Overview of the Pan-Canadian Trust Framework v2.0 (a.k.a. the "Beta" Version)

Consultation Deck
For Discussion Purposes Only

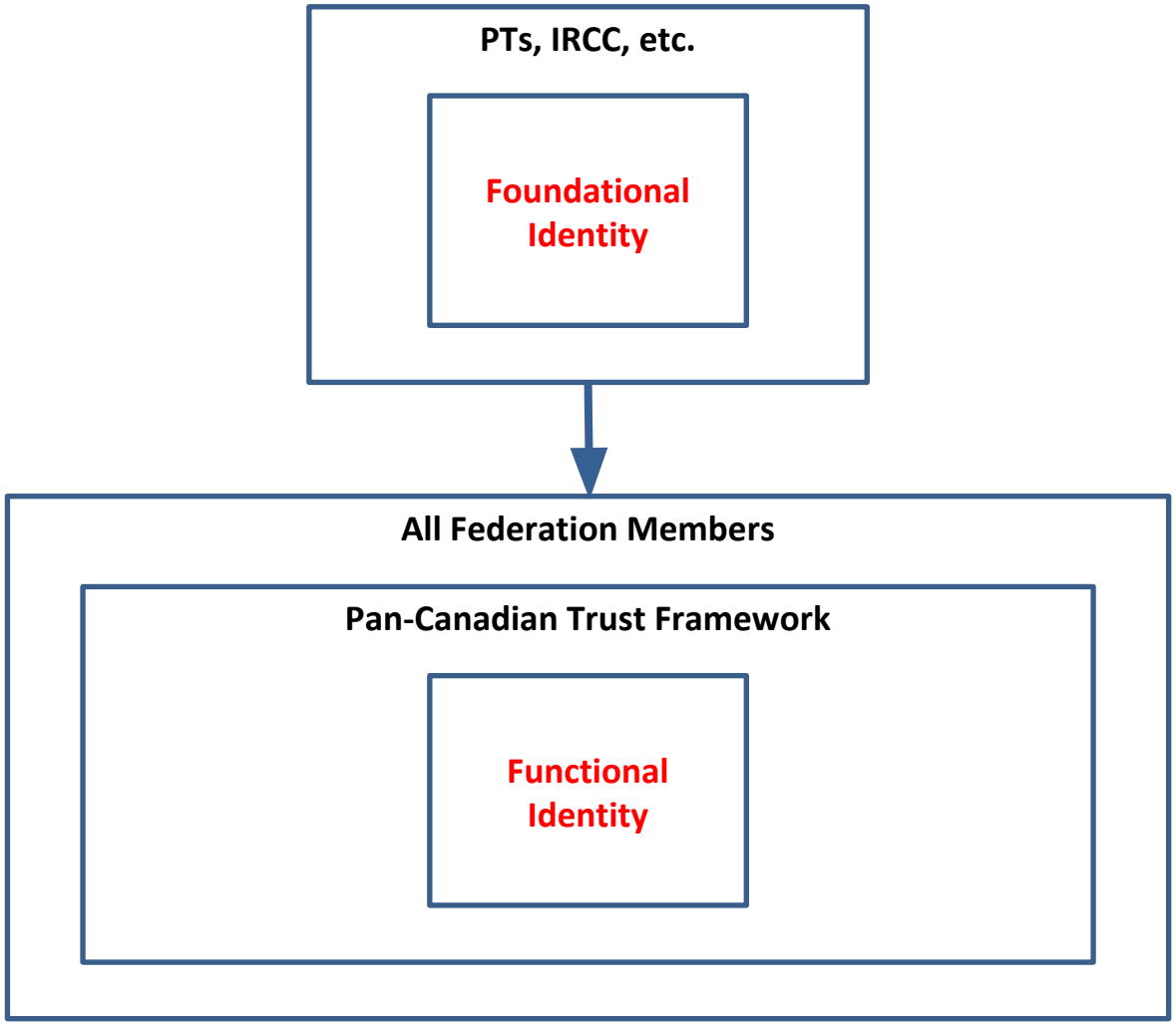
Framework Goals