The IMSC Pan-Canadian Trust Framework (PCTF)
Public Sector Profile
Version 1.0

Consultation Deck v0.5
(for Discussion Purposes Only)

(This contents of this document have not yet been endorsed by either the IMSC or DIACC)

2019-05-30

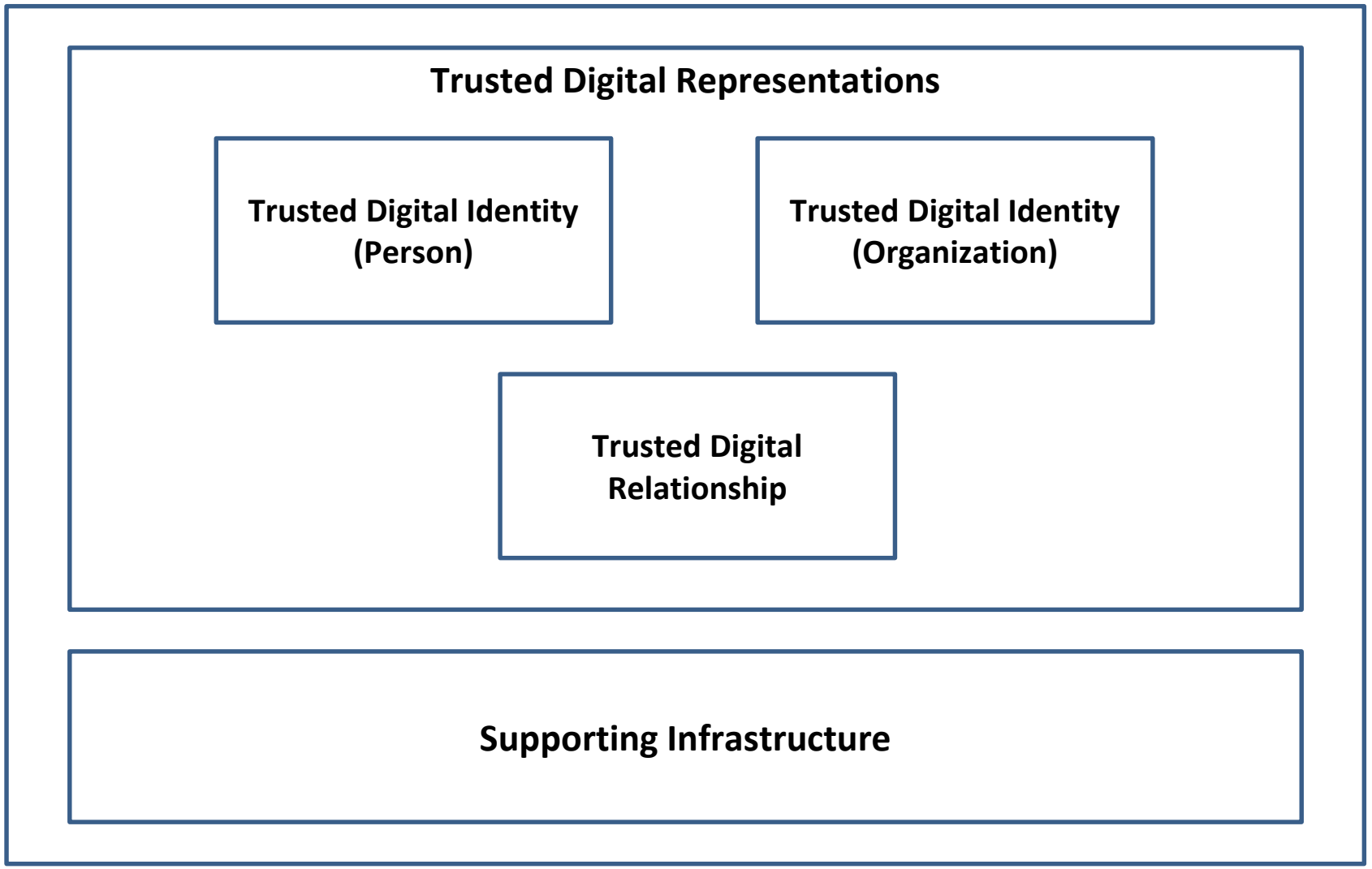
Characteristics of the PCTF

1. **A simple and integrative framework** that is easy to understand yet capable of being applied in a complex environment
2. **Technology-agnostic**: provides flexibility and logical precision in assessing the trustworthiness of digital identity solutions and digital identity providers
3. **Complements existing frameworks** (security, privacy, service delivery, etc.)
4. **Provides clear links to applicable policy, regulation, and legislation** by defining conformance criteria that can be easily mapped
5. **Normalizes (standardizes) key processes and capabilities** to enable cross-sector collaboration and digital identity ecosystem development

Trusted Digital Representations and Trusted Processes

- Currently, the PCTF recognizes:
  - 2 types of trusted digital representations
  - 24 *atomic* processes
- Atomic processes can be grouped together to form various *compound* processes such as:
  - Identity Assurance
  - Credential Assurance
  - Informed Consent
- The PCTF is extensible and interoperable:
  - additional atomic processes can be added as required
  - the atomic processes can be mapped to various conformance criteria qualifiers

Pan-Canadian Trust Framework Model



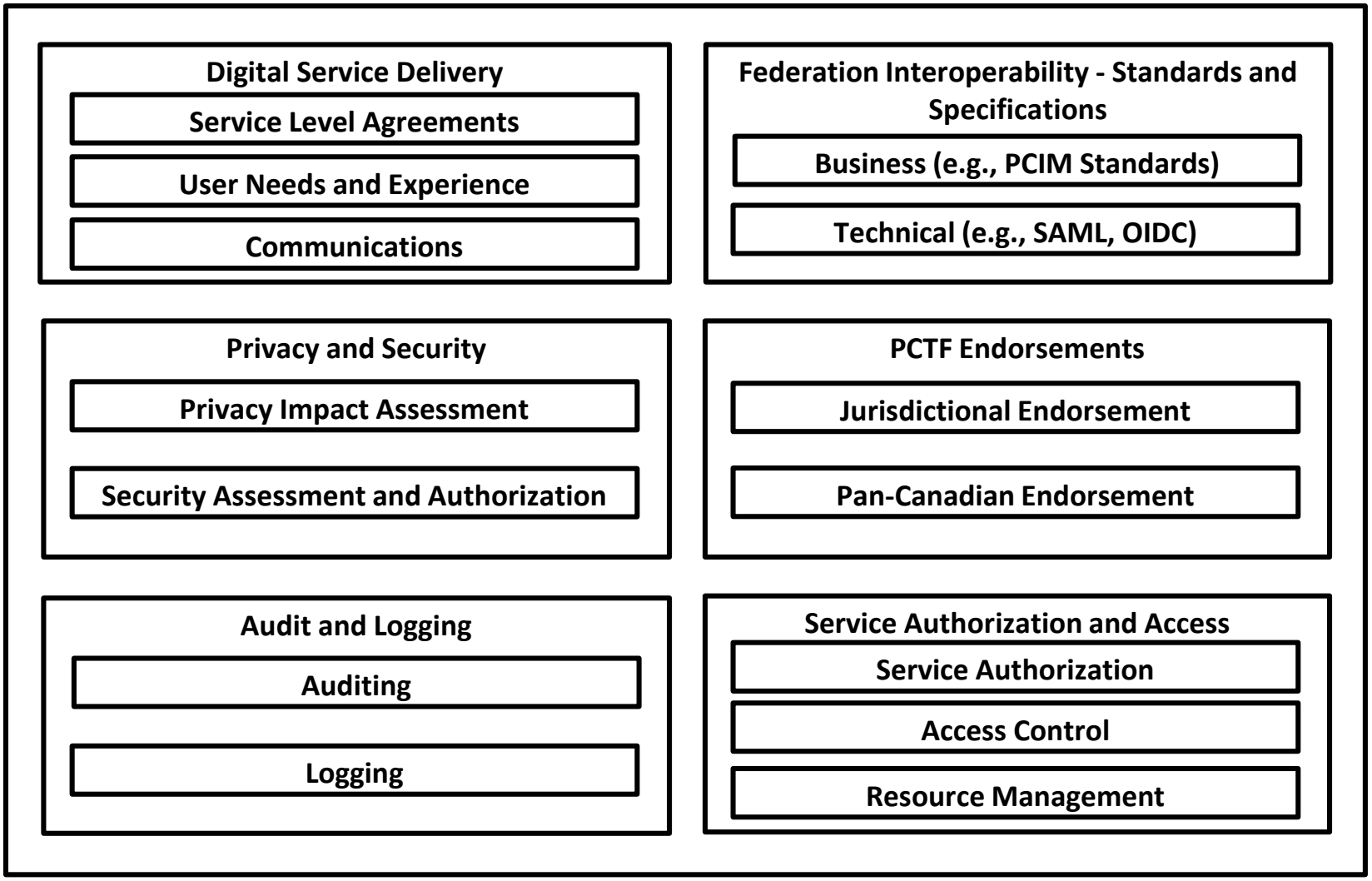
Trusted Digital Representations

Trusted Digital Identity (Person)

