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

Consultation Deck
(for Discussion Purposes Only)

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

2019-03-28

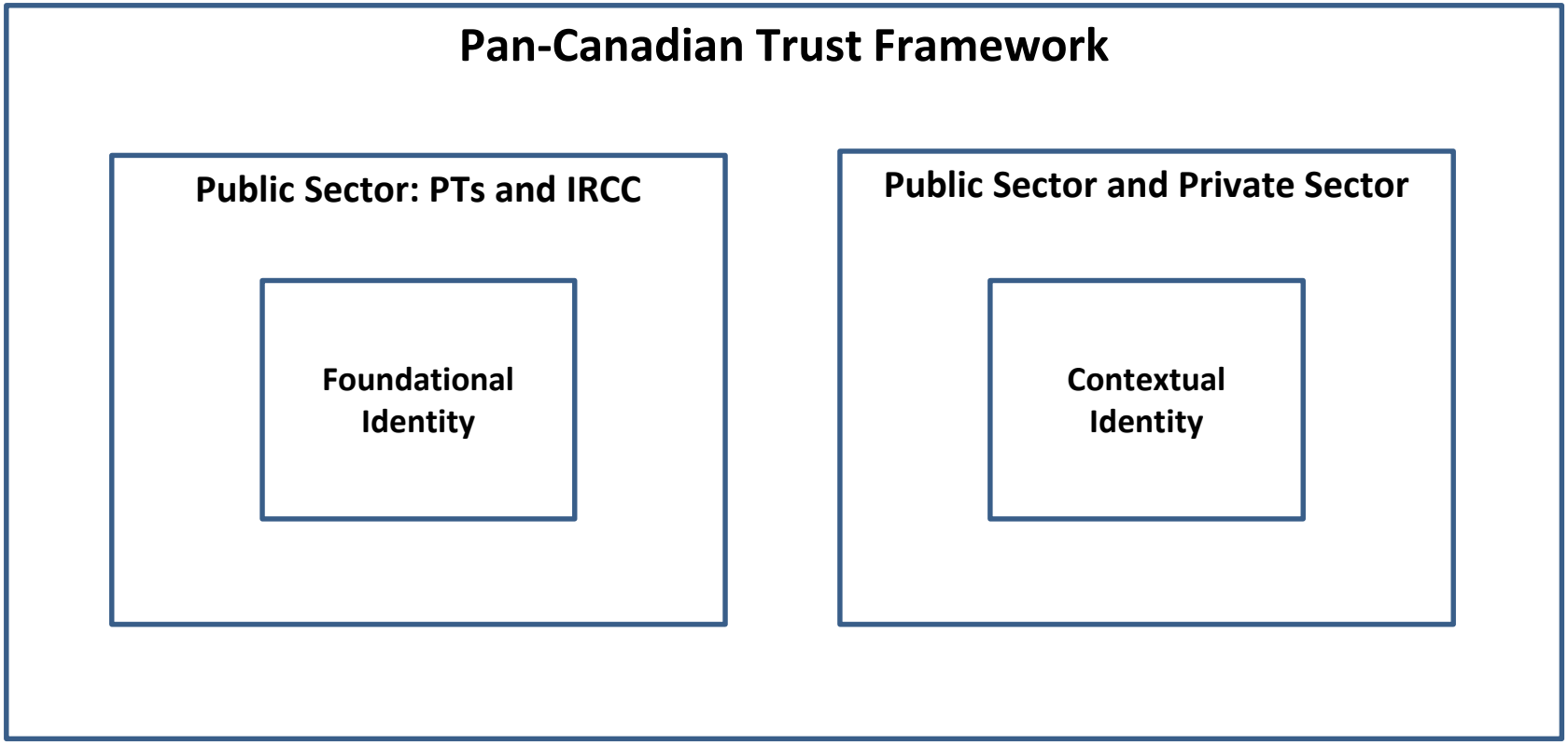
Characteristics of the PCTF

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 ecosystem development

Trusted Digital Representations and Trusted Processes

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

Identity Domains



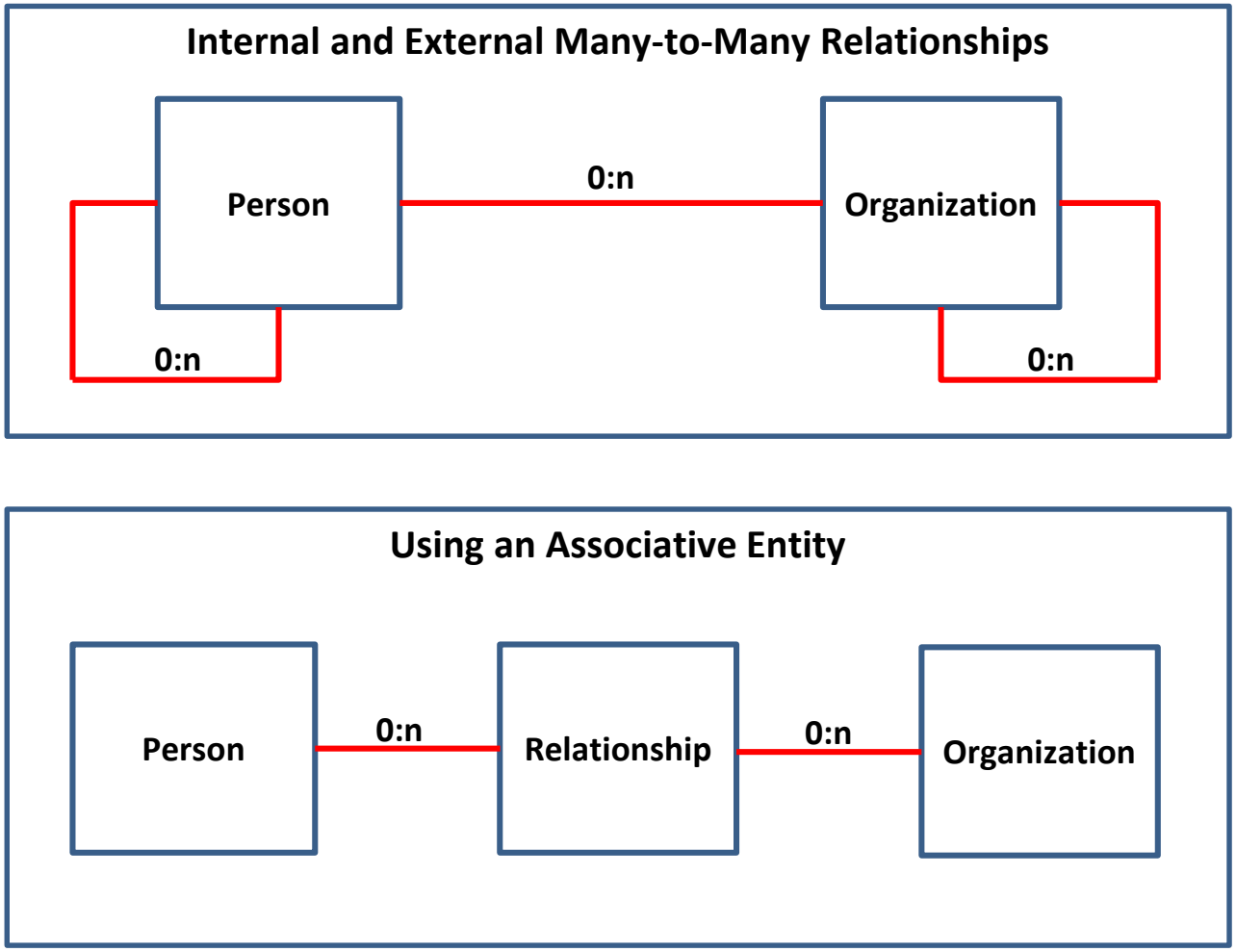
Trusted Digital Representations

Trusted Digital Identity (Person)

