# Glossary of Key Terms

The terms and definitions listed in this glossary are used throughout the Identity Information Management Standards Package to define key terms in the context of Identity Information Management.

| Term | Definition | Source |
|---|---|---|
| Access Control | The processes by which access to resources are permitted or denied | Claims Information Standard |
| Access Management | A set of principles, practices, policies, processes and procedures that are used within an organization, to manage access to information | Identity Information Management Architecture Summary |
| AP | see **Authoritative Party** | Identity Assurance Standard |
| Application (Desktop) | An Information System that is accessed by a user through software on their computer; the client software may also interact with a server application over a network such as the internet or intranet | Claims Technology Standard |
| Application (Web-based) | An Information System that is accessed by a user via a web browser over a network such as the Internet or an intranet | Claims Technology Standard |
| Assurance | see **Identity Assurance** | Identity Assurance Standard |
| Assurance Level | see **Identity Assurance Level** and **Transaction Assurance Level** | Identity Assurance Standard |
| Authentication (Business) | The act of establishing or confirming something (or someone) as authentic, that is that claims made by or about the thing are true | Identity Assurance Standard |
| Authentication (technical) | The process by which an individual or system's identity is determined by another by verifying the presented credentials | Electronic Credential and Authentication Standard |
| Authentication Level | Relative measure (i.e., low, medium, high, very high) of the strength of an authentication event | Identity Assurance Standard |
| Authoritative Party | An organization or individual that is trusted to be an authority on the identity related attributes or roles associated with users and subjects of services. Authoritative Parties may issue credentials.<br>see **Credential Service Providers** | Identity Assurance Standard |

| Term | Definition | Source |
|---|---|---|
| Authoritative Party Proxy | An organization or system that acts on behalf of the original authoritative source | Claims Information Standard |
| Authorization | The process to validate that a person has the permission to use a protected resource | Identity Information Reference Model |
| Biometric | Physiological or behavioral aspects of an individual that can be measured and used to identify or verify that individual | Identity Assurance Standard |
| Biometric Authentication | The automated use of biometric attributes to establish or verify an individual's identity (biometric recognition) | Identity Assurance Standard |
| Business Role | Users may be associated with one or more "business roles" which describe the business function of the user. For each business role there is an Authoritative Party that manages the definition and use of the business role | Claims Information Standard |
| Claim<br>(business) | An assertion that something is true.<br>(NOTE: for the purposes of the Identity Information Management Standards Package, 'claim' is used as related to identity)<br>see **Identity Claim** | Identity Assurance Standard |
| Claim<br>(technical) | An attribute related to an identity in a particular context | Claims Information Standard |
| Claims Based Architecture | An Architecture describing a scalable, privacy enhancing and secure way to exchange identity information (claims) between parties using electronic services | Identity Information Management Architecture Summary |
| Claims Technology Profile | Profile describing a specific secure communication protocol of requesting claims and sending claims between Information Systems or applications | Claims Technology Standard |
| Contact information | Information used to contact an individual or organization | Evidence of Identity Standard |
| Context | see **Identity Context** | Identity Assurance Standard |
| Credential | A physical or electronic object (or identifier) that is issued to, or associated with, one party by another party and attests to the truth of certain stated facts and/or confers a qualification, competence, status, clearance or privilege. Identity credentials can be | Identity Assurance Standard |

| Term | Definition | Source |
|---|---|---|
| | cards, like a driver's license or smart card; documents like a passport; or, in the context of digital identities, a User ID and password or digital certificate | |
| Credential Service Provider | A party that issues and manages a credential (over its lifecycle) that asserts identity attributes or privileges associated with an individual | Identity Assurance Standard |
| Credential Strength | A measure of the ability of the credential to withstand attack or compromise | Identity Assurance Standard |
| Credential Strength Level | Relative measure (i.e., low, medium, high, very high) of the strength that can be placed in a credential | Identity Assurance Standard |
| Digital Certificate | An electronic credential that binds the identity of a user, organization or computer to their public key | Electronic Credential and Authentication Standard |
| Digital Identity | The electronic representation of a set of characteristics by which a person or thing is definitively recognized or known | Claims Technology Standard |
| Digital Signature | An electronic signature that can be used to authenticate the identity of the sender of an electronic message or the signer of a digital document. Considered to be legally binding | Claims Technology Standard |
| Electronic Credential | A digital object or document that contains a token, such as a password or cryptographic key, used for authentication to bind to a digital identity. | Electronic Credential and Authentication Standard |
| Evidence of Identity | The information, types of evidence and verification processes that, when combined, provide sufficient confidence that individuals are who they say they are | Evidence of Identity Standard |
| Federation<br>(technical) | A technical approach where one security domain has a system to authenticate users and another security domain has a system that trusts the authenticating system | Claims Technology Standard |
| Foundation Identity Credential | A credential that establishes the foundation of an individual's identity in Canada (e.g. Birth Certificate, Citizenship Card, etc) | Evidence of Identity Standard |
| Given name | A name other than a surname (includes first and middle names) | Evidence of Identity Standard<br>(Adapted from the BC Name Act) |