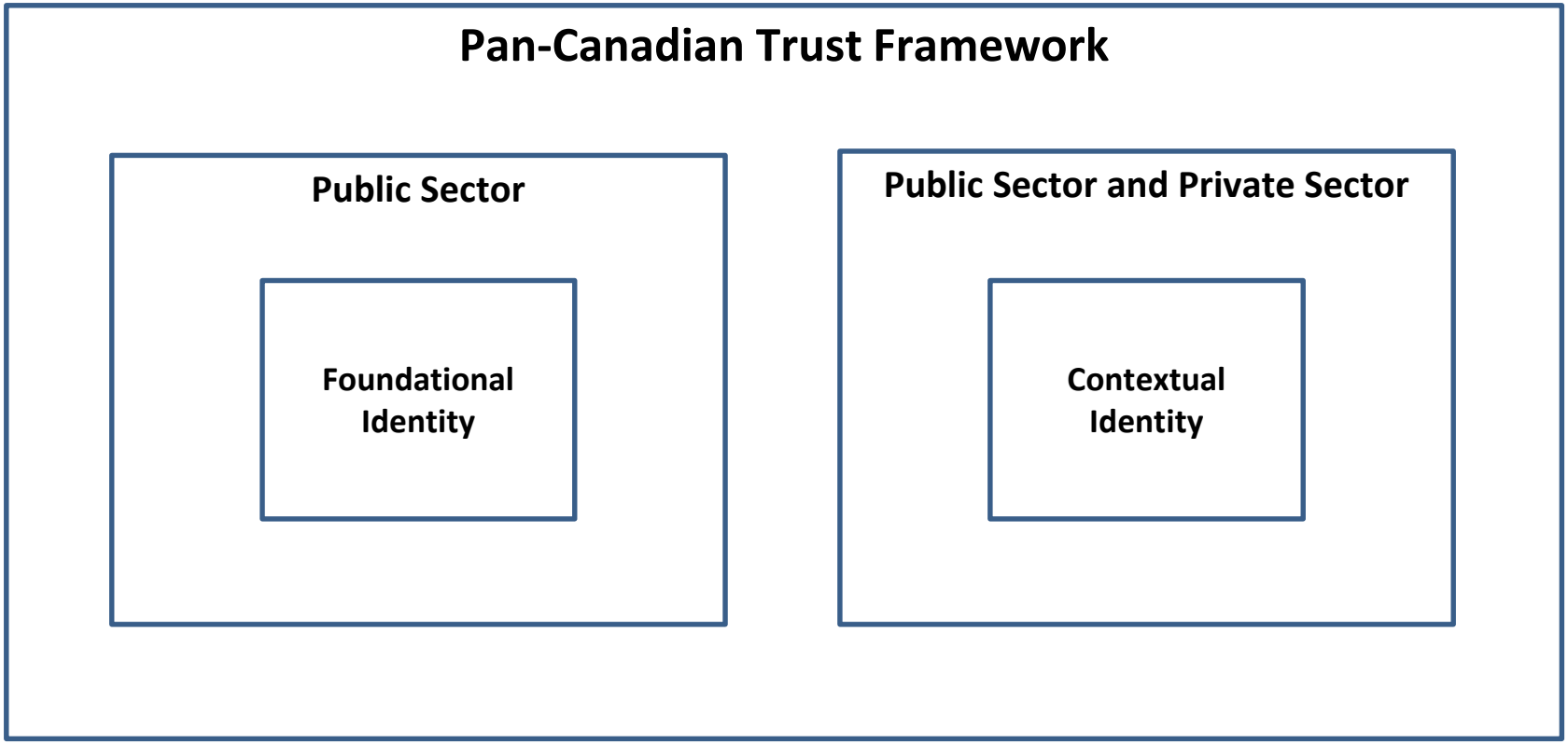
Trusted Digital Identity (Organization)