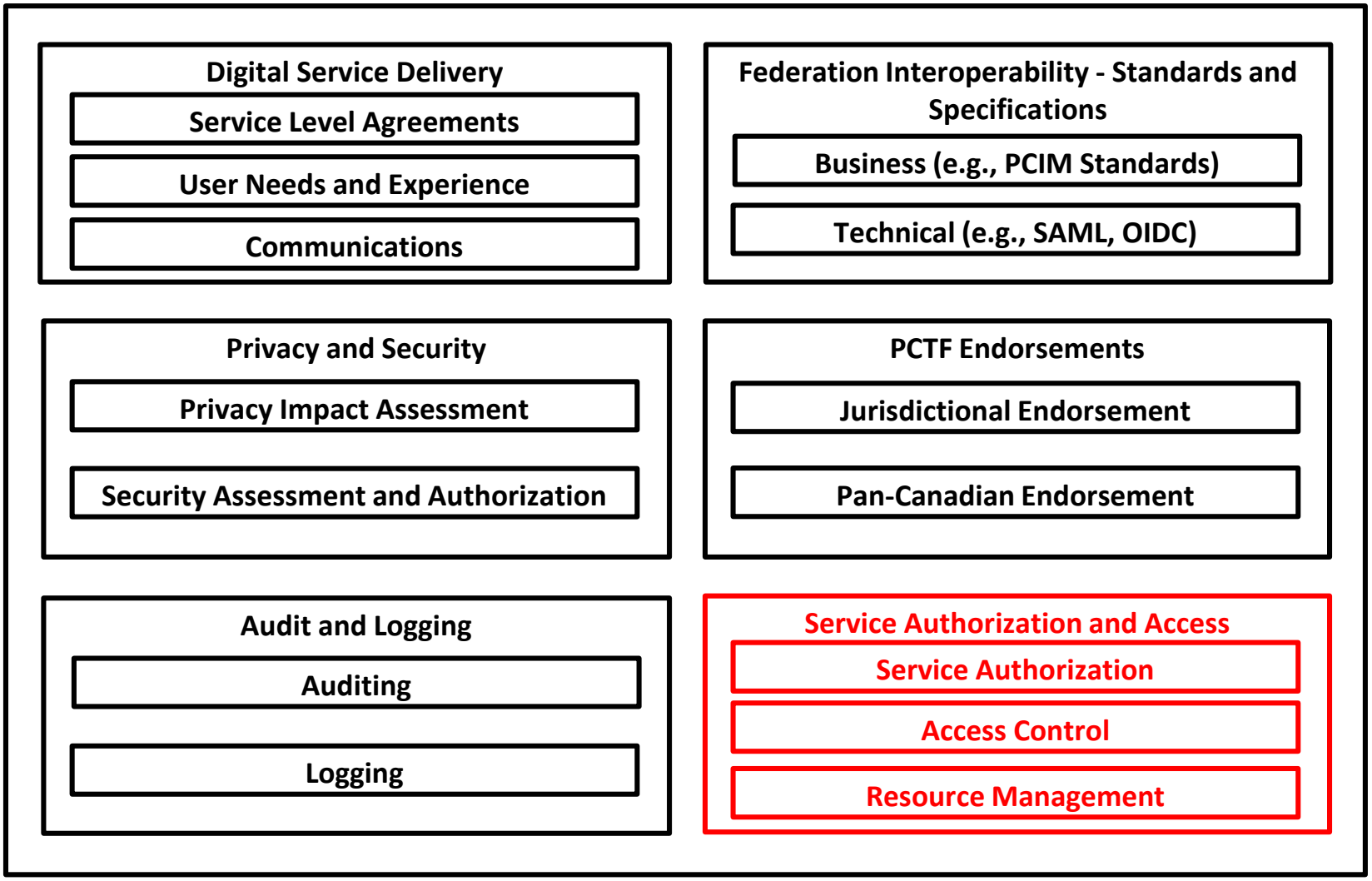
Trusted Digital Identity (Organization)

