# Assessment Evidence: Identity Wide

| **PSP PCTF V1.3 ID** | *Qualifier(s)* | ***Conformance Criteria***  **Evidence** |
| --- | --- | --- |
| **IDWI** |  | **Identity Wide:** General requirements for identity domain atomic processes |
| **IDWI.01** | IP1 **AND** IO1 | The entity under assessment SHOULD adhere to applicable identity management controls, standards, and guidelines, and SHOULD have an auditable process to demonstrate adherence. |
| **IDWI.02** | IP2,IP3 **AND** IO2,IO3 **AND** PFID,OFID | The entity under assessment MUST adhere to applicable identity management controls, standards, and guidelines, and MUST have an auditable process to demonstrate adherence. |
| **IDWI.03** | IP2,IP3 **AND** IO2,IO3 **AND** PFID,OFID | The entity under assessment MUST provide a list of the applicable identity management controls, standards, and guidelines that are in effect. |
| **IDWI.04** | IP2,IP3 **AND** IO2,IO3 **AND** PFID,OFID | The entity under assessment MUST demonstrate the equivalency of the applicable identity management controls, standards, and guidelines to those used by the assessor. |
| **IDWI.05** | IP1,IP2,IP3 **AND** PFID | The entity under assessment MUST have in place policies and procedures to safeguard the identity information of a person. |
| **IDWI.06** | IP1,IP2,IP3 **AND** PFID | The entity under assessment MUST have in place policies and procedures to detect the misuse of the identity information of a person. |
| **IDWI.07** | IP1 | The entity under assessment SHOULD ensure that identity information validation of Agents, meets or exceeds the identity information validation requirements applicable to the IP1 (for persons) qualifier in Identity Information Validation. |
| **IDWI.08** | IP2 | The entity under assessment MUST ensure that identity information validation of Agents, meets or exceeds the identity information validation requirements applicable to the IP2 (for persons) qualifier in Identity Information Validation. |
| **IDWI.09** | IP3 | The entity under assessment MUST ensure that identity information validation of Agents, meets or exceeds the identity information validation requirements applicable to the IP3 (for persons) qualifier in Identity Information Validation. |
| **IDWI.10** | IP3 | The entity under assessment MUST ensure that identity verification of Agents, meets or exceeds the identity verification requirements applicable to the IP3 (for persons) qualifier in Identity Verification. |
| **IDWI.11** | IP1,IP2,IP3 **AND** PFID | In cases involving children, minors, and other vulnerable individuals, the entity under assessment MUST:  1. Have in place additional safeguards, compensating factors, or a documented exception process to reduce risk and to initiate interventions, as appropriate; AND 2. Confirm that the applicant (for example, a parent or guardian) has the legal authority to carry out a request or obtain a service on behalf of the child, minor, or other vulnerable individual. |
| **IDID** |  | **Identity Information Determination:** Identity Information Determination is the process of determining the identity context, the identity information requirements, and the identifier. |
| **IDID.01** | IP1,IP2,IP3 **AND** IO1,IO2,IO3 **AND** PFID,OFID | The entity under assessment MUST specify the identity context of the program or service.  The following considerations should be kept in mind when defining the identity context of a program or service:   ● Intended recipients of the program or service – recipients may be external to the program/service provider (e.g., citizens, businesses, non-profit organizations), or internal to the program/service provider (e.g., employees, departments)  ● Size, characteristics, and composition of the client population  ● Commonalities with other programs and services (i.e., across program/service providers)  ● Program/service providers with similar mandates  ● Use of shared services where the shared service delivery context may differ from the program context |
| **IDID.02** | IP1,IP2,IP3 **AND** IO1,IO2,IO3 **AND** PFID,OFID | The entity under assessment MUST define the identity information requirements of the program or service.  For any given program or service, identity information is the set of identity attributes that is both:  ● Sufficient to distinguish between different persons or organizations within the program/service population (i.e., achieve the uniqueness requirement for identity); and  ● Sufficient to describe the person or organization as required by the program or service. |
| **IDID.03** | IP1,IP2,IP3 **AND** IO1,IO2,IO3 **AND** PFID,OFID | The entity under assessment MUST define the set of identity attributes that will be used to uniquely distinguish a particular entity within the program/service population. This set of identity attributes is referred to as the identifier. |
| **IDED** |  | **Identity Evidence Determination:** Identity Evidence Determination is the process of determining the acceptable evidence of identity (whether physical or electronic). |