Trusted Digital Relationship

Supporting Infrastructure

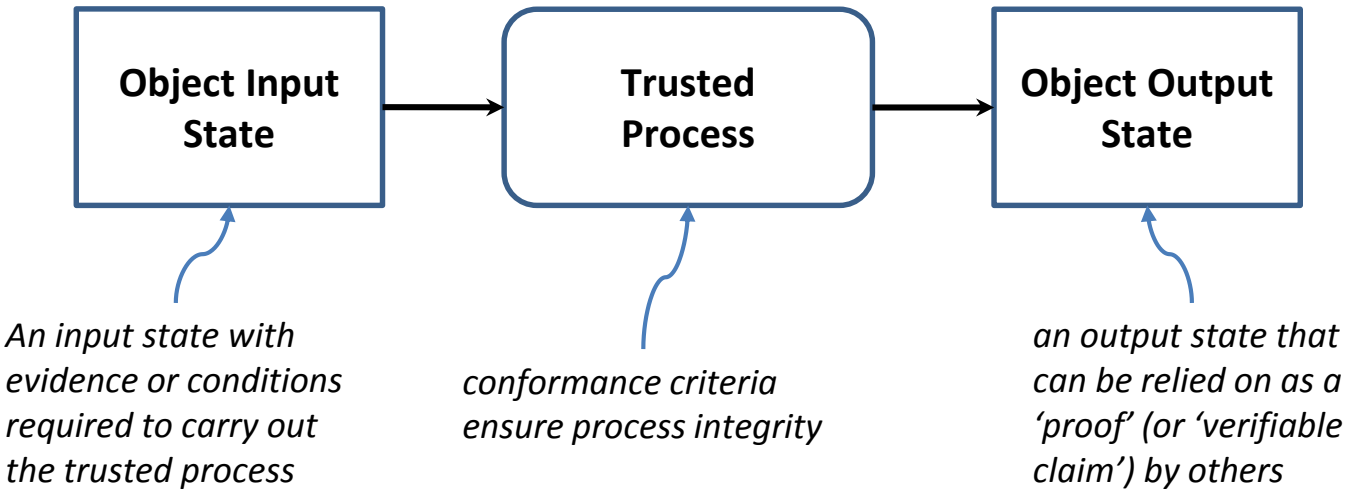


Identity Domains



Trusted Process Model

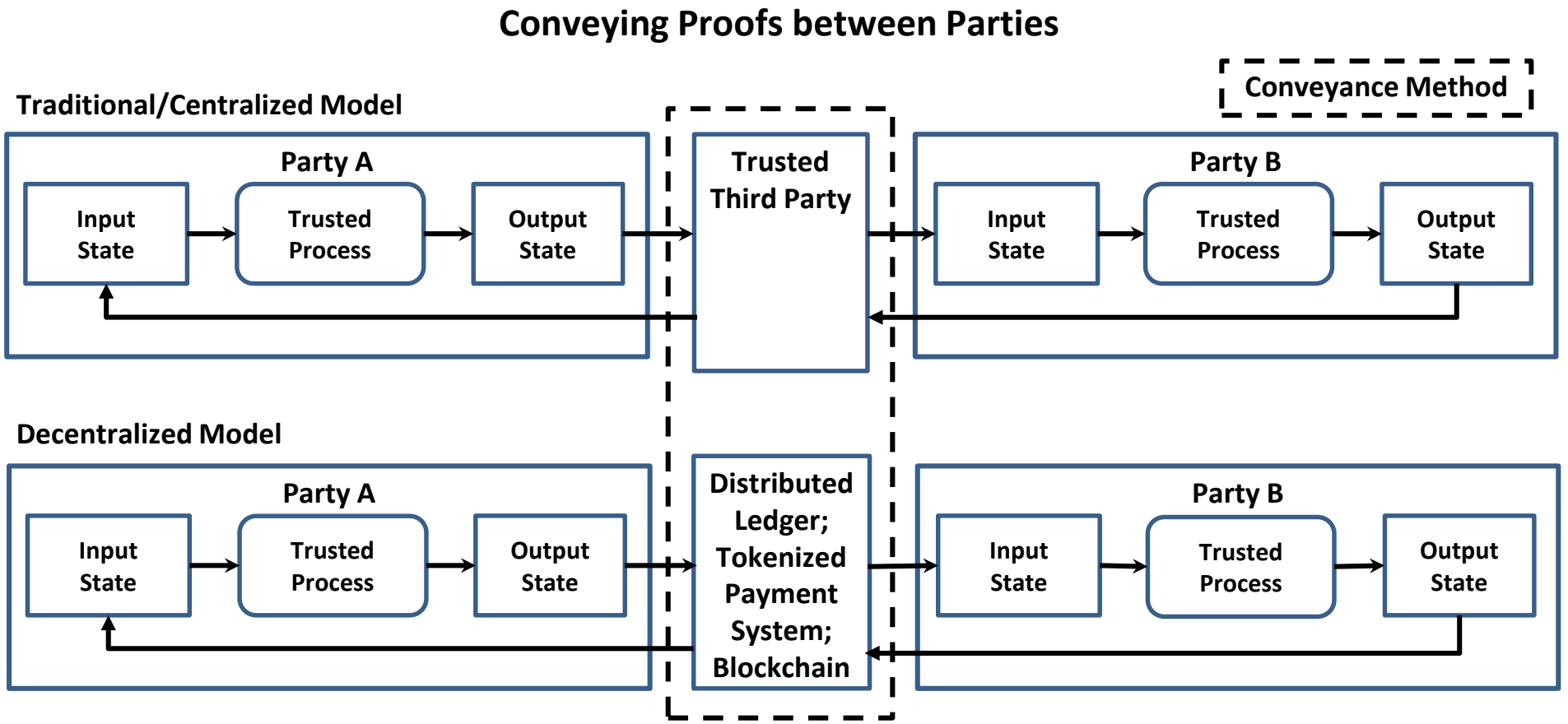
A trusted process is a set of activities that results in the state transition of an object. The object's output state can be relied on as a 'proof' by other processes.



*Formalizing (and standardizing) the **trusted processes**, the **input states**, the **output states**, and the **conformance criteria**, is the essence of defining the trust framework.*

Trusted Process Proofs and Conveyance

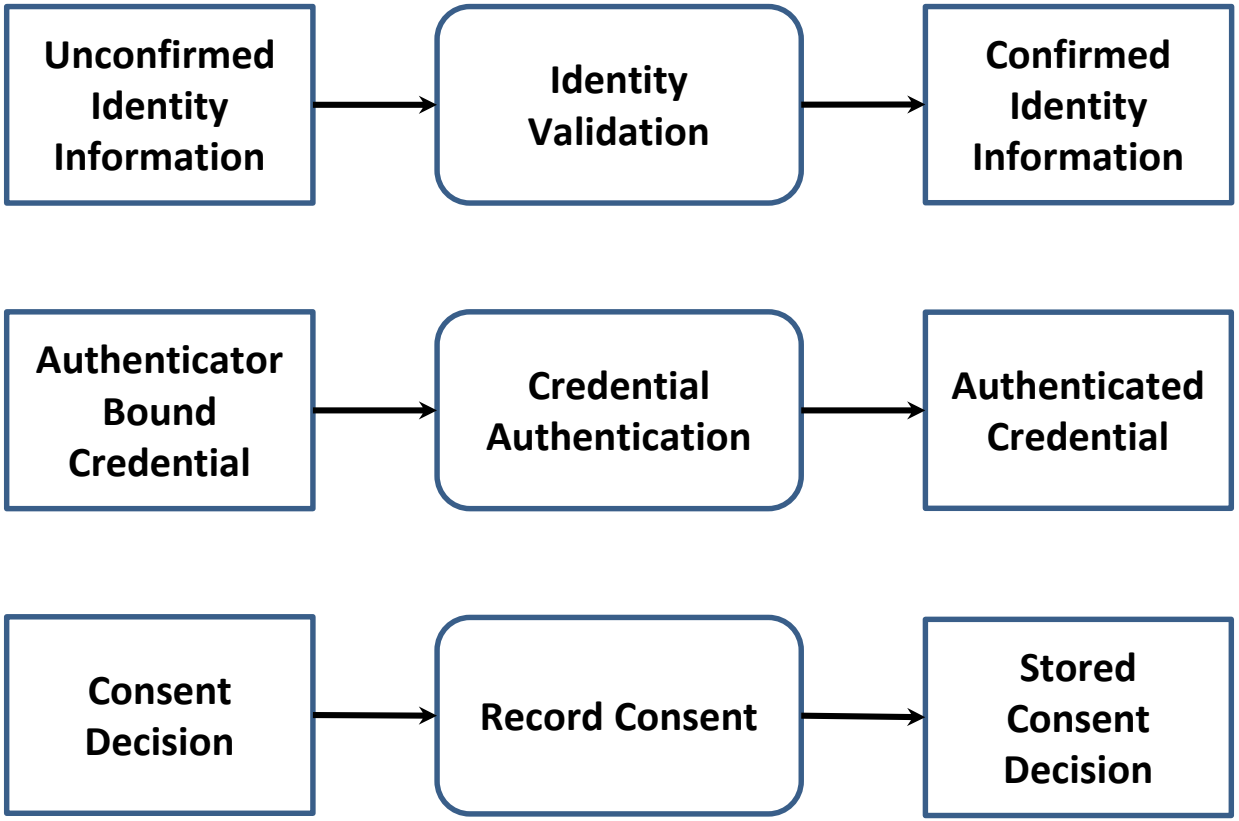
*Trusted process inputs and outputs (i.e., proofs) are **independent** of the conveyance model.*