Trusted Digital Relationship

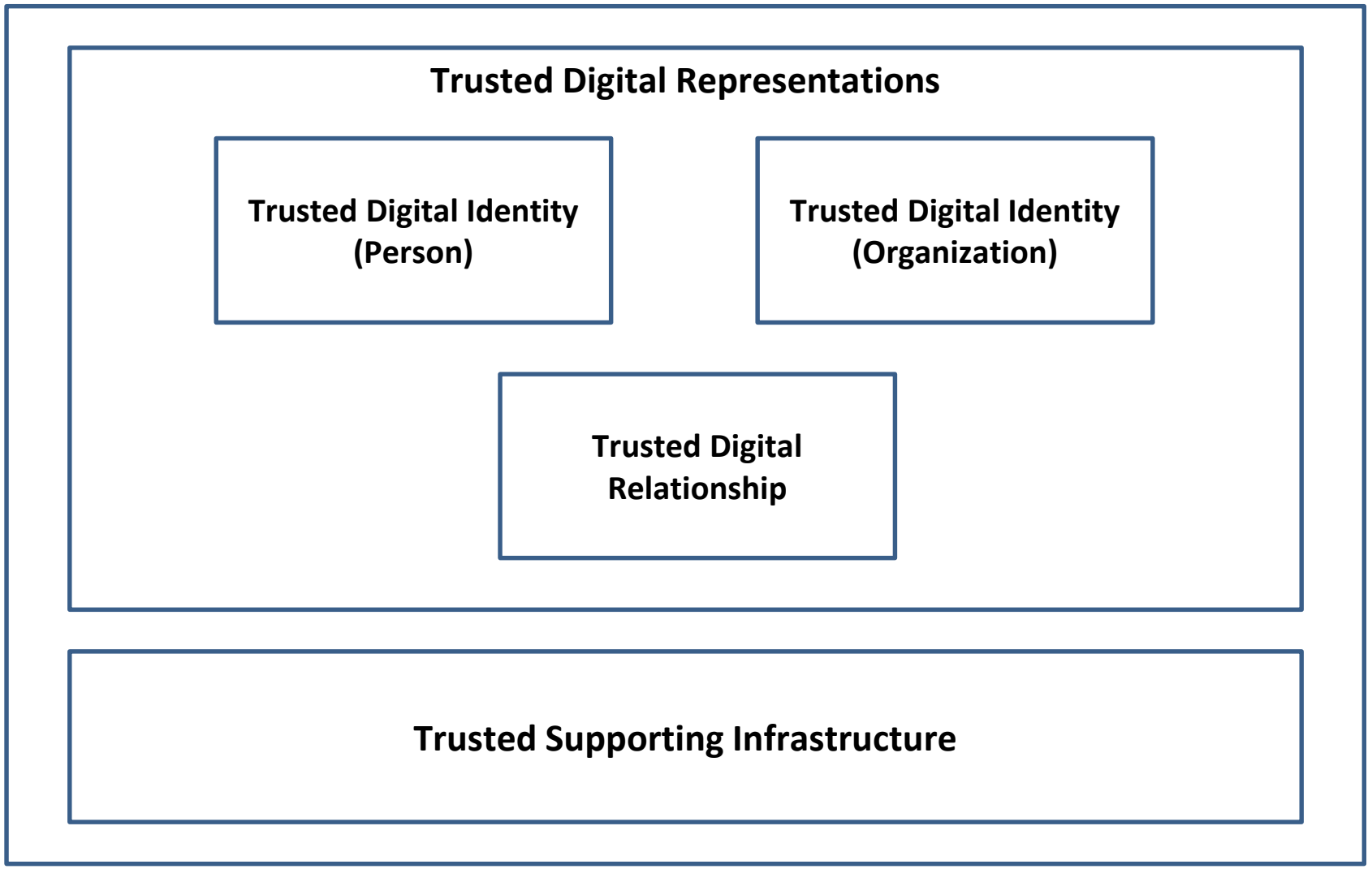
Entities and Relationships



Trusted Supporting Infrastructure

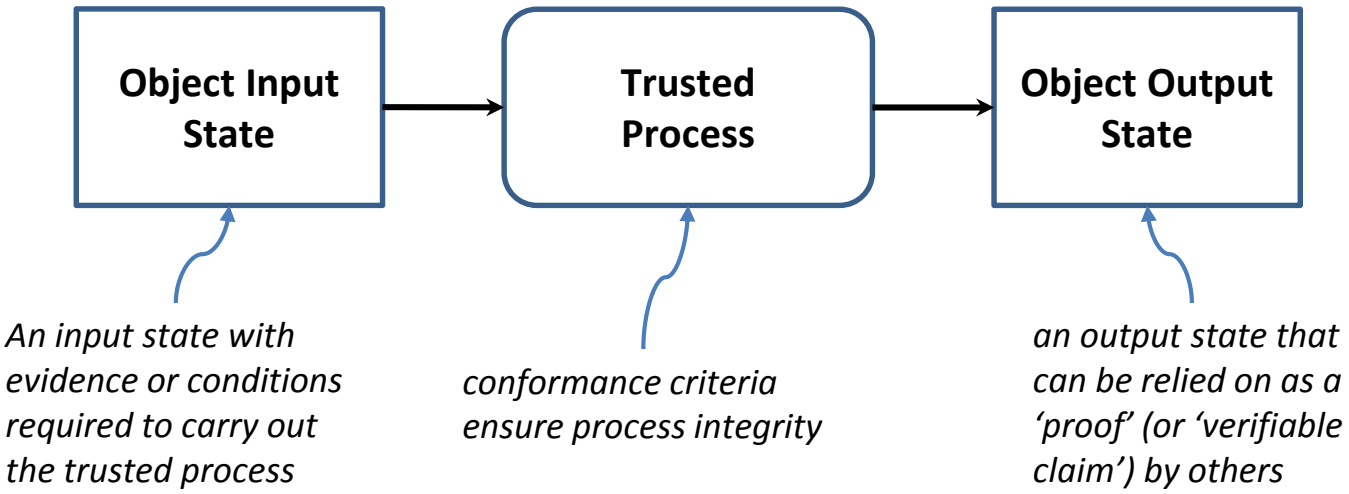


Pan-Canadian Trust Framework Model



Trusted Process Model

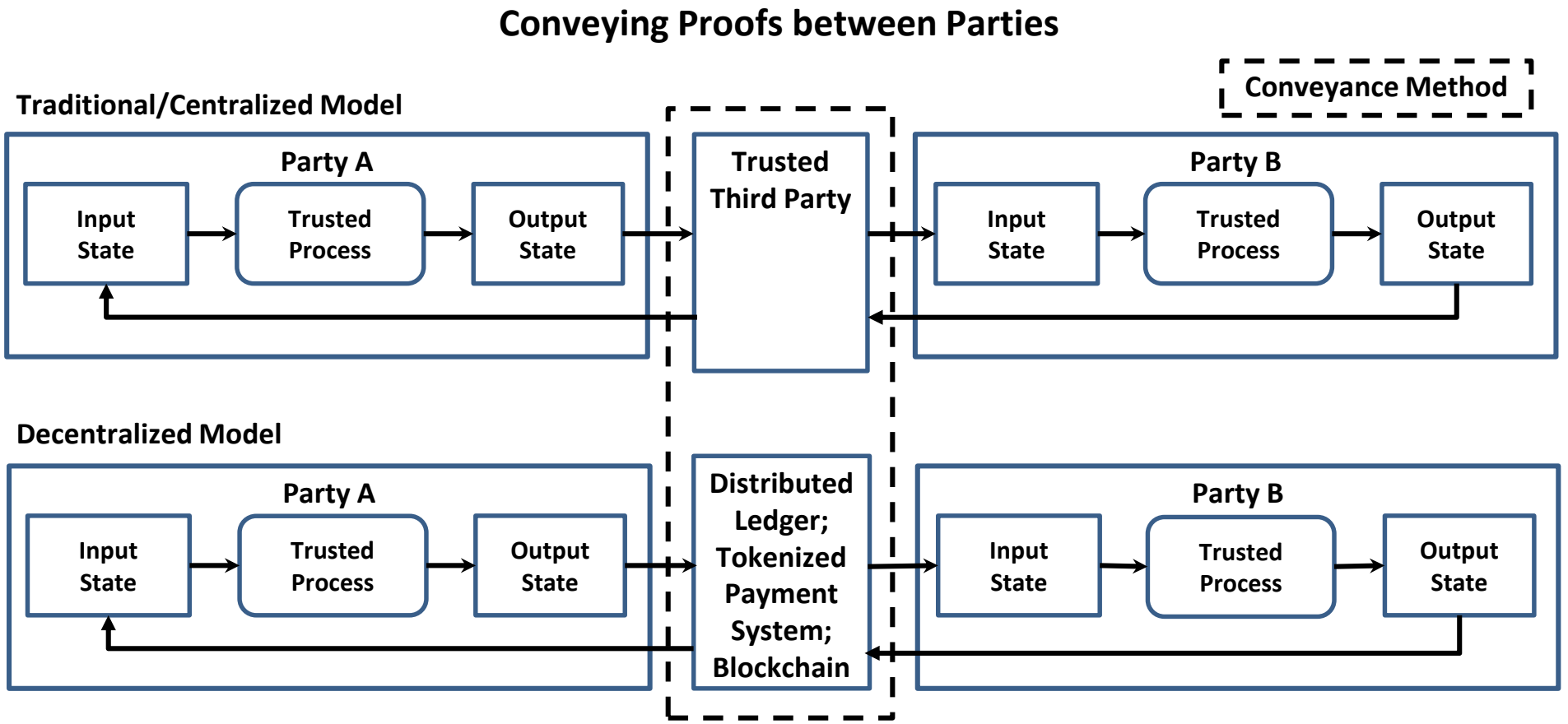
A trusted process is an activity (or set of activities) that results in the state transition of an object; the object's output state can be relied on by other trusted processes.



*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

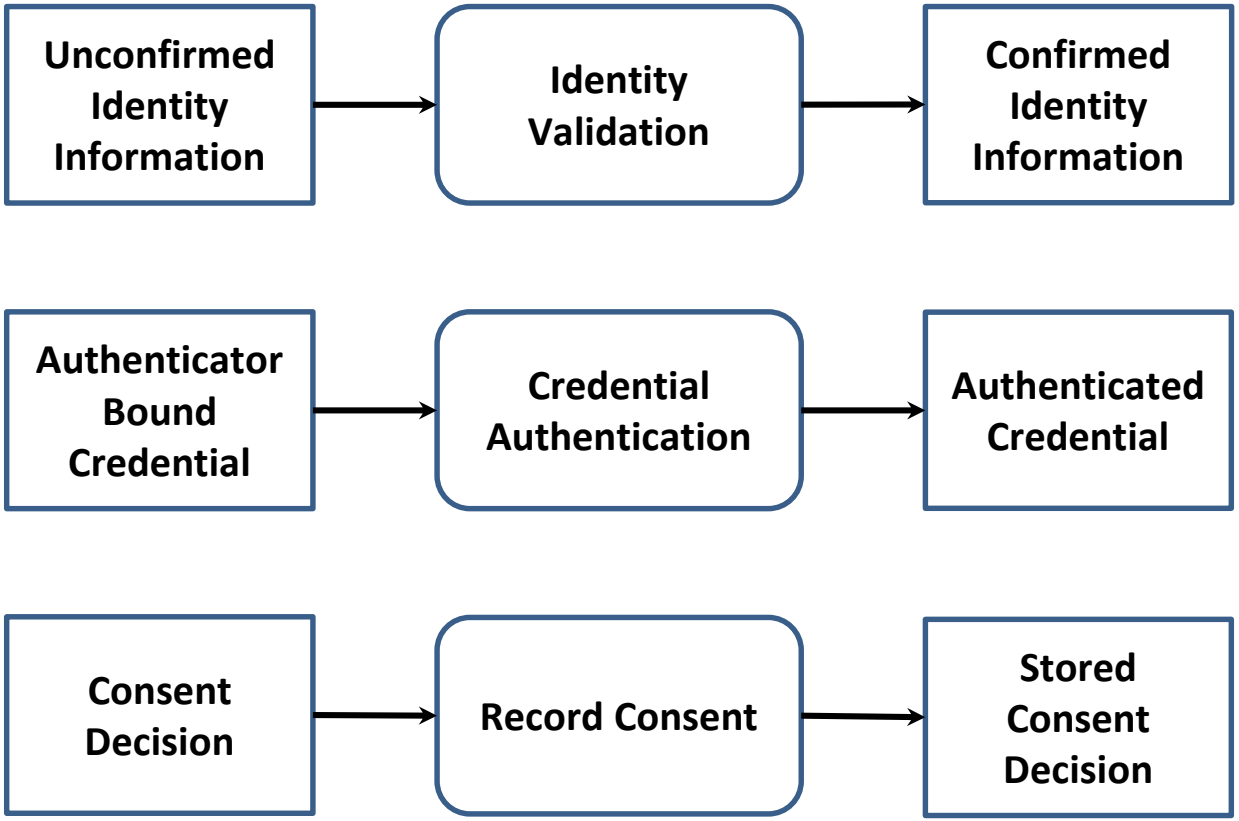
*Trusted process inputs and outputs (i.e., proofs) are **independent** of the conveyance model.*