| **IDED.01** | IP1,IP2,IP3 **AND** IO1,IO2,IO3 | The entity under assessment MUST determine the acceptable evidence of foundational identity (whether physical or electronic) for its programs and services.  The entity under assessment MUST ensure that the evidence of foundational identity originates from an authoritative source that: 1. Is under the control of a federal, provincial, or territorial government, or the local equivalent abroad (Note: When the authoritative source is outside Canadian jurisdiction, the acceptability criteria will be determined through a risk-managed approach); and 2. Registers specific foundational events, or determines legal status.Acceptable authoritative records and credentials: 1. Vital statistics records used in the issuance of birth certificates; 2. Legal status records used in the issuance of citizenship certificates, naturalization certificates, and permanent resident cards;  3. Business registration records; and 4. Other authoritative records enabled by government legislation. |
| **IDED.02** | IP1,IP2,IP3 **AND** IO1,IO2,IO3 | The entity under assessment MUST determine the acceptable evidence of contextual identity (whether physical or electronic) for it programs and services.   The entity under assessment MUST ensure that the evidence of contextual identity originates from an authoritative source that is under the control of an organization that has been approved by the entity under assessment.  Some examples of acceptable authoritative records and credentials are:  ● Licensing and registration records used in the issuance of a health insurance card or a driver's licence;  ● Records of professional qualifications used in the issuance of professional credentials; and  ● Membership records used in the issuance of membership credentials. |
| **IDED.03** | IP1,IP2,IP3 **AND** IO1,IO2,IO3 | When assessing authoritative sources of evidence of contextual identity (whether physical or electronic), the entity under assessment MUST take the following into consideration:  1. The recognition of the authoritative source in law; 2. The ability of the authoritative source to satisfy relevant regulatory authorities; 3. The historic performance of the authoritative source; 4. The provenance of the evidence of contextual identity; and 5. The robustness of the processes employed to collect and store the evidence of contextual identity. |
| **IDED.04** | IP1,IP2,IP3 **AND** IO1,IO2,IO3 | For evidence of contextual identity, the entity under assessment MAY rely on a recognized independent accreditation of an authoritative source instead of conducting their own assessment. |
| **IDED.05** | IP1,IP2,IP3 **AND** IO1,IO2,IO3 | The entity under assessment MUST identify the acceptable information providers (including third parties such as Agents or Issuers) from which evidence of contextual or foundational identity will be accepted. |
| **IDED.06** | IP1,IP2,IP3 **AND** IO1,IO2,IO3 | The entity under assessment MUST identify the acceptable information providers (including third parties such as Agents or Issuers) permitted to present evidence of contextual or foundational identity. |
| **IDEA** |  | **Identity Evidence Acceptance:** Identity Evidence Acceptance is the process of confirming that the evidence of identity presented (whether physical or electronic) is acceptable. |
| **IDEA.01** | IP1 **AND** IO1 | The entity under assessment MUST NOT restrict what is provided as evidence of identity. |
| **IDEA.02** | IP2 **AND** IO2 | The entity under assessment MUST require that one instance of evidence of identity (either foundational or contextual) be provided. |
| **IDEA.03** | IP3 **AND** IO3 | The entity under assessment MUST require that two instances of evidence of identity (at least one of which must be evidence of foundational identity) be provided. |
| **IDEA.04** | IP2,IP3 **AND** IO2,IO3 | In cases where evidence of foundational Identity is inconsistent with the identity information provided by an entity about a Subject (e.g., due to a name change), the entity under assessment MAY require additional confirmation by the authoritative source of foundational identity, or additional evidence of contextual identity. |
| **IDEA.05** | IP3 **AND** IO3 | In cases where evidence of contextual identity is incomplete or inconsistent with the identity information provided by the evidence of foundational identity (e.g., due to a name change), the entity under assessment MAY require additional evidence of contextual identity. The entity under assessment MAY require an endorsement or certification to verify that the evidence of contextual identity is a true copy of the original. |
| **IDEA.06** | IP3 **AND** PFID | In cases involving children, minors, and other vulnerable individuals, the entity under assessment MUST require evidence of identity of the applicant (for example, a parent or guardian) in addition to evidence of identity of the child, minor, or other vulnerable individual. For example, the passport of a parent could be used as evidence of contextual identity of the child. |