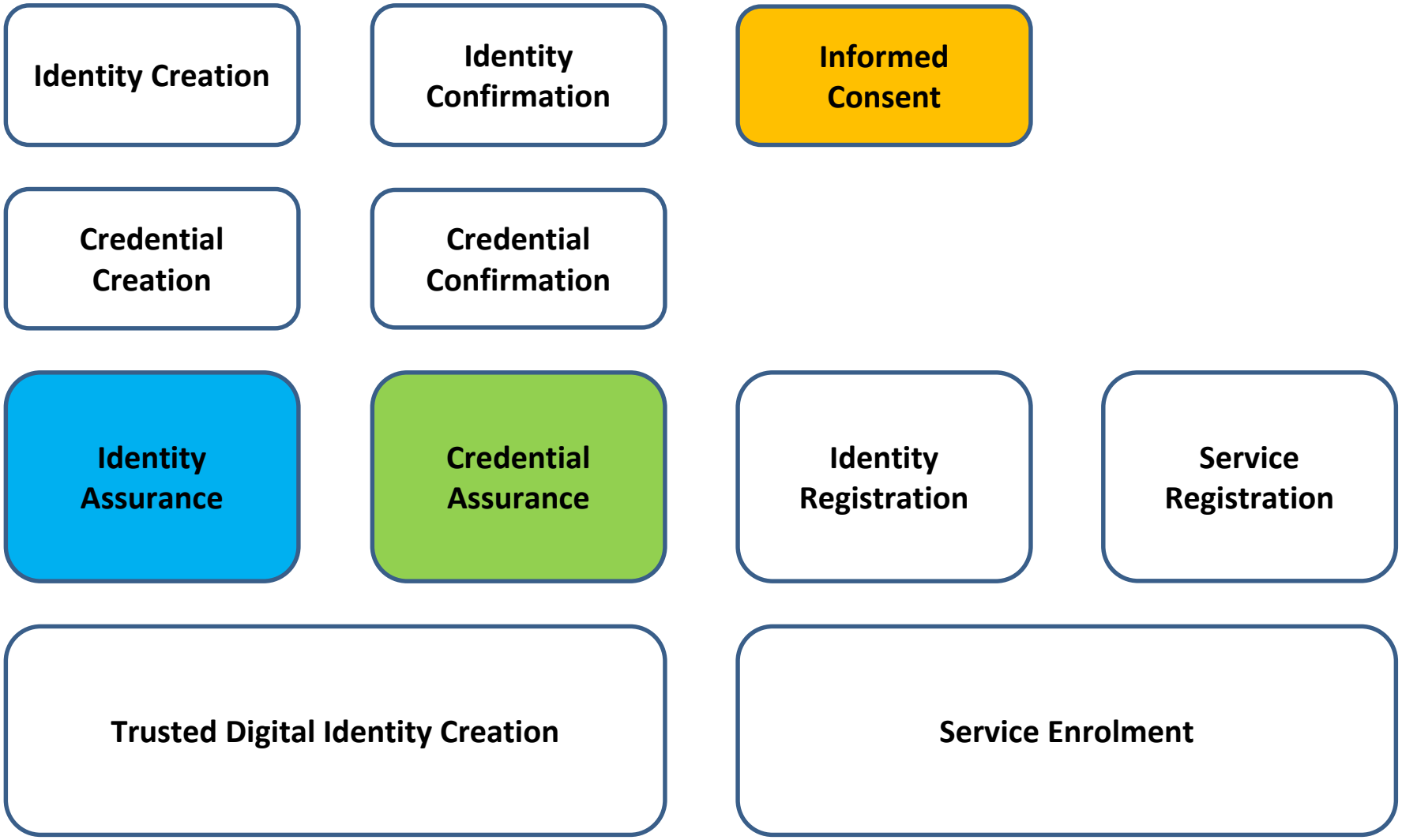
Atomic Processes

Identity Resolution	Identity Maintenance	Credential Recovery	Request Consent
Identity Establishment	Identity-Credential Binding	Credential Revocation	Record Consent
Identity Validation	Identity Linking	Credential Authentication	Review Consent
Identity Verification	Credential Issuance	Create Signature	Renew Consent
Evidence Validation	Credential-Authenticator Binding	Check Signature	Expire Consent
Identity Presentation	Credential Suspension	Formulate Notice	Revoke Consent

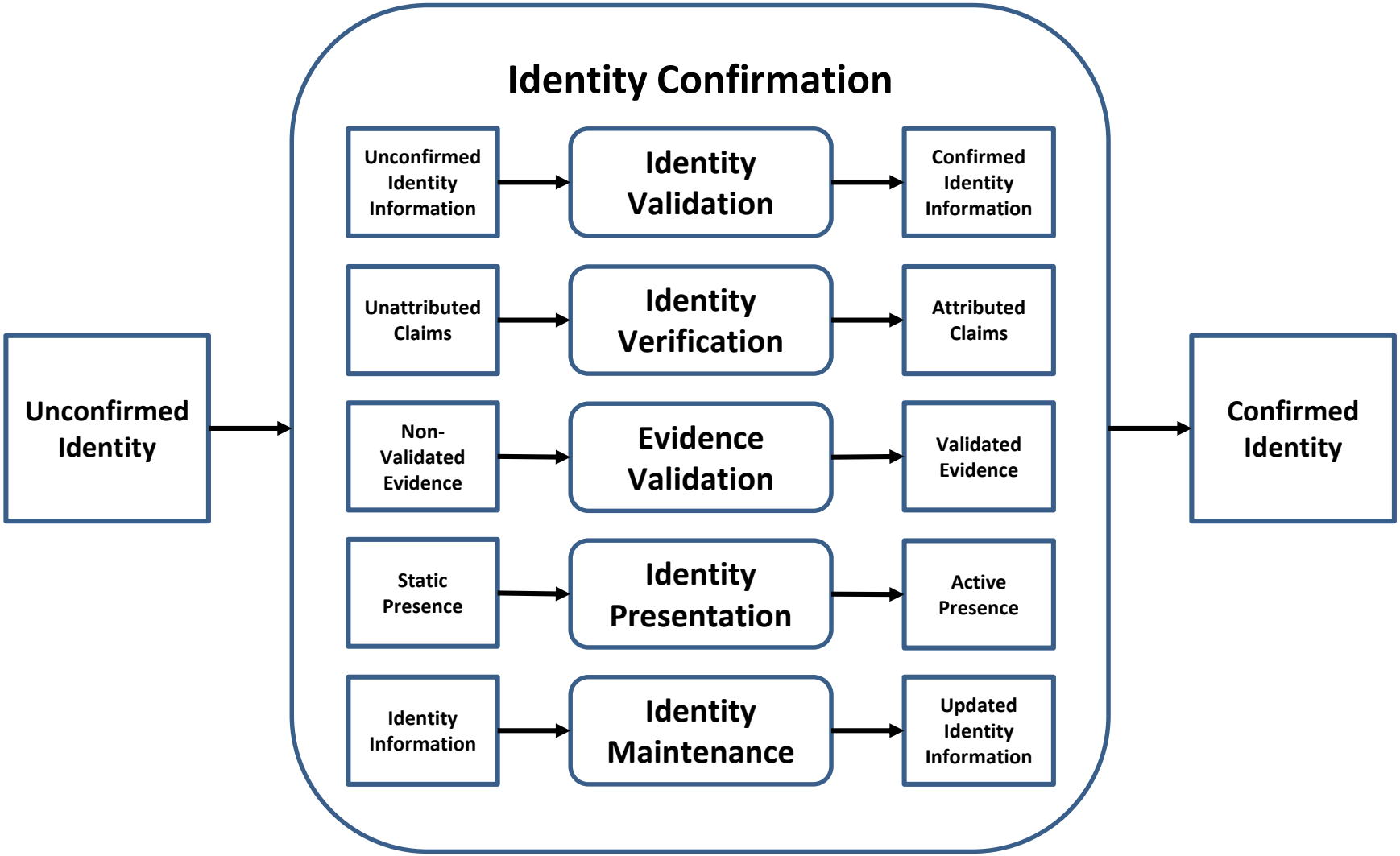
Examples of Atomic Processes (Modeled)