| Term | Definition | Source |
|---|---|---|
| Identification | The process of associating identity-related attributes with a particular person | Identity Assurance Standard |
| Identification Level | Relative measure (i.e., low, medium, high, very high) of the strength associated with an identification process | Identity Assurance Standard |
| Identity | A set of characteristics by which a person or thing is definitively recognized or known | Identity Assurance Standard |
| Identity Agent | Software on an individual's personal computer or other device that acts on behalf of the individual by facilitating the flow of identity claims about the individual between Authoritative Parties and Relying Parties | Claims Technology Standard |
| Identity Assurance | A measure of confidence that an identity claim or set of claims is true | Identity Assurance Standard |
| Identity Assurance Level | Relative measure (i.e., low, medium, high, very high) of the strength of assurance that can be placed in an identity claim or set of claims | Identity Assurance Standard |
| Identity Assurance Model | A four level model that illustrates several key concepts about Identity Assurance Levels, their relationship to Transaction Assurance Levels and their dependency on registration processes, credential strength, authentication events and the underlying operational infrastructure and processes | Identity Assurance Standard |
| Identity Claim | An assertion of the truth of something which pertains to a person's identity<br><br>An identity claim could convey a single attribute such as an identifier (e.g. a student number) or it could convey that a person is part of a certain group or has certain entitlements (e.g. I am over 18, I am a company employee)<br><br>A set of identity claims could provide sufficient identity attributes (e.g. name, date of birth address) to permit the identification of a person | Identity Assurance Standard |
| Identity Context | The environment or circumstances in which identity information is communicated and perceived. Individuals operate in multiple identity contexts (e.g., legal, social, employment, business, pseudonymous) and identify themselves differently based on the context | Identity Assurance Standard |
| Identity information | A set of attributes used to describe a person and | Evidence of Identity |

| Term | Definition | Source |
|---|---|---|
| | may be used to distinguish a unique and particular individual or organization | Standard |
| Identity Information Management | A set of principles, practices, policies, processes and procedures that are used within an organization to manage identity information and realize desired outcomes concerning identity | Identity Information Management Architecture Summary |
| Identity Metasystem | A model and architecture that represents how existing identity management infrastructure can be leveraged to provide secure access to information and systems. Similar to claims-based architecture | Claims Technology Standard |
| Identity Provider | see **Authoritative Party** | Claims Technology Standard |
| Identity Selector | see **Identity Agent** | Identity Assurance Standard |
| IDIM | see **Identity Information Management** | Identity Information Management Architecture Summary |
| Information Card | A digital representation of an identity card. Contains a reference to the Identity Provider that issued it where a user can get a security token containing claims about their digital identity | Claims Technology Standard |
| Legal Name | A name that a person uses for official or legal purposes | Evidence of Identity Standard |
| Multi-factor authentication | Authentication that utilizes one or more credentials that incorporate multiple factors (e.g., something you know, something you have, or something you are) | Electronic Credential and Authentication Standard |
| Multi-factor credential | A credential that utilizes multiple factors of different types (e.g., something you know, something you have, or something you are) for authentication | Identity Assurance Standard |
| Name | Given name or surname (or both) of an individual | Evidence of Identity Standard<br>(adapted from the BC Name Act) |
| Password Authentication | The use of a password (a character string) known only by the user to verify an individual's identity | Electronic Credential and Authentication Standard |

| Term | Definition | Source |
|---|---|---|
| Personal Information | Recorded information about an identifiable individual other than business contact information | Freedom of Information and Protection of Privacy Act (RSBC 1996, c. 165) |
| PIN | Personal Identification Number. A numeric password | Electronic Credential and Authentication Standard |
| Pseudonym | A fictitious name used by an individual to conceal or obscure his or her identity | Evidence of Identity Standard |
| Registering Organization | A organization that collects and verifies identity claims a person makes during a registration process | Evidence of Identity Standard |
| Relying Party (RP)<br>(business) | A party that controls access to a resource or service and relies on an Authoritative Party to provide identity assurance and identity related attributes about a user or subject | Identity Assurance Standard |
| Relying Party (RP)<br>(technical) | An electronic service that requests claims about users from one or more Authoritative Parties so that it can apply its own security or access control policies to determine whether to allow the user access to a resource or service | Claims Technology Standard |
| RP | see **Relying Party** | Identity Assurance Standard |
| Security Token | A package of data that contains claims that typically are digitally signed and encrypted to ensure security. It is used to prove identity to obtain access to a resource or service | Claims Technology Standard |
| Smart Card | A high strength credential with an embedded chip that can be used for authentication | Electronic Credential and Authentication Standard |
| Surname | The last name of a person (includes a family name and patronymic such as 'Mac' or '-son') | Evidence of Identity Standard<br>(adapted from BC Name Act) |
| Transaction Assurance Level | A pre-established assurance level (i.e., low, medium, high, very high) that applies to a transaction or service. It pre-sets the level of certainty in an identity claim that is needed to access information or | Identity Assurance Standard |

| Term | Definition | Source |
|---|---|---|
| | conduct a transaction | |
| User Centric | In the context of Identity Management, this describes providing users with choice, consent and control when sharing their identity and related information. This term also describes providing a consistent user experience and creating a less confusing service environment | Identity Information Management Architecture Summary |
| Web Services | A technical approach to support interoperable machine-to-machine interaction over a network. The interaction may be to exchange information or invoke an action. It typically uses SOAP XML-based messages communicated over HTTP/HTTPS | Claims Technology Standard |