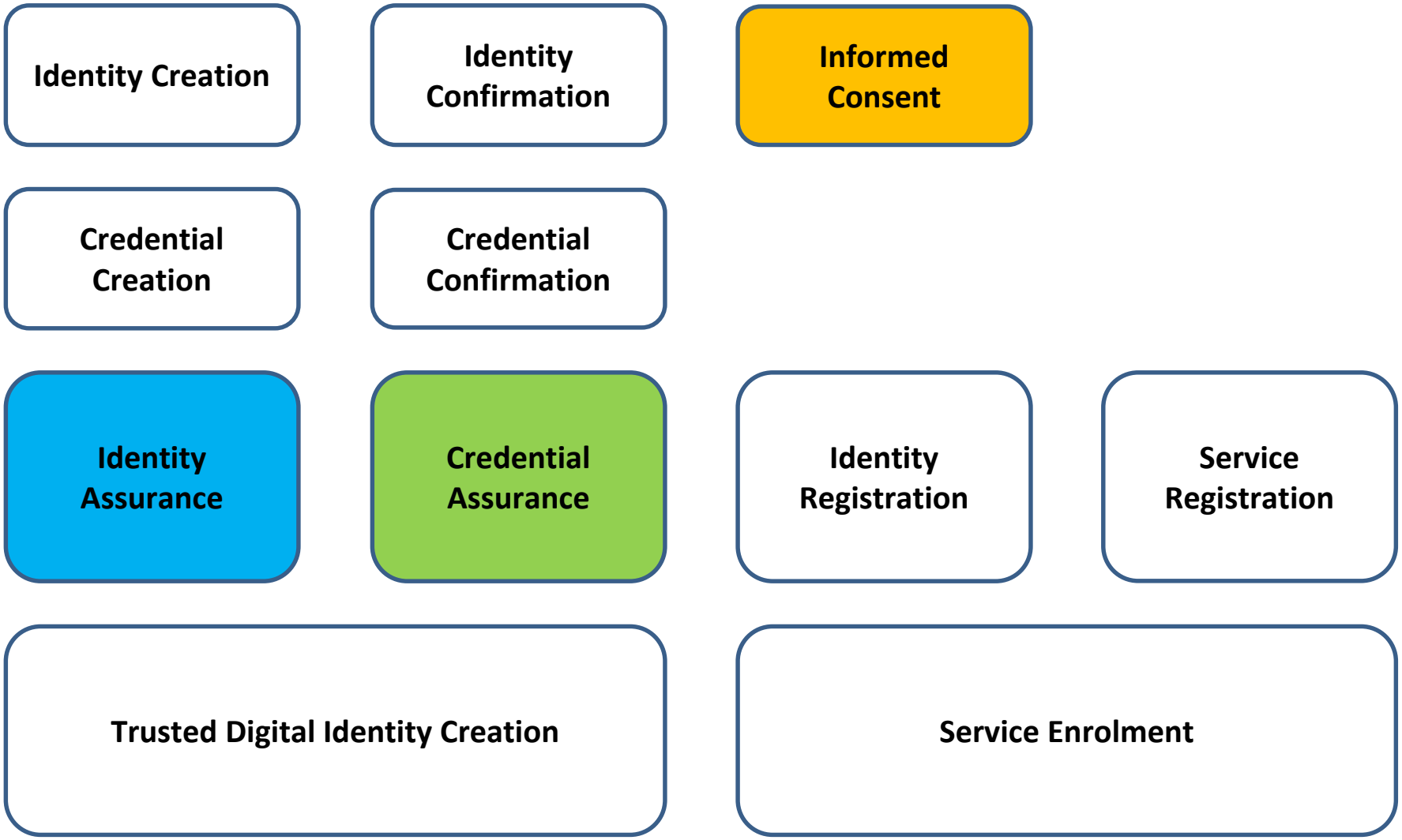
Atomic Trusted Processes

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

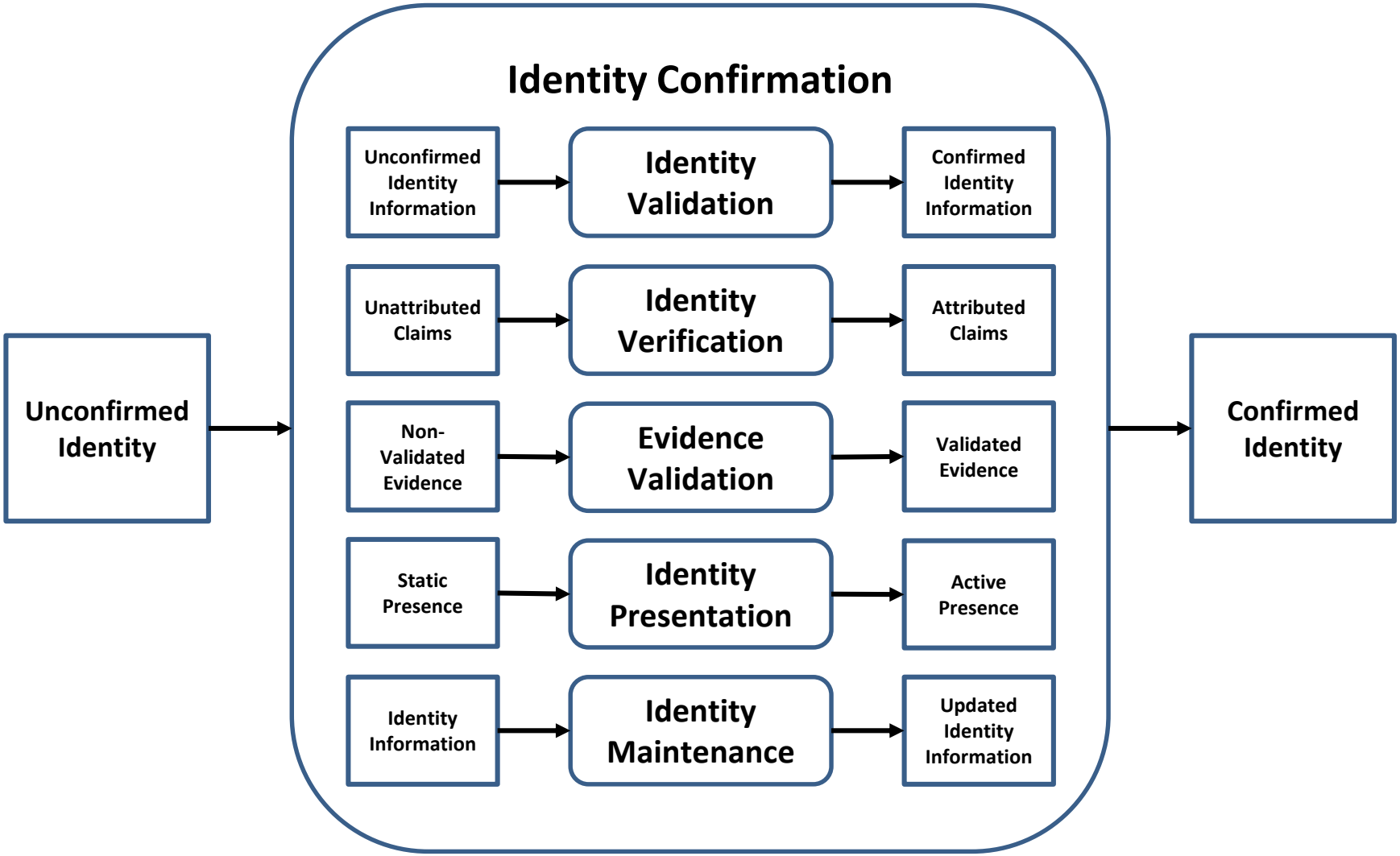
Examples of Atomic Trusted Processes (Modeled)