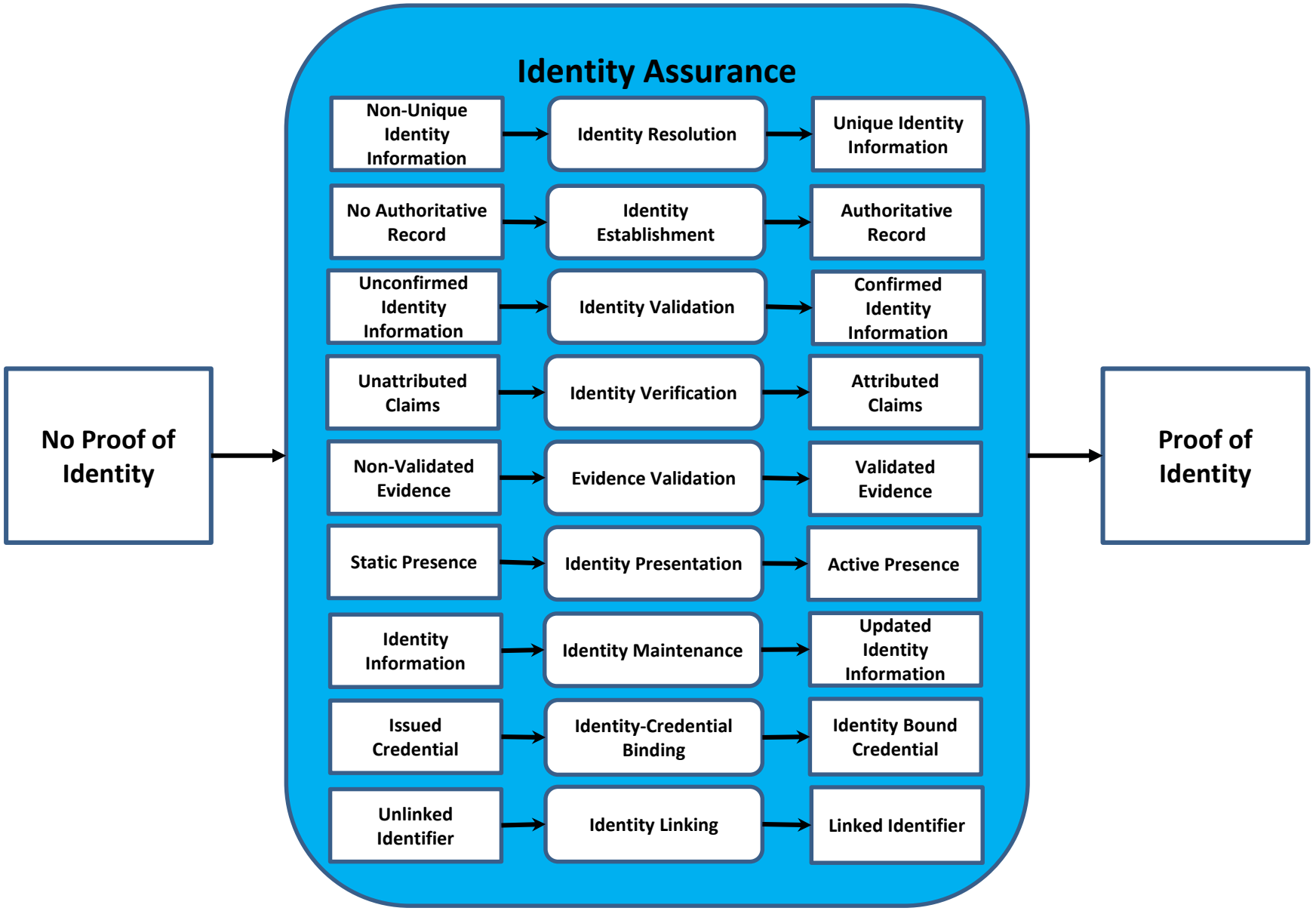
Compound Processes



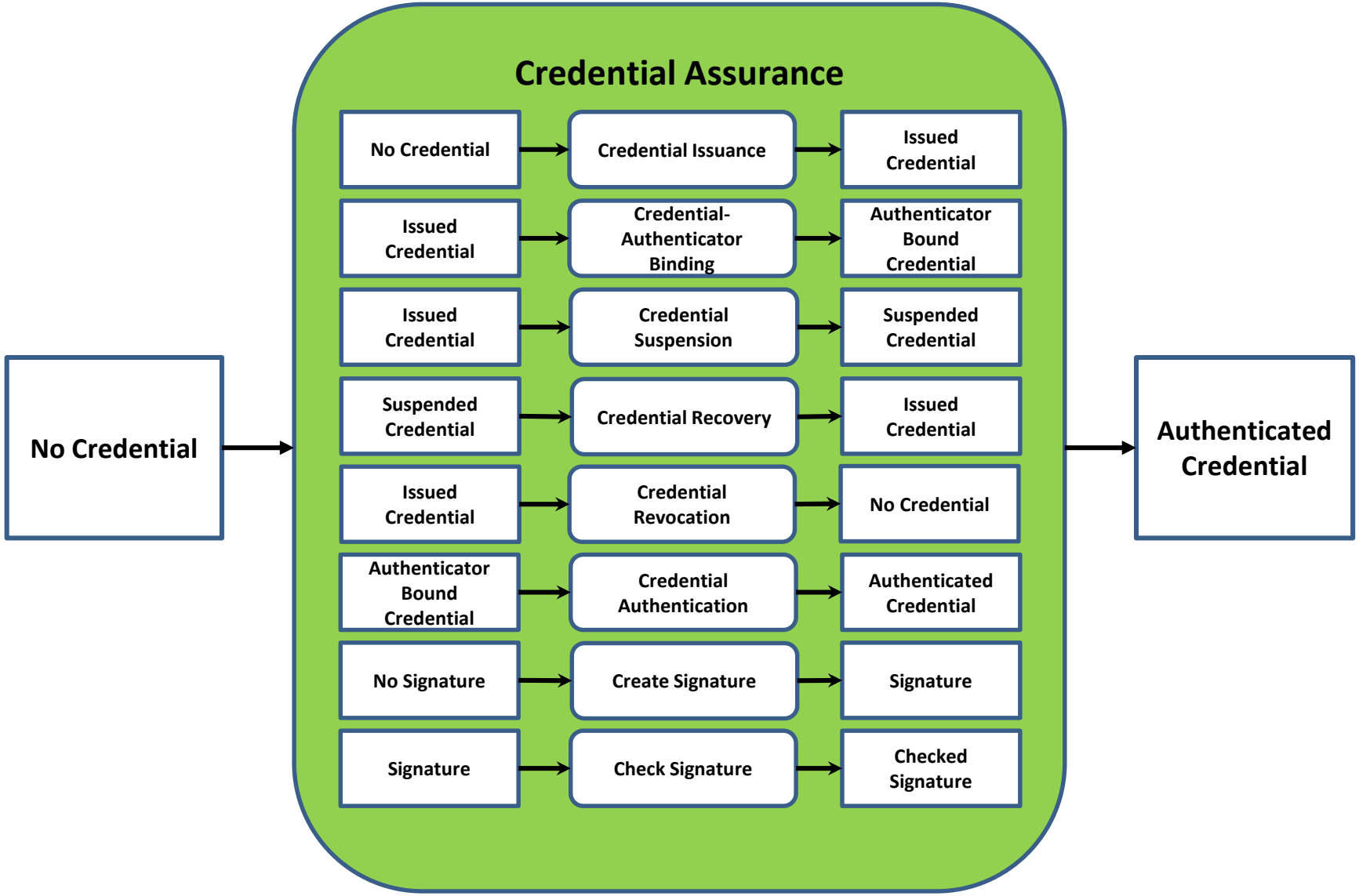
Compound Process: *Identity Confirmation* (Modeled)



