structure that relies on a mutually agreed-upon third party. A	IAM Reference Architecture

	trust root derives from the operation of a Trust Framework.	
Two-Factor Authentication (2FA)	A specific case of Multi-Factor Authentication (see: IDPro's Consolidated Terminology) where two factors must be checked to validate a user's identity.	Designing MFA for Humans
Universal Resolver	An identifier resolver that works with any decentralized identifier system through DID drivers. The purpose of a universal resolver is to return a DID document containing DID metadata when given a specific DID value. This capability is very useful because DIDs can be anchored on any number of disparate dPKI implementations.	A Peek into the Future of Decentralized Identity
User or Subject	a person or entity who may receive access within an access control system.	Introduction to Policy-Based Access Controls (v2)
User Agent	A user agent is any software that retrieves, renders, and facilitates end-user interaction with Web content.	Cloud Service Authenticates Via Delegation – SAML
User Provisioning	The means by which user accounts are created, maintained, and deactivated/deleted in a system according to defined policies.	User Provisioning in the Enterprise
User Provisioning and Lifecycle Management	how user records get where they need to be but only as long as they are needed	Introduction to Identity - Part 1: Admin-time (v2)
Username	a common term used for an external identifier	Identifiers and Usernames
Username	An identifier unique to the authentication service used in conjunction with a shared secret to authenticate a user.	Account Recovery (v2), Managing Identity in Customer Service Operations

Validator	An entity that verifies a certificate and confirms that the other party controls the private key in the transaction.	Practical Implications of Public Key Infrastructure for Identity Professionals
Verifiable Credentials	Attestations that an issuer makes about a subject. Verifiable credentials are digitally signed by the issuer.	A Peek into the Future of Decentralized Identity
Verifiable Presentations	The packaging of verifiable credentials, self-issued attestations, or other such artifacts that are then presented to verifiers for verification. Verifiable presentations are digitally signed by the holder and can encapsulate all the information that a verifier is requesting in a single package. This is also the place where holders can describe the specific terms of use under which the presentation is performed.	A Peek into the Future of Decentralized Identity
Verifier	The entity that verifies verifiable credentials so that it can provide services to a holder.	A Peek into the Future of Decentralized Identity
Workforce Framework	An outline of the job categories, work roles, and competency models needed to execute workforce planning.	Identity and Access Management Workforce Planning
Workforce Planning	Activities that ensure an organization has the right talent to execute business and technical objectives.	Identity and Access Management Workforce Planning
X.509	An ISO standard from the X.500 series that defines the basic rules for encoding public key certificates.	Practical Implications of Public Key Infrastructure for Identity Professionals
Zero Standing Privilege (ZSP)	a state where JIT access is used for all permissions and no long-standing permissions are assigned to principals.	Techniques To Approach Least Privilege

Zero Trust	From NIST Draft Special Publication 800-207, “Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet)”	Introduction to Identity – Part 2: Access Management