| **IDIV** |  | **Identity Information Validation:** Identity Information Validation is the process of confirming the accuracy of identity information about a Subject as established by the Issuer. |
| **IDIV.01** | IP1 **AND** IO1 | The entity under assessment MAY accept assertions of identity information made by an entity about a Subject. |
| **IDIV.02** | IP1 **AND** IO1 | The entity under assessment SHOULD ensure that the evidence of identity has a defined validity period. |
| **IDIV.03** | IP2,IP3 **AND** IO2,IO3 | The entity under assessment MUST ensure that the evidence of identity has a defined validity period. |
| **IDIV.04** | IP2,IP3 **AND** IO2,IO3 | The entity under assessment MUST ensure that assertions of identity information made by an entity about a Subject acceptably match all instances of evidence of identity (foundational and/or contextual) provided by the Holder. |
| **IDIV.05** | IP2 **AND** IO2 | The entity under assessment MUST confirm the the evidence of contextual identity with the issuing authority AND MUST validate the identity information against the authoritative record AND SHOULD request the status of the Subject from the issuing authority.   If confirmation with the issuing authority or validation of the identity information is not feasible, then the entity under assessment MUST ensure that the evidence of contextual identity is confirmed by a trained examiner. |
| **IDIV.06** | IP3 **AND** IO3 | The entity under assessment MUST confirm the the evidence of foundational identity with the issuing authority AND MUST validate the identity information against the authoritative record AND MUST request the status of the Subject from the issuing authority.   If confirmation with the issuing authority or validation of the identity information is not feasible, then the entity under assessment MUST ensure that the evidence of foundational identity is confirmed by a trained examiner. |
|  |  |  |
| **IDRE** |  | **Identity Resolution:** Identity Resolution is the process of establishing the uniqueness of a Subject within a program/service population through the use of identity information. |
| **IDRE.01** | IP1,IP2,IP3 **AND** IO1,IO2,IO3 **AND** PFID,OFID | The entity under assessment MUST ensure that the identity information provided uniquely resolves to only one entity within its program/service population. |
| **IDES** |  | **Identity Establishment:** Identity Establishment is the process of creating a record of identity of a Subject within a program/service population that may be relied on by others for subsequent programs, services, and activities. |
| **IDES.01** | IP1 **AND** IO1 | The entity under assessment SHOULD be a registered public sector or private sector entity (e.g., a government department, agency, or ministry, a proprietorship, corporation, association, etc.). |
| **IDES.02** | IP2 **AND** IO2 | The entity under assessment MUST be a registered public sector or private sector entity (e.g., a government department, agency, or ministry, a proprietorship, corporation, association, etc.). |
| **IDES.03** | IP3 **AND** IO3 | The entity under assessment MUST be a government department, agency, ministry, or other public sector entity operating under the authority of a Canadian federal, provincial, or territorial government, or a government-regulated private sector entity. |
| **IDES.04** | PFID,OFID | The entity under assessment MUST be a provincial or territorial vital statistics registrar, IRCC, a provincial or territorial business registrar, or Corporations Canada. |
| **IDES.05** | IP1,IP2,IP3 **AND** IO1,IO2,IO3 | The entity under assessment MUST ensure that the creation of a record of contextual identity is confirmed by and referenceable to a relevant event or activity. |
| **IDES.06** | PFID | The entity under assessment MUST ensure that the creation of a record of foundational identity of a person is confirmed by and referenceable to one of the following events:  ● Birth in Canada  ● Acquired Status   o Canadian birth abroad (outside of Canada)  o Confirmation of status of parent(s)  ● Grant of Status   o Citizenship  o Permanent residency  o Temporary residency (including protected persons)  The entity under assessment MUST ensure that an inspection of all the relevant documents and evidence is conducted by a trained examiner using a risk-based approach. |
| **IDES.07** | OFID | The entity under assessment MUST ensure that the creation of a record of foundational identity of an organization is confirmed by and referenceable to one of the following events:  ● Incorporation  ● Amalgamation (of one or more incorporated entities)  The entity under assessment MUST ensure that an inspection of all the relevant documents and evidence is conducted by a trained examiner using a risk-based approach. |