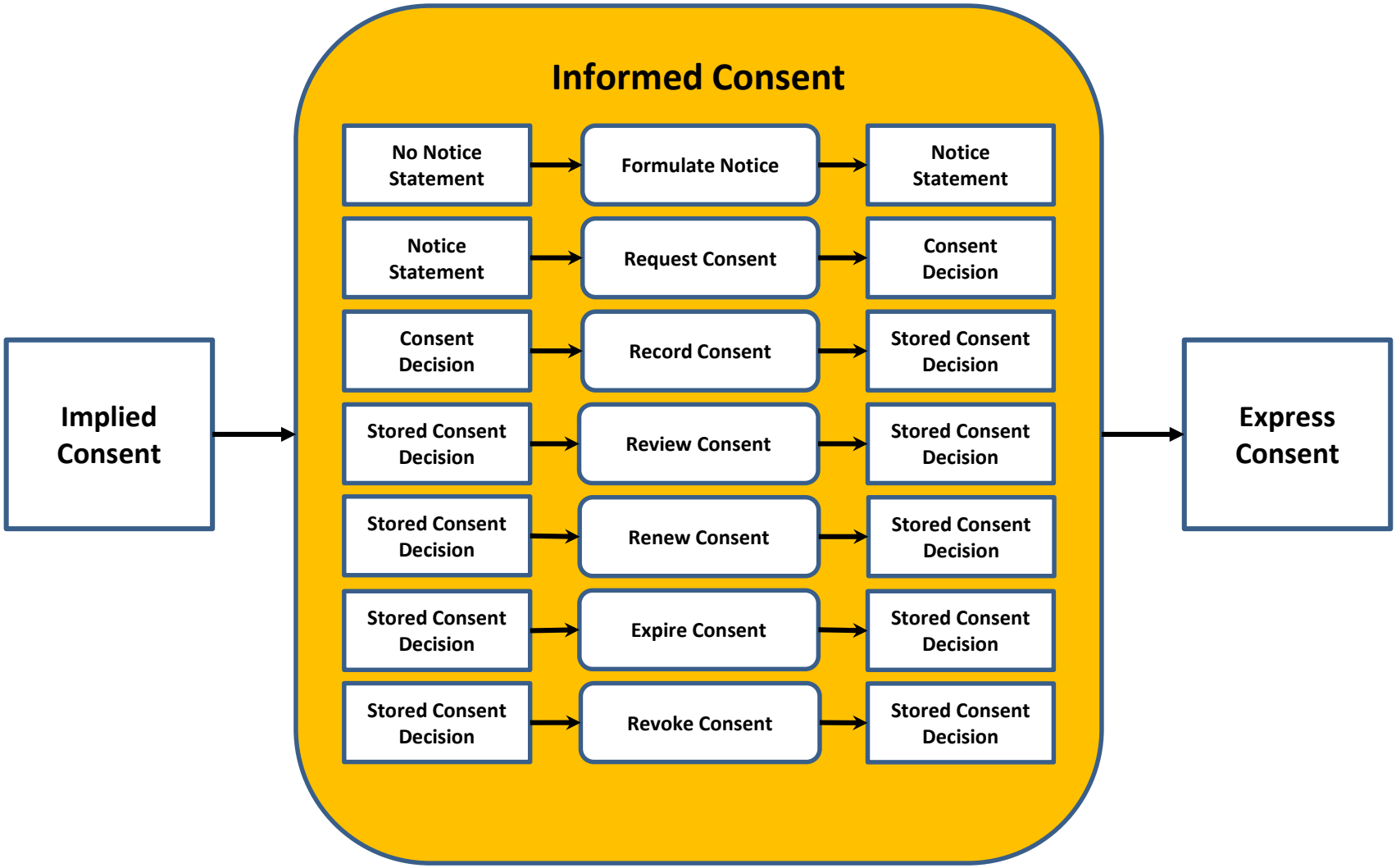
Compound Process: *Identity Assurance*



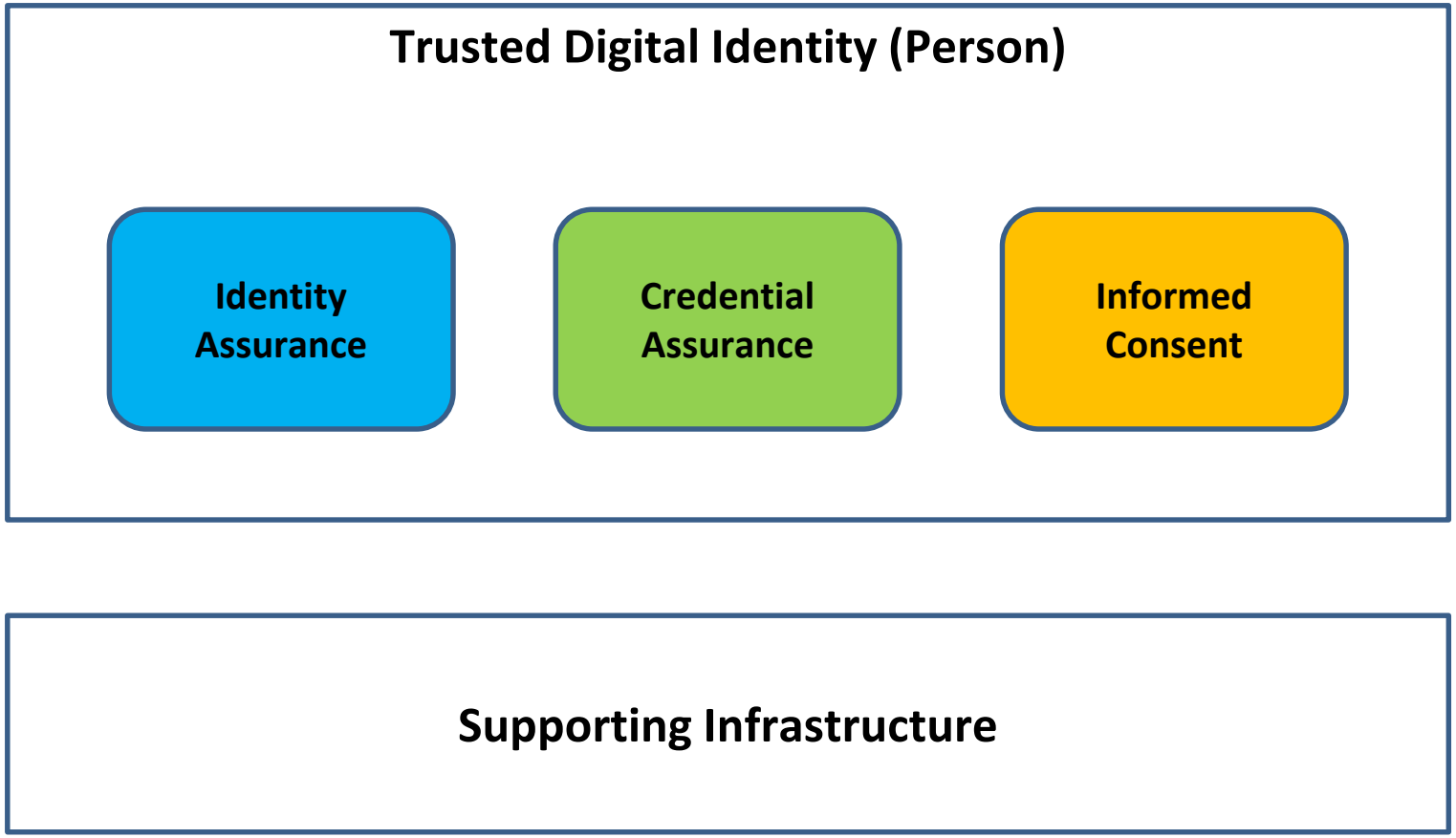
Compound Process: *Credential Assurance*



