# PCTF Key Concepts Lexicon

**Abstract:** details to come

| Term | Definition | Source(s) |
|---|---|---|
| **Anonymous Credential** | A credential that, while still making an assertion about some property, status, or right of the person, does not reveal the person's identity. A credential may contain identity attributes but still be treated as anonymous if the identity attributes are not recognized or used for identity validation purposes.<br><br>Anonymous credentials provide persons with a means by which to prove statements about themselves and their relationships with public and private organizations anonymously. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Assigned Identifier** | A numeric or alphanumeric string that is generated automatically and that uniquely distinguishes between individuals without the use of any other identity characteristics. | Guideline on Identity Assurance, Dec 2015, TBS<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Assurance** | A measure of certainty that a statement or fact is true. | Standard on Identity and Credential Assurance, TBS<br><br>Guideline on Identity Assurance, Dec 2015, TBS<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |

| | | |
|---|---|---|
| **Assurance level** | A level of confidence that may be relied on by others. | Standard on Identity and Credential Assurance, TBS<br><br>Guideline on Identity Assurance, Dec 2015, TBS<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Attribute** | See **Identity Attribute** | |
| **Authentication** | The process of establishing truth or genuineness to generate an assurance. | Guideline on Defining Authentication Requirements, TBS<br><br>Guideline on Identity Assurance, Dec 2015, TBS<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Authoritative Party** | A federation member that provides assurances of credential or identity to other members (i.e., **relying parties**) | Standard on Identity and Credential Assurance, TBS<br><br>Guideline on Identity Assurance, Dec 2015, TBS<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |

| | | |
|---|---|---|
| **Authoritative Source** | A collection or registry of records maintained by an authority that meets established criteria. | Standard on Identity and Credential Assurance, TBS<br><br>Guideline on Identity Assurance, Dec 2015, TBS<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Biological or Behavioural Characteristic Confirmation** | A process that compares biological (anatomical and physiological) characteristics in order to establish a link to an individual (for example, facial photo comparison). | Standard on Identity and Credential Assurance, TBS<br><br>Guideline on Identity Assurance, Dec 2015, TBS<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Biometrics** | A general term used alternatively to describe a characteristic or a process.<br><br>As a characteristic, it can refer to a measurable biological (anatomical and physiological) or behavioural characteristic that can be used for automated recognition.<br><br>As a process, it can refer to automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioural characteristics. | Biometrics Consortium Glossary<br><br>Guideline on Identity Assurance, Dec 2015, TBS<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |

| | | |
|---|---|---|
| **Business Event** | A significant discrete episode that occurs in the life span of a business. By law, a business event must be recorded with a government entity and is subject to legislation and regulation.<br><br>Examples of business events are registration of charter, merger, amalgamation, surrender of charter, and dissolution. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Conformance Criteria** | Criteria used to assess a trusted process or a set of trusted processes, and to provide evidence that these trusted processes are carried out with integrity. | Verified Person Conformance Profile, IMSC |
| **Credential** | A unique physical or electronic object (or identifier) issued to, or associated with, a person, organization or device (e.g. key, token, document, program identifier). | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Credential Assurance** | The assurance that a person, organization or device has maintained control over the credential with which they have been entrusted (e.g. key, token, document, identifier) and that the credential has not been compromised (e.g. tampered with, corrupted, modified). | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Credential Assurance Level** | The level of confidence that a person, organization, or device has maintained control over the credential with which they have been entrusted (e.g. key, token, document, identifier) and that the credential has not been compromised (e.g. tampered with, corrupted, modified). | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Credential Risk** | The risk that a person, organization, or device has lost control over the credential with which they have been entrusted. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Documentary evidence** | Any physical record of information that can be used as evidence. This is widely understood to mean information written on paper, but the more general definition is preferable. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |

| | | |
|---|---|---|
| **Document Authentication** | The process of confirming the authenticity of a document: genuine, counterfeit, forged, etc.<br><br>Document authentication is achieved by checking the security features of a document, such as secure laminate, holographic images, etc. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Electronic or Digital Evidence** | Any data that are recorded or preserved on any medium in, or by, a computer system or other similar device. Examples include database records, audit logs and electronic word processing documents. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC<br><br>Guideline on Identity Assurance, Dec 2015, TBS |
| **Evidence of Identity** | A record from an authoritative source that supports the integrity and accuracy of the claims made by a person.<br><br>Evidence of identity falls into two major categories: **Foundational Evidence of Identity** and **Supporting Evidence of Identity**. | Verified Person Component Overview, Version 1.0, IMSC<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC<br><br>Guideline on Identity Assurance, Dec 2015, TBS |
| **Federation** | A cooperative agreement between autonomous entities that have agreed to relinquish some of their autonomy in order to work together effectively to support a collaborative effort. The federation is supported by trust relationships and standards to support interoperability. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |

| | | |
|---|---|---|
| **Foundational Evidence of Identity** | Issued by a government institution relating to the registration of a vital or major life event, foundational evidence of identity is used to establish core identity information such as given name(s), surname, date of birth and place of birth.<br><br>Examples of foundational evidence of identity include, but are not limited to: birth certificates, permanent resident cards, and certificates of citizenship. | Verified Person Component Overview, Version 1.0, IMSC |
| **Identifier** | The set of identity attributes used to uniquely distinguish a unique and particular person, organization, or device. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Identity** | A reference or designation used to distinguish a unique and particular person, organization or device. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Identity Assurance** | A measure of certainty that a person, organization or device is who or what it claims to be. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Identity Assurance Level** | The level of confidence that a person, organization or device is who or what it claims to be. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Identity Attribute** | A property or characteristic associated with an identifiable person, organization, or device (also known as "identity data element"). | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Identity Claim** | An assertion of the truth of something that pertains to a person's identity. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Identity Context** | A set of circumstances, a situation or a scenario in which an individual interacts with other individuals or with an organization. | Guideline on Identity Assurance, Dec 2015, TBS |

| | | |
|---|---|---|
| **Identity Establishment** | The creation of an authoritative record of identity that is relied on by others for subsequent government activities, programs, and services. | Verified Person Component Overview, Version 1.0, IMSC<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Identity Fraud** | The deceptive use of personal information in connection with frauds such as the misuse of debit/credit cards or applying for loans using stolen personal information. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Identity Information** | The set of identity attributes that is sufficient to distinguish one person from all other persons within a program/service population and that is sufficient to describe the person as required by the program or service. Identity information is a subset of personal information. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Identity Issuance** | The creation of evidence of identity that is issued to an individual and can relied on by others for subsequent government activities, programs, and services. | Verified Person Component Overview, Version 1.0, IMSC |
| **Identity Maintenance** | The process of ensuring that identity information is as accurate, complete, and up-to-date as is required.<br><br>Identity maintenance also includes **identity notification**. | Verified Person Component Overview, Version 1.0, IMSC |
| **Identity Management** | The set of principles, practices, processes and procedures used to realize an organization's mandate and its objectives related to identity. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC<br><br>Standard on Identity and Credential Assurance, TBS<br><br>Guideline on Identity Assurance, Dec 2015, TBS |

| | | |
|---|---|---|
| **Identity Notification** | The disclosure of identity information triggered by a change in identity information, (e.g., a vital or a major life event) or an indication that identity information has been exposed to a risk factor. | Pan-Canadian Identity Notification Standard |
| **Identity Resolution** | The establishment of the uniqueness of a person within a program/service population through the use of identity information. | Verified Person Component Overview, Version 1.0, IMSC<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Identity Risk** | The risk that a person, organization or device is not who or what it claims to be. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Identity Validation** | The confirmation of the accuracy of identity information about a person as established by an authoritative party.<br><br>It should be noted that identity validation does not ensure that the person is using their own identity information (this is identity verification) – only that the identity information the person is using is accurate and up to date. | Verified Person Component Overview, Version 1.0, IMSC<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Identity Verification** | The confirmation that the identity information being presented relates to the person who is making the claim.<br><br>It should be noted that identity verification is a separate process from identity validation and may employ different methods and use personal information that is not related to identity. | Verified Person Component Overview, Version 1.0, IMSC<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |

| | | |
|---|---|---|
| **Knowledge-based Confirmation** | A process that compares personal or private information (i.e., shred secrets) to establish a person's identity.<br><br>Examples of information that can be used for knowledge-based confirmation include passwords, personal identification numbers, hint questions, program-specific information and credit or financial information. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Level of Assurance** | See **Assurance level** | |
| **Linkage** | The process of determining that identity information relates to the individual making the claim. | Guideline on Identity Assurance, Dec 2015, TBS |
| **Personal Information** | Information about an identifiable individual. | Notice and Consent Conformance Profile, Version 0.2, DIACC |
| **Physical Possession Confirmation** | A process that requires physical possession or presentation of evidence to establish a person's identity. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Relying Party** | A federation member that relies on assurances of credential or identity from other federation members (i.e., **authoritative parties**). | Standard on Identity and Credential Assurance, TBS<br><br>Guideline on Identity Assurance, Dec 2015, TBS<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |

| | | |
|---|---|---|
| **Supporting Evidence of Identity** | Issued by a government institution or a private sector organization, supporting evidence of identity is used for the purpose of program administration or to facilitate service delivery. Supporting evidence of identity:<br><br>• corroborates existing foundational evidence of identity or the corresponding authoritative record;<br>• assists in linking identity information to a presenting individual; and<br>• may provide information in addition to identity information such as an address of residence.<br><br>Examples of supporting evidence of identity include, but are not limited to: driver's licences and health cards. | Verified Person Component Overview, Version 1.0, IMSC |
| **Trusted Digital Identity** | An electronic representation of a person, used exclusively by that person, to receive valued services and to carry out transactions with trust and confidence. A person can be a 'natural person' (e.g., an individual) or it can be a 'legal person', which includes corporations and other organizations. | Verified Person Component Overview, Version 1.0, IMSC |
| **Trusted Process** | A business process or activity (or a set of business processes or activities) that results in a process output upon which others rely. | Verified Person Component Overview, Version 1.0, IMSC<br><br>Verified Person Conformance Criteria, IMSC |
| **Trusted Referee Confirmation** | A process that relies on a trusted referee to establish a link to a person. The trusted referee is determined by program-specific criteria. Examples of trusted referees include guarantors, notaries and certified agents. | PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |

| | | |
|---|---|---|
| **Trust Framework** | A formalized scheme that ensures that federation members have continued confidence in one another. A trust framework formally underpins trust relationships by stipulating adherence to standards, formalizing assessment processes, and defining roles and responsibilities of multi-party arrangements. | Guideline on Identity Assurance, Dec 2015, TBS<br><br>PCIM Validation Standard, Version 1.9, Aug 2016, IMSC |
| **Trust Relationship** | A defined arrangement or agreement that ensures confidence between the parties to the relationship | Guideline on Identity Assurance, Dec 2015, TBS |
| **Verified Person** | Knowing (or having a degree of certainty) that an individual is real, identifiable, and has truthfully claimed who he or she is. | Verified Person Component Overview, Version 1.0, IMSC |
| **Verified Person Acceptance Policy** | The set of conditions (rules, conformance criteria, etc.) that determine what is acceptable for use by a relying party. | Verified Person Component Overview, Version 1.0, IMSC |
| **Vital Event** | A significant discrete episode that occurs in the life span of a person. By law, a vital event must be recorded with a government entity and is subject to legislation and regulation.<br><br>Examples of vital events are live birth, foetal death (i.e. stillbirth), adoption, legitimation, recognition of parenthood, marriage, annulment of marriage, legal separation, divorce, and death. | PCIM Validation Standard, Verion1.9, Aug 2016, IMSC |