| **IDES.08** | IP1,IP2,IP3 | The entity under assessment MUST ensure that the record of contextual identity of a person contains the following minimum identity information:  ● PERSON NAME indicating the name by which a person is known or referred to  ● The initiating party for the establishment of the identity record  ● Any other Identity information requirements that are specified in applicable regulations |
| **IDES.09** | IO1,IO2,IO3 | The entity under assessment MUST ensure that the record of contextual identity of an organization contains the following minimum identity information:  ● LEGAL NAME indicating the name by which an organization is legally recognized or referred to  ● JURISDICTION OF INCORPORATION indicating the jurisdiction in which the organization is incorporated  ● The initiating party for the establishment of the identity record  ● Any other Identity information requirements that are specified in applicable regulations |
| **IDES.10** | PFID | The entity under assessment MUST ensure that the record of foundational identity of a person contains the following minimum identity information:   For Birth in Canada:   ● ASSIGNED IDENTIFIER that uniquely distinguishes a person from all other persons within a population  ● PERSON NAME indicating the name by which a person is registered  ● EVENT TYPE (indicatig birth or stillbirth)  ● EVENT DATE  o Event Year, Event Month, Event Day  ● PLACE OF EVENT  o At least one of: Municipality Name, Province/Territory Code, Province/Territory Name  ● ASSOCIATED PERSON  o At least one other person who has an affiliation with or a legal authority to act on behalf of a person (e.g., spouse, parent, guardian, power of attorney, etc.)  ● The initiating party for the establishment of the identity record  ● Any other Identity information requirements that are specified in applicable regulations  For Acquired Status:   ● ASSIGNED IDENTIFIER that uniquely distinguishes a person from all other persons within a population   ● PERSON NAME indicating the name by which a person is registered  ● EVENT TYPE (indicating birth)  ● EVENT DATE (whether available in whole or in part)  o Event Year, Event Month, Event Day (if available)  ● PLACE OF EVENT  o At least one of: Country Code, Country Name  ● PARENT(S) STATUS at time of the person’s birth abroad  ● The initiating party for the establishment of the identity record  ● Any other Identity information requirements that are specified in applicable regulations  For Grant of Status:  ● ASSIGNED IDENTIFIER that uniquely distinguishes a person from all other persons within a population  ● PERSON NAME indicating the name by which a person is registered  ● EVENT TYPE (indicating birth)  ● EVENT DATE (whether available in whole or in part)  o Event Year, Event Month, Event Day (if available)  ● PLACE OF EVENT  o At least one of: Country Code, Country Name  ● The initiating party for the establishment of the identity record  ● Any other Identity information requirements that are specified in applicable regulations |
| **IDES.11** | OFID | The entity under assessment MUST ensure that the record of foundational identity of an organization contains the following minimum identity information:   ● ASSIGNED IDENTIFIER that uniquely distinguishes an organization from all other organizations within a population  ● LEGAL NAME indicating the name by which an organization is legally recognized or referred to  ● JURISDICTION OF INCORPORATION indicating the jurisdiction in which the organization is incorporated   ● EVENT TYPE  ● EVENT DATE (whether available in whole or in part)  o Event Year, Event Month, Event Day (if available)  ● PLACE OF EVENT  o At least one of: Municipality Name, Province/Territory Code, Province/Territory Name  ● ORGANIZATION TYPE (e.g., Association, Corporation, Trust, Sole Proprietorships, Partnerships, Co-Operatives, Credit Unions, Other, etc.)  ● The initiating party for the establishment of the identity record  ● Any other Identity information requirements that are specified in applicable regulations |
| **IDVE** |  | **Identity Verification:** Identity Verification is the process of confirming that the identity information is under the control of the Subject. |
| **IDVE.01** | IP1 | There is no requirement that the entity under assessment confirm that the identity information of a person is under the control of the Subject. |
| **IDVE.02** | IP2 | The entity under assessment SHOULD use appropriate methods to confirm that the identity information of a person is under the control of the Subject. |
| **IDVE.03** | IP3 | The entity under assessment MUST use at least one of the following methods to confirm that the identity information of a person is under the control of the Subject:   ● Knowledge-based confirmation  ● Biological or behavioural characteristic confirmation  ● Physical possession confirmation  ● Trusted referee confirmation  If the above methods are not feasible then the entity under assessment MUST define and document alternative methods in an exception process. These alternative methods MAY include:  ● Additional safeguards  ● Compensating factors |