Compound Process: *Informed Consent*

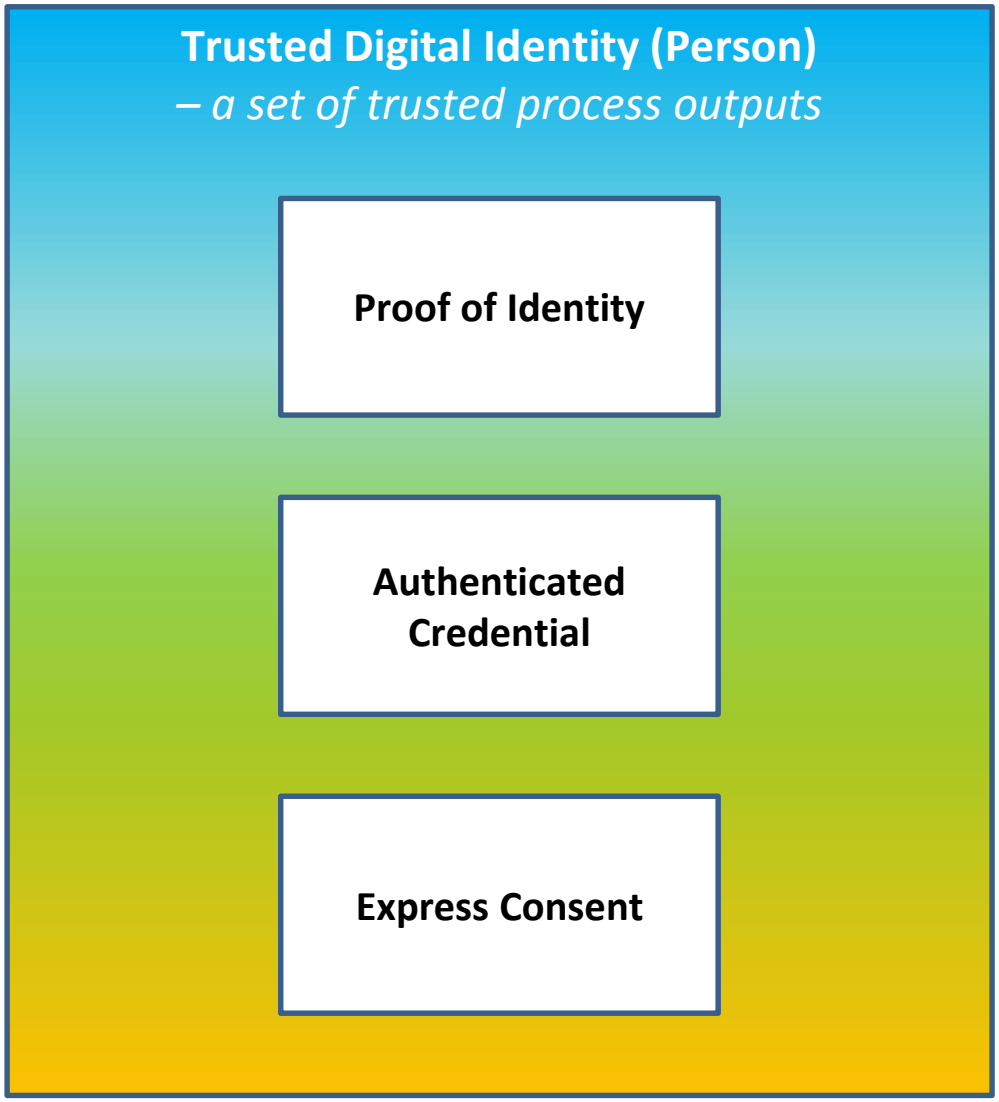


Compound Process: *Trusted Digital Identity (Person) Creation*

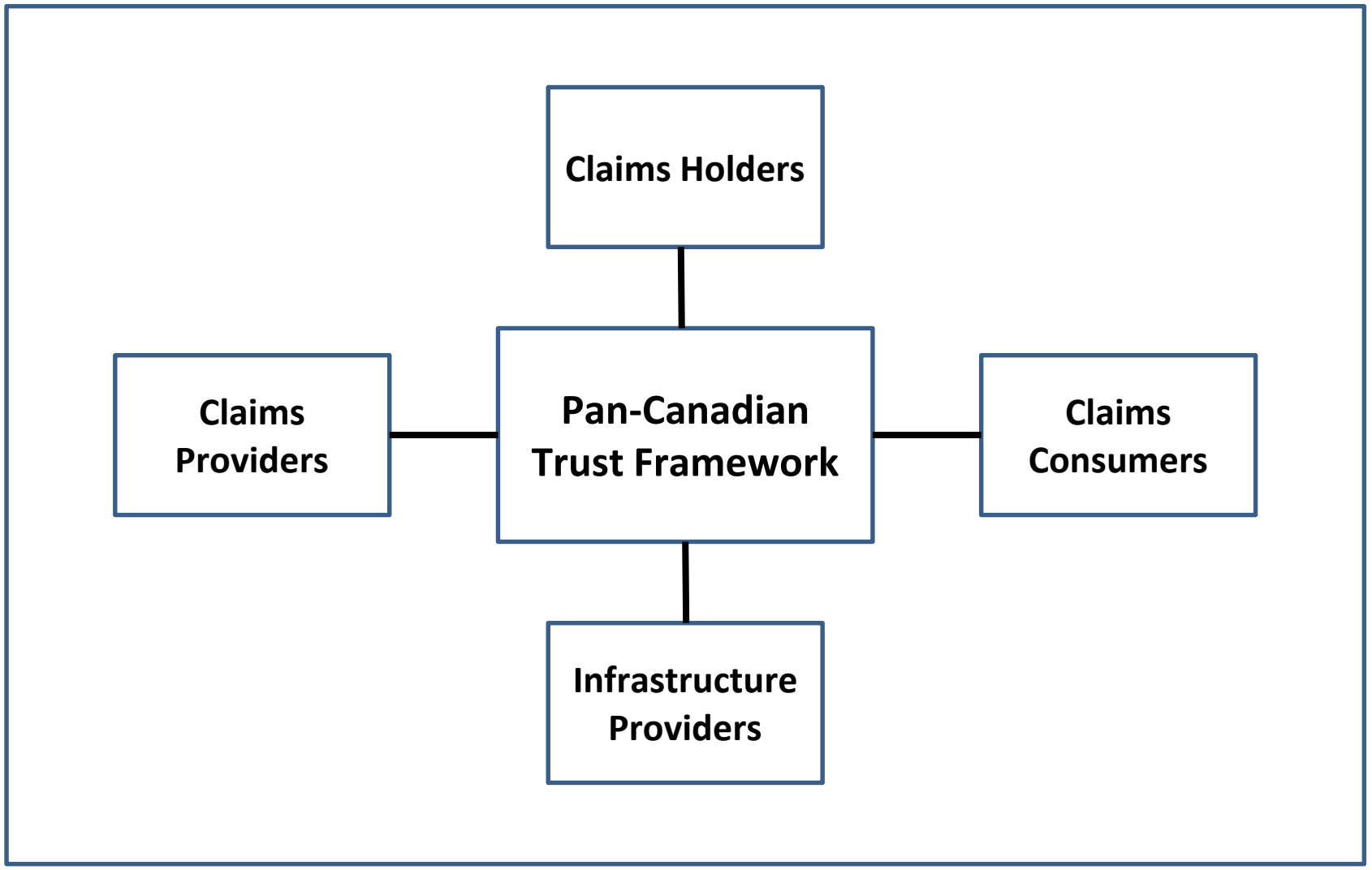


*A **trusted digital Identity** can be conceptualized as a set of trusted process outputs (proofs) that are independent of the conveyance method.*

Depending on the digital ecosystem, some of these trusted processes may be carried out by different parties at different points in time.



Canadian Digital Ecosystem Stakeholders



Participant Roles

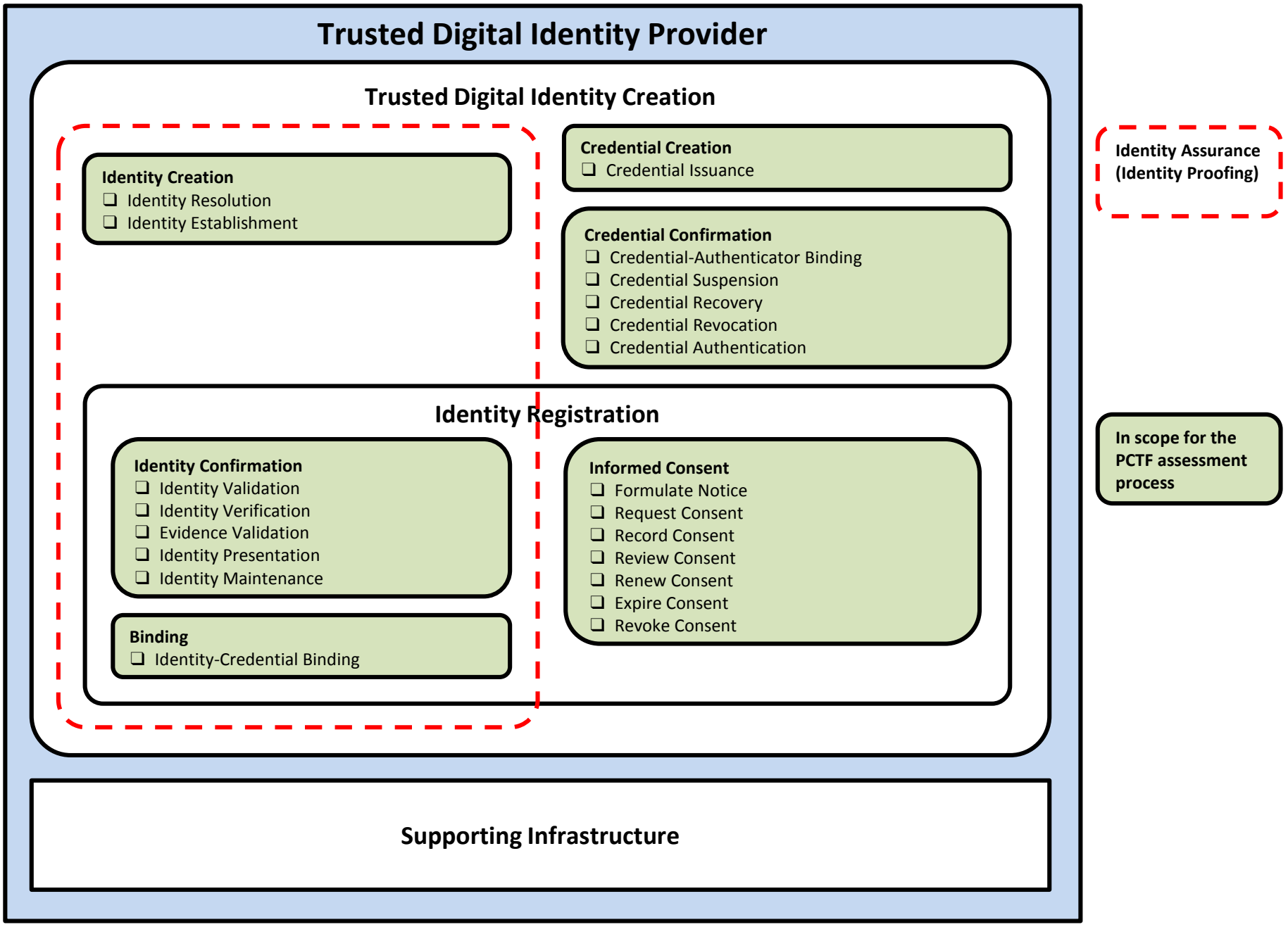
- Identity Assurance Providers
- Credential Assurance Providers
- Trusted Digital Identity (TDI) Providers
- Relying Parties (as TDI Consumers)
- Digital Identity Owners

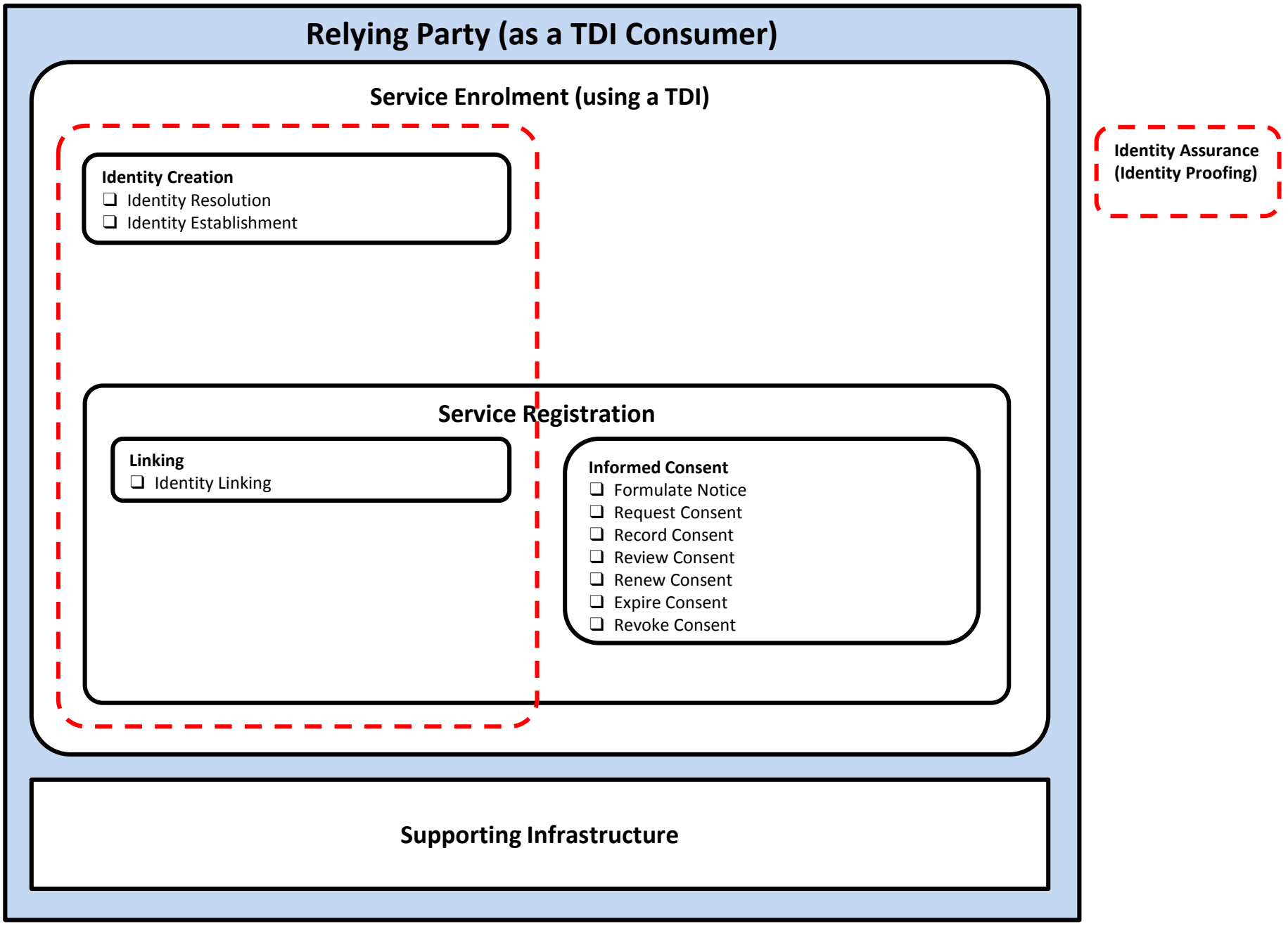
Atomic Processes by Participant Roles

No.	Atomic Process	Identity Assurance Provider	Credential Assurance Provider	Trusted Digital Identity (TDI) Provider	Relying Party (as a TDI Consumer)
1	Identity Resolution	X		X	X
2	Identity Establishment	X		X	X
3	Identity Validation	X		X	
4	Identity Verification	X		X	
5	Evidence Validation	X		X	
6	Identity Presentation	X		X	
7	Identity Maintenance	X		X	
8	Identity-Credential Binding			X	
9	Identity Linking				X
10	Credential Issuance		X	X	
11	Credential-Authenticator Binding		X	X	
12	Credential Suspension		X	X	
13	Credential Recovery		X	X	
14	Credential Revocation		X	X	
15	Credential Authentication		X	X	
16	Create Signature			X	X
17	Check Signature			X	X
18	Formulate Notice			X	X
19	Request Consent			X	X
20	Record Consent			X	X
21	Review Consent			X	X
22	Renew Consent			X	X
23	Expire Consent			X	X
24	Revoke Consent			X	X

Atomic Processes can be carried out by multiple parties
(e.g., a Provincial/Territorial Trusted Digital Identity being consumed by a Federal service)

No.	Atomic Process	Pan-CDN LOA	Trusted Digital Identity (TDI) Provider	Relying Party (as a TDI Consumer)
1	Identity Resolution	…	Province/Territory	Federal service
2	Identity Establishment	3	Province/Territory	Federal service
3	Identity Validation	3	Province/Territory	
4	Identity Verification	3	Province/Territory	
5	Evidence Validation	3	Province/Territory	
6	Identity Presentation	…	Province/Territory	
7	Identity Maintenance	3	Province/Territory	
8	Identity-Credential Binding	…	Province/Territory	
9	Identity Linking	…		Federal service
10	Credential Issuance	2	Province/Territory	
11	Credential-Authenticator Binding	2	Province/Territory	
12	Credential Suspension	2	Province/Territory	
13	Credential Recovery	2	Province/Territory	
14	Credential Revocation	2	Province/Territory	
15	Credential Authentication	2	Province/Territory	
16	Create Signature	…	Province/Territory	Federal service
17	Check Signature	…	Province/Territory	Federal service
18	Formulate Notice	…	Province/Territory	Federal service
19	Request Consent	…	Province/Territory	Federal service
20	Record Consent	…	Province/Territory	Federal service
21	Review Consent	…	Province/Territory	Federal service
22	Renew Consent	…	Province/Territory	Federal service
23	Expire Consent	…	Province/Territory	Federal service
24	Revoke Consent	…	Province/Territory	Federal service


Trusted Digital Identity Provider
Trusted Digital Identity Creation
Identity Creation
❑ Identity Resolution
❑ Identity Establishment
Credential Creation
❑ Credential Issuance
Credential Confirmation
❑ Credential-Authenticator Binding
❑ Credential Suspension
❑ Credential Recovery
❑ Credential Revocation
❑ Credential Authentication
Identity Registration
Identity Confirmation
❑ Identity Validation
❑ Identity Verification
❑ Evidence Validation
❑ Identity Presentation
❑ Identity Maintenance
Binding
❑ Identity-Credential Binding
Informed Consent
❑ Formulate Notice
❑ Request Consent
❑ Record Consent
❑ Review Consent
❑ Renew Consent
❑ Expire Consent
❑ Revoke Consent
Supporting Infrastructure
Identity Assurance (Identity Proofing)
In scope for the PCTF assessment process


Relying Party (as a TDI Consumer)
Service Enrolment (using a TDI)
Identity Creation
❑ Identity Resolution
❑ Identity Establishment
Service Registration
Linking
❑ Identity Linking
Informed Consent
❑ Formulate Notice
❑ Request Consent
❑ Record Consent
❑ Review Consent
❑ Renew Consent
❑ Expire Consent
❑ Revoke Consent
Supporting Infrastructure
Identity Assurance
(Identity Proofing)

Government of Canada Digital Standards

A Set of Guiding Principles