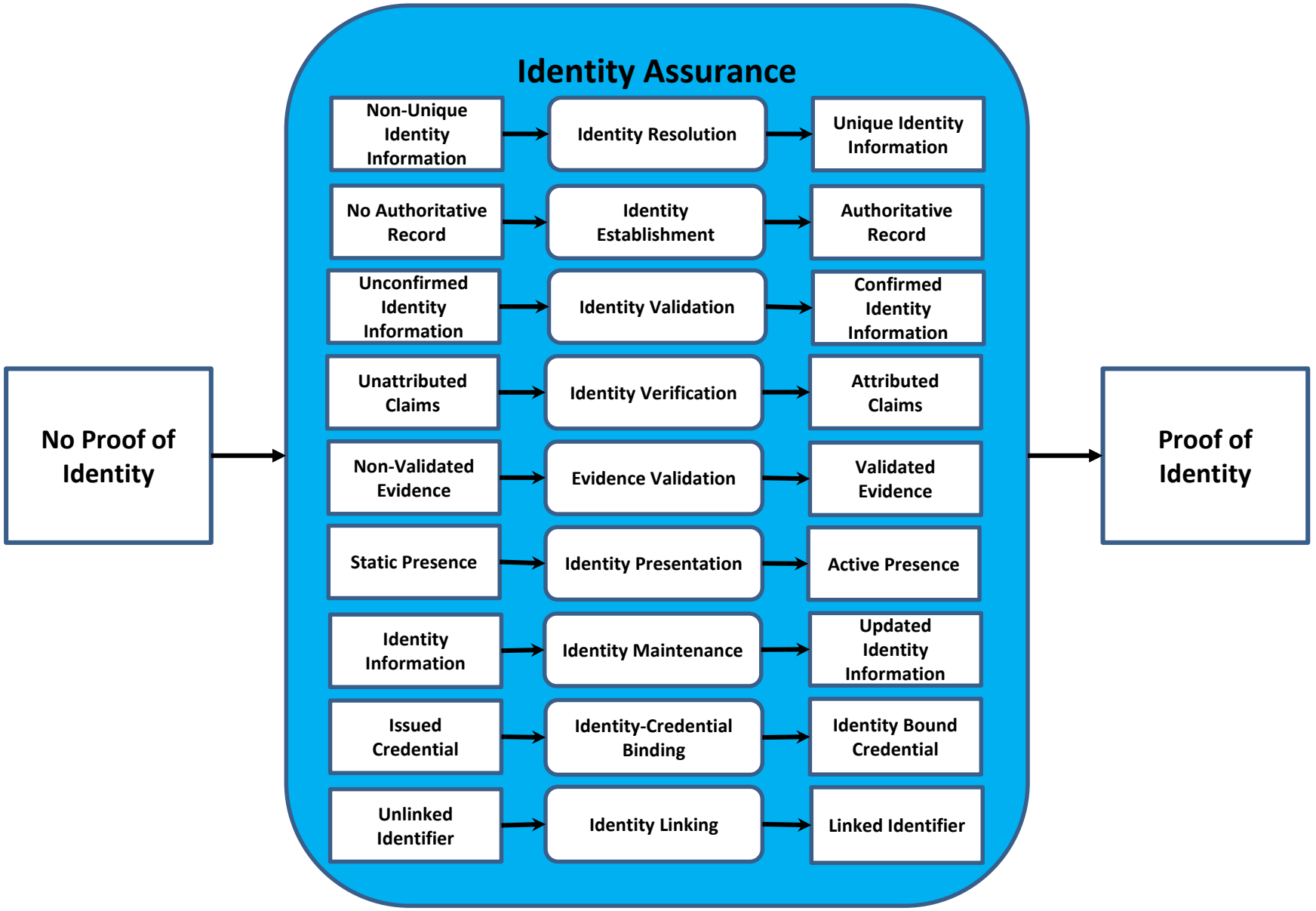
Compound Trusted Processes



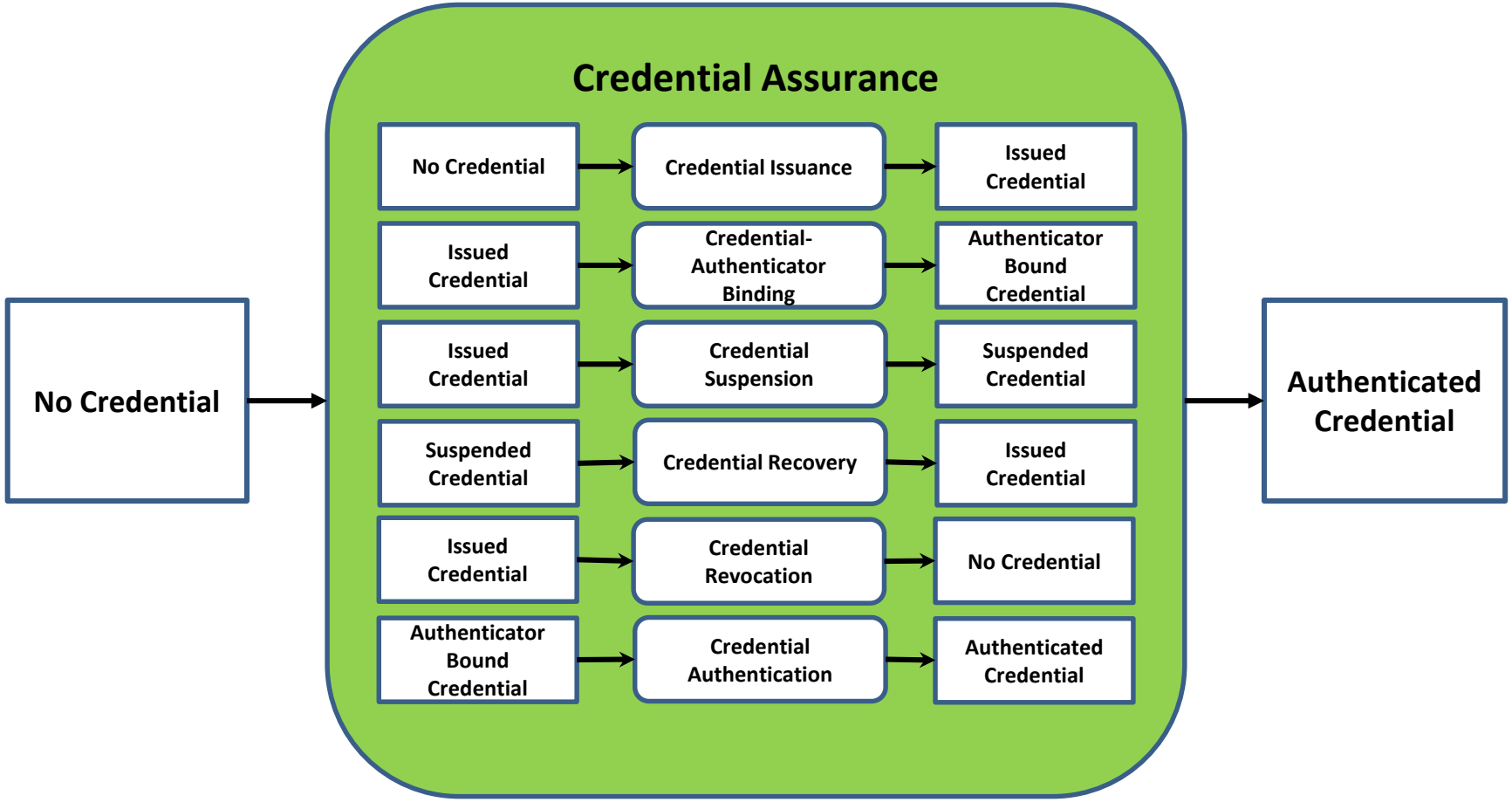
Compound Trusted Process: *Identity Confirmation* (Modeled)



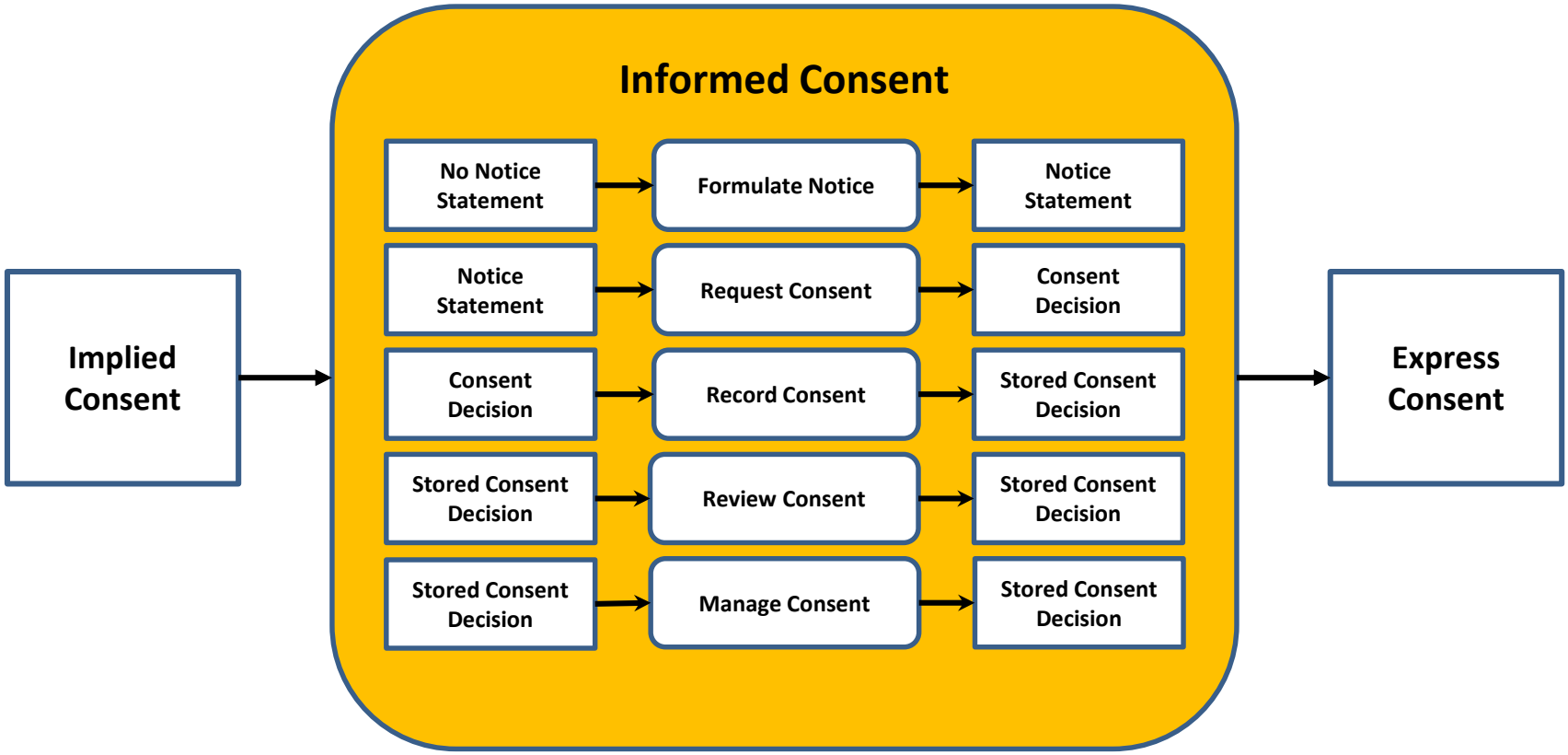
Compound Trusted Process: *Identity Assurance*



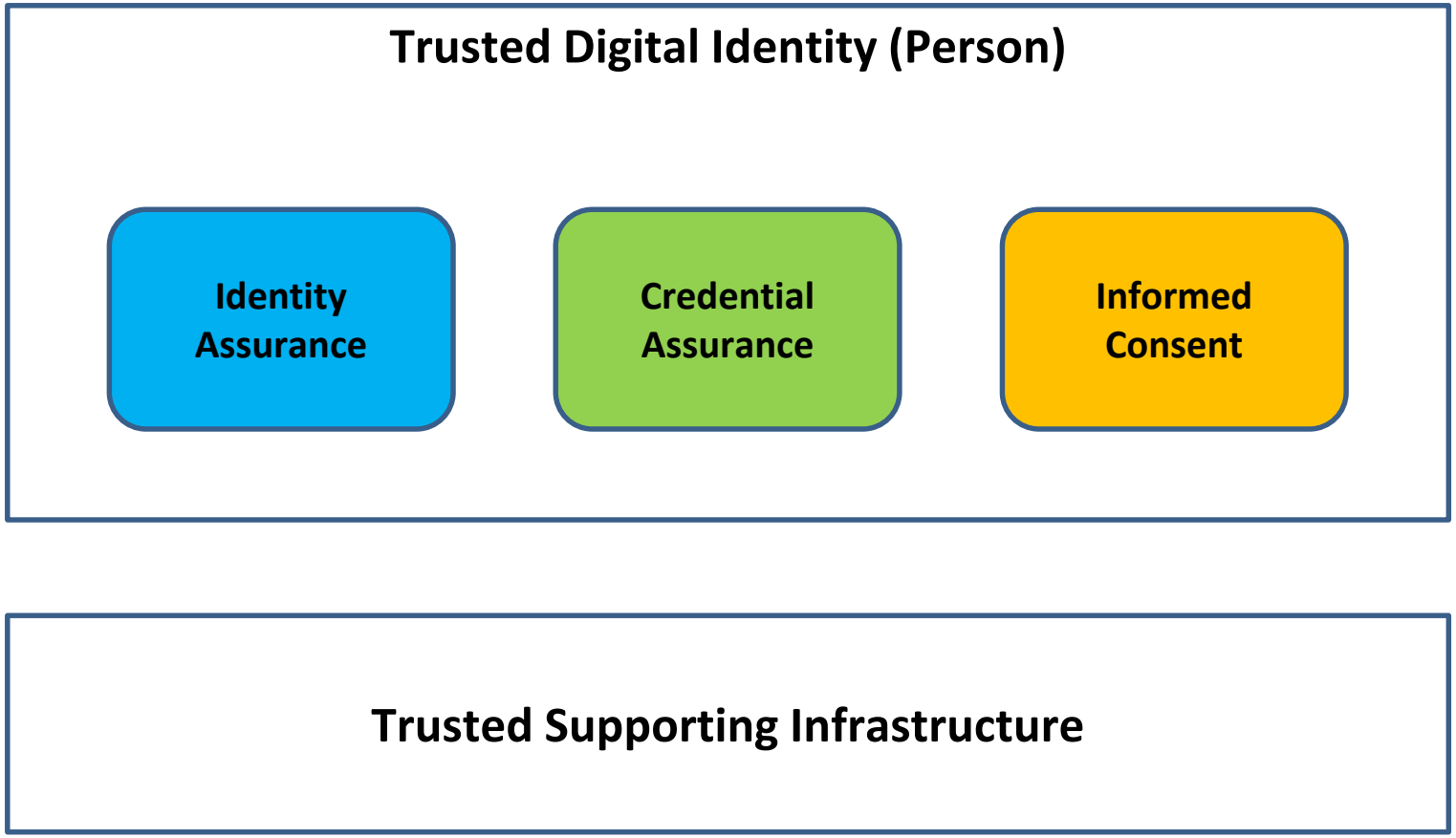
Compound Trusted Process: *Credential Assurance*



Compound Trusted Process: *Informed Consent*

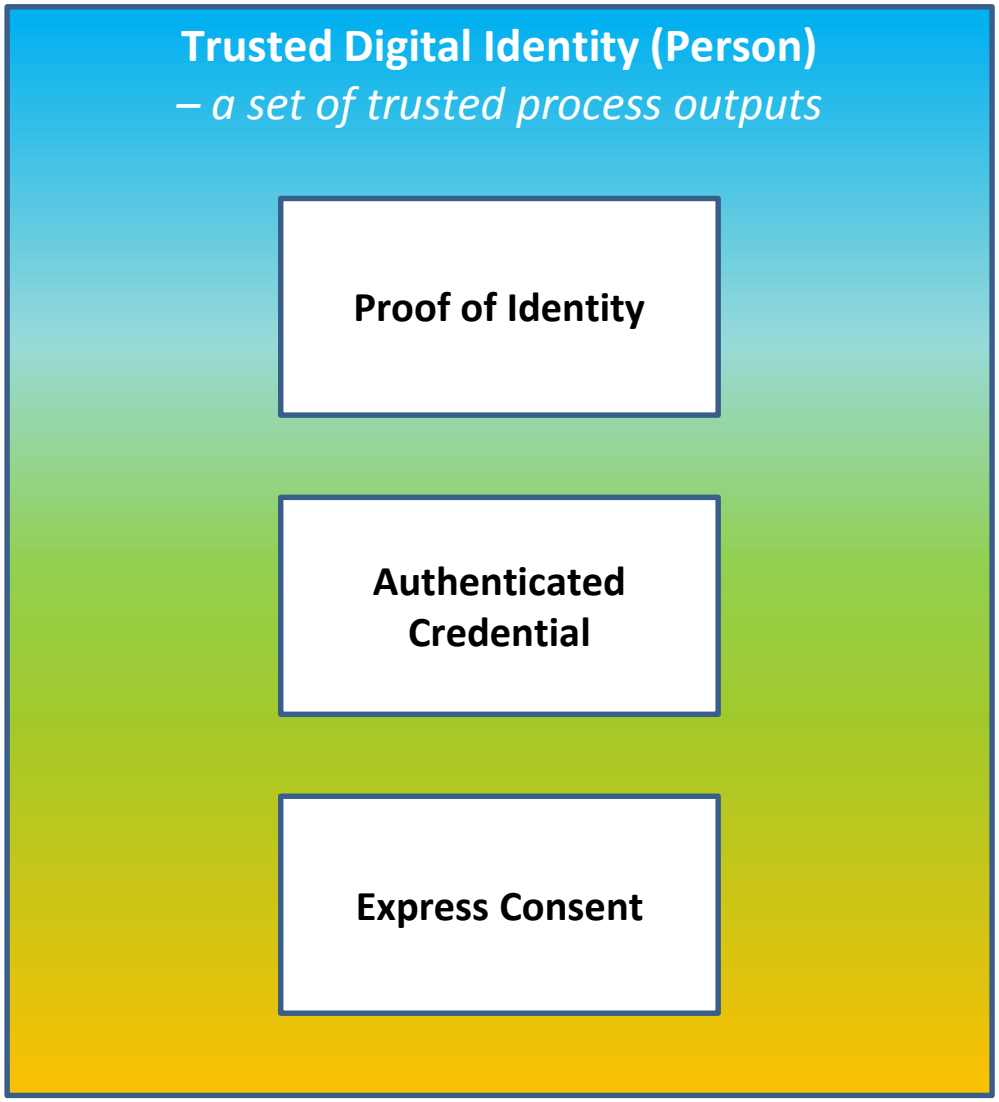


Compound Trusted Process: *Trusted Digital Identity (Person) Creation*

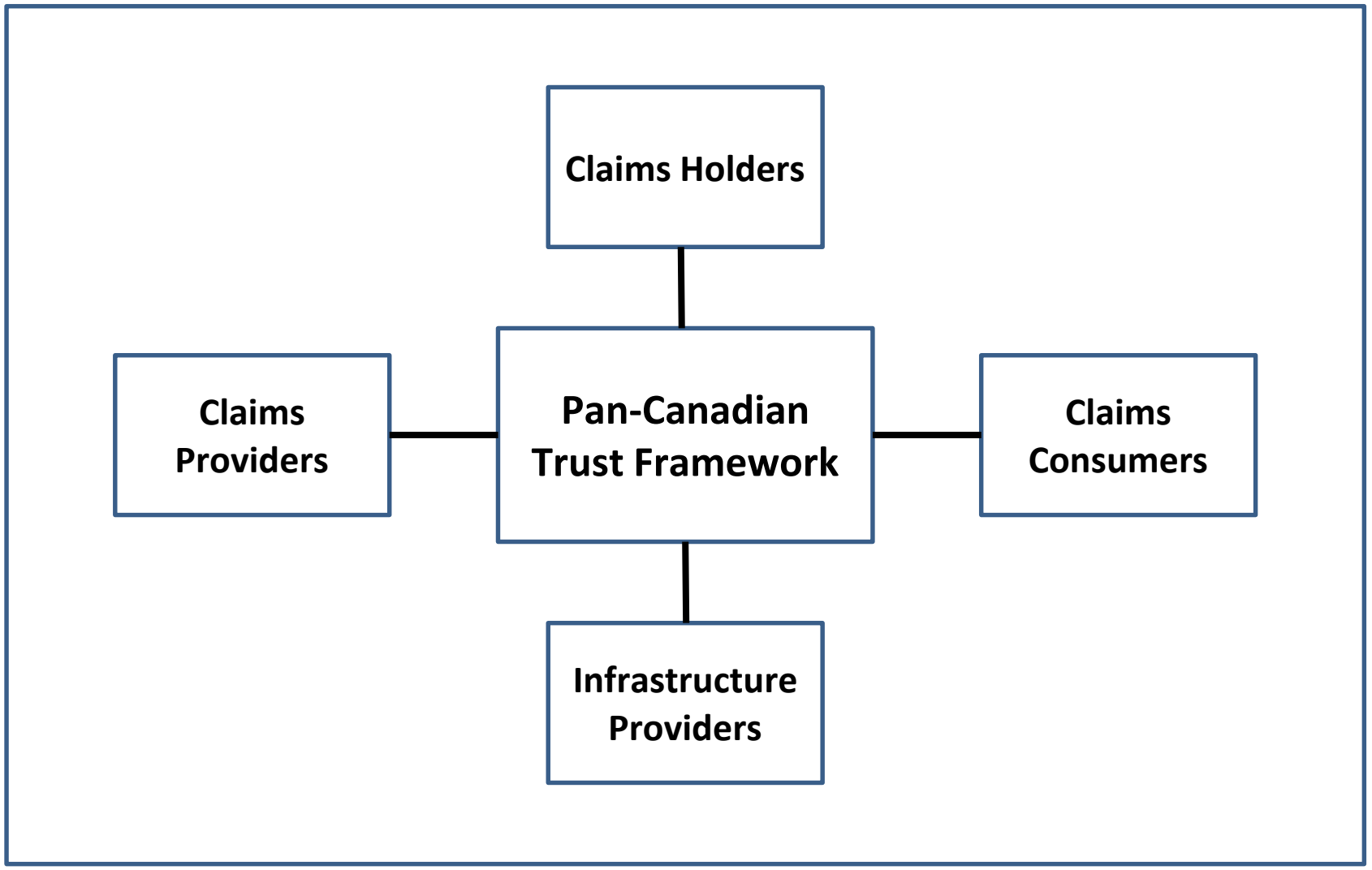


*A **trusted digital Identity** can be conceptualized as a set of trusted process outputs (proofs) that are independent of the conveyance method.*

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 Roles



Participant Roles

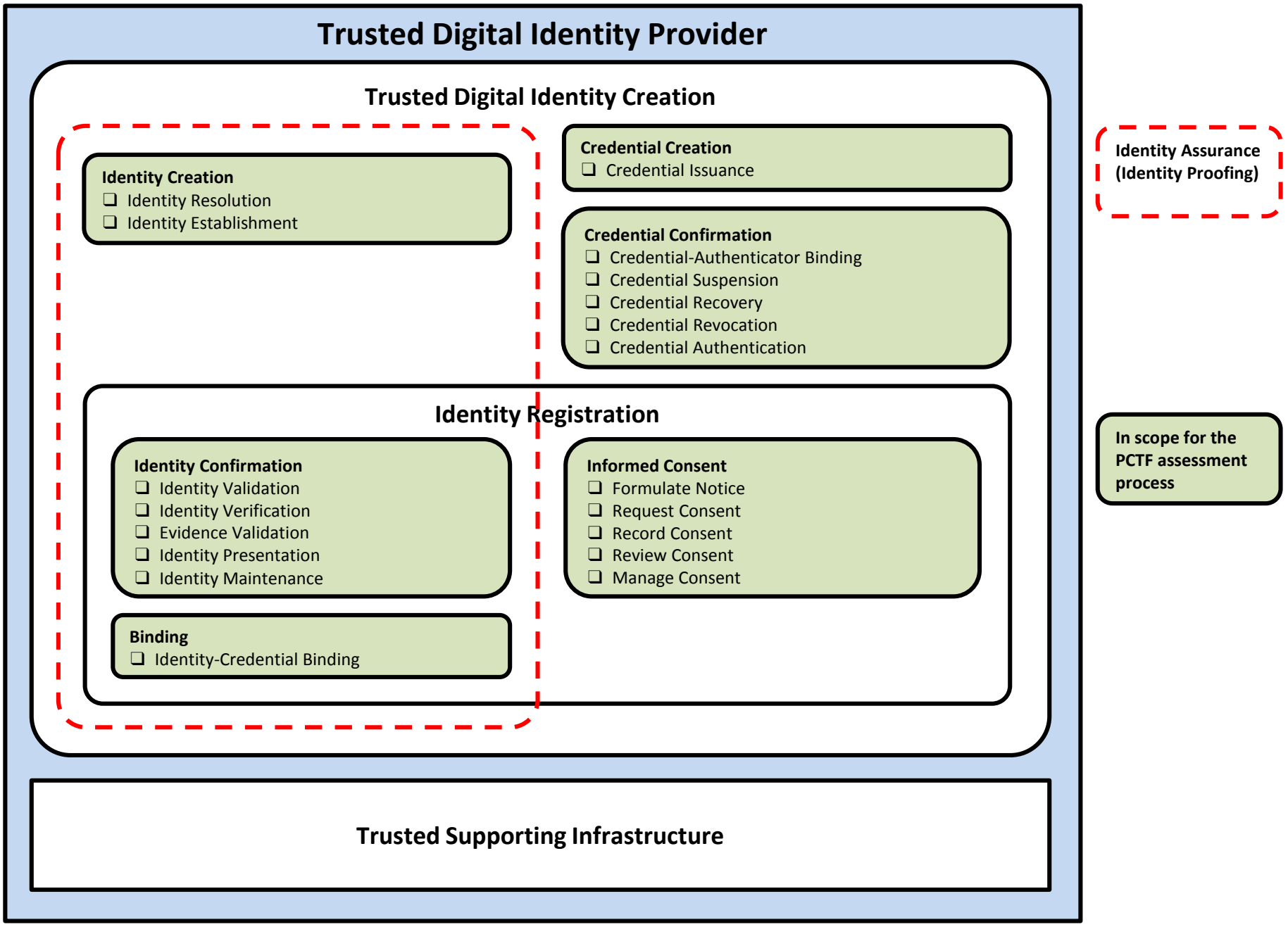
- Identity Assurance Providers
- Credential Assurance Providers
- Trusted Digital Identity (TDI) Providers
- Relying Parties (as TDI Consumers)
- Digital Identity Owners
- Infrastructure Providers

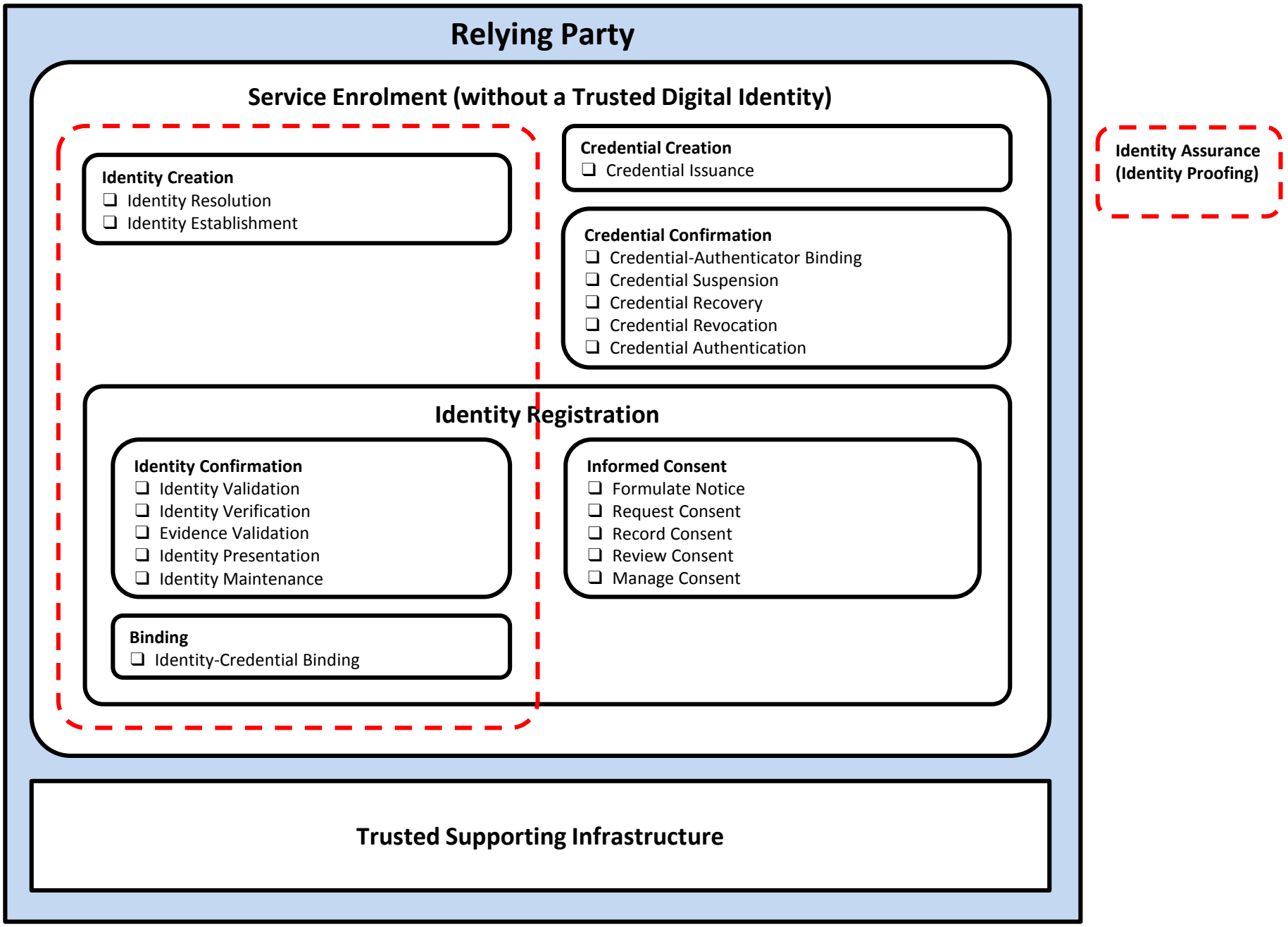
Trusted Processes by Participant Roles

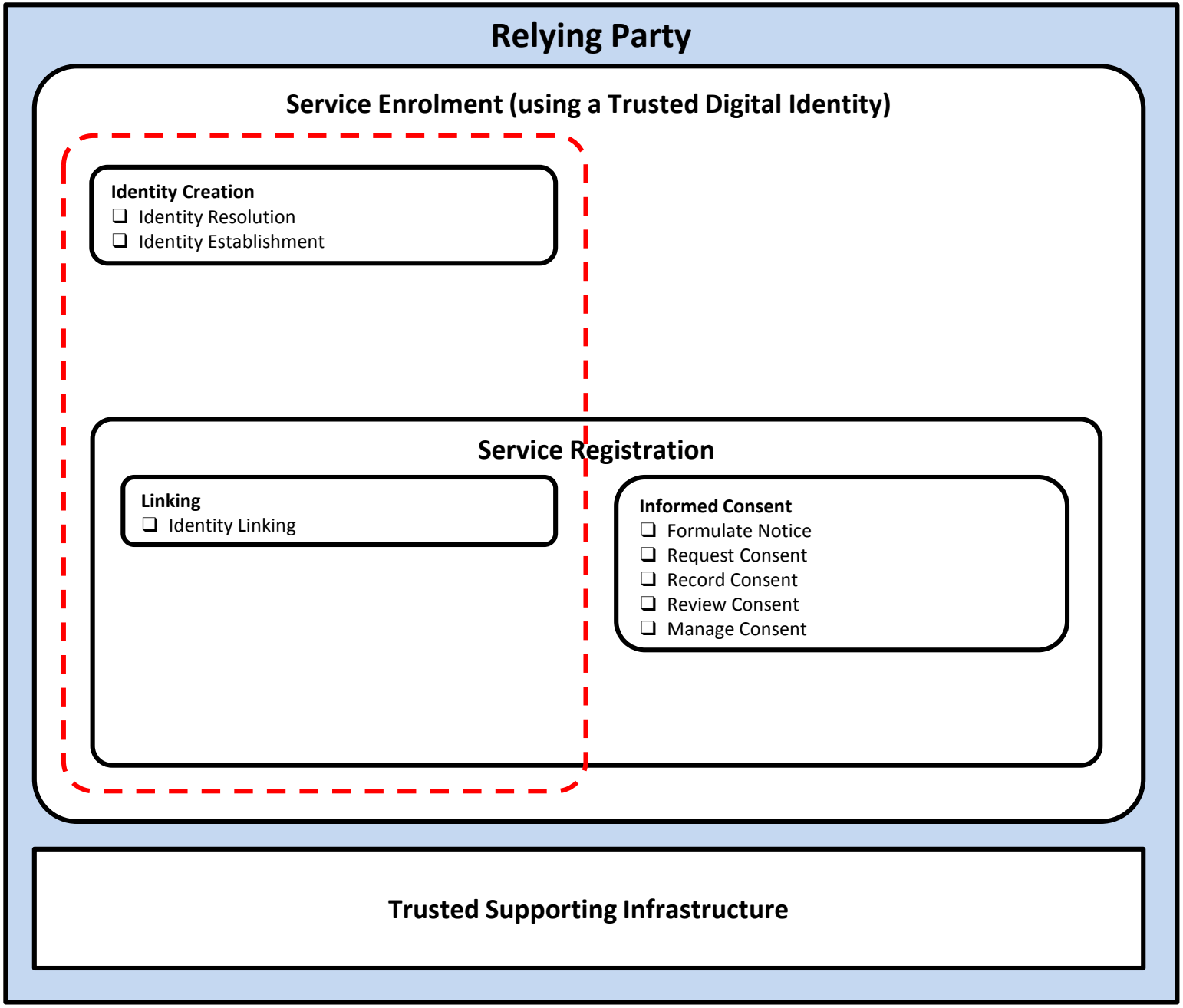
No.	Trusted Process	Identity Assurance Provider	Credential Assurance Provider	Trusted Digital Identity (TDI) Provider	Relying Party (as a TDI Consumer)
1	Identity Resolution	X		X	X
2	Identity Establishment	X		X	X
3	Identity Validation	X		X	
4	Identity Verification	X		X	
5	Evidence Validation	X		X	
6	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	Formulate Notice			X	X
17	Request Consent			X	X
18	Record Consent			X	X
19	Review Consent			X	X
20	Manage Consent			X	X
21	Signature				X

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

No.	Trusted Process	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	Formulate Notice	…	Province/Territory	Federal service
17	Request Consent	…	Province/Territory	Federal service
18	Record Consent	…	Province/Territory	Federal service
19	Review Consent	…	Province/Territory	Federal service
20	Manage Consent	…	Province/Territory	Federal service
21	Signature	…		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
Informed Consent
❑ Formulate Notice
❑ Request Consent
❑ Record Consent
❑ Review Consent
❑ Manage Consent
Binding
❑ Identity-Credential Binding
Trusted Supporting Infrastructure
Identity Assurance (Identity Proofing)
In scope for the PCTF assessment process


Relying Party
Service Enrolment (without a Trusted Digital Identity)
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
Informed Consent
❑ Formulate Notice
❑ Request Consent
❑ Record Consent
❑ Review Consent
❑ Manage Consent
Binding
❑ Identity-Credential Binding
Trusted Supporting Infrastructure
Identity Assurance
(Identity Proofing)


Relying Party
Service Enrolment (using a Trusted Digital Identity)
Identity Creation
❑ Identity Resolution
❑ Identity Establishment
Service Registration
Linking
❑ Identity Linking
Informed Consent
❑ Formulate Notice
❑ Request Consent
❑ Record Consent
❑ Review Consent
❑ Manage Consent
Trusted Supporting Infrastructure
Identity Assurance
(Identity Proofing)

Government of Canada Digital Standards

A Set of Guiding Principles