| **IDCO** |  | **Identity Continuity:** Identity Continuity is the process of dynamically confirming that the Subject has a continuous existence over time (i.e., “genuine presence”). This process can be used to ensure that there is no malicious or fraudulent activity (past or present) and to address identity spoofing concerns. |
| **IDCO.01** |  | Currently, no conformance criteria exist for Identity Continuity due to the uncertain status of this process.  If it is decided to proceed with the creation of conformance criteria the following points should be considered:  ● Main players in this may include credit bureaus and financial institutions.  ● Transaction Monitoring: Enable capture of additional information such as geolocation, IP address, or identity of digital device used.  ● Organizations can define a non-refutable source and/or could participate in a common shared registry (of company names and data). For a person, this might be more difficult. |
| **IDMA** |  | **Identity Maintenance:** Identity Maintenance is the process of ensuring that a Subject’s identity information is accurate, complete, and up-to-date. |
| **IDMA.01** | IP1,IP2,IP3 **AND** IO1,IO2,IO3 **AND** PFID,OFID | The entity under assessment MUST ensure that records of identity are updated in a timely manner. |
| **IDMA.02** | IP1 | The entity under assessment SHOULD confirm with the foundational identity authority any changes to identity information of a person for the following events:  ● Name change   ● Gender change  ● Death |
| **IDMA.03** | IO1 | The entity under assessment SHOULD confirm with the foundational identity authority any changes to identity information of an organization for the following events:  ● Legal Name change   ● Registered Office Address change  ● Board of Directors Composition change  ● Changes to provisions in the corporation articles  ● Dissolution or insolvency |
| **IDMA.04** | IP2, IP3 | The entity under assessment MUST confirm with the foundational identity authority any changes to identity information of a person for the following events:  ● Name change   ● Gender change  ● Death |
| **IDMA.05** | IO2, IO3 | The entity under assessment MUST confirm with the foundational identity authority any changes to identity information of an organization for the following events:  ● Legal Name change   ● Registered Office Address change  ● Board of Directors Composition change  ● Changes to provisions in the corporation articles  ● Dissolution or insolvency |
| **IDMA.06** | IP1 **AND** IO1 | The entity under assessment SHOULD ensure that the identity information is automatically updated from the authoritative record of identity at pre-established intervals. |
| **IDMA.07** | IP2,IP3 **AND** IO2,IO3 | The entity under assessment MUST ensure that the identity information is automatically updated from the authoritative record of identity at pre-established intervals. |
| **IDMA.08** | IP1,IP2,IP3 **AND** IO1,IO2,IO3 **AND** PFID,OFID | The entity under assessment MUST ensure that they undertake a reassessment of the updated identity information and, where warranted, they MUST ensure that appropriate administrative action is subsequently taken. |
| **IDMA.09** | IP1,IP2,IP3 **AND** IO1,IO2,IO3 **AND** PFID,OFID | The entity under assessment MUST record the initiating party for an identity record modification and the date of modification of an identity record. |
| **IDLI** |  | **Identity Linking:** Identity Linking is the process of mapping two or more identifiers to the same Subject. |
| **IDLI.01** | IP1 | The entity under assessment SHOULD perform identity verification to ensure that the assigned identitfiers are referencing the same entity prior to linking. Identity verification MUST meet or exceed the identity verification requirements applicable to the IP1 (for persons) qualifier in Identity Verification. |
| **IDLI.02** | IP2 | The entity under assessment MUST perform identity verification to ensure that the assigned identitfiers are referencing the same entity prior to linking. Identity verification MUST meet or exceed the identity verification requirements applicable to the IP2 (for persons) qualifier in Identity Verification. |
| **IDLI.03** | IP3 | The entity under assessment MUST perform identity verification to ensure that the assigned identitfiers are referencing the same entity prior to linking. Identity verification MUST meet or exceed the identity verification requirements applicable to the IP3 (for persons) qualifier in Identity Verification. |
| **IDLI.04** | IP3 | The entity under assessment MUST use confirmation methods that are independent of each other (the use of one method cannot compromise the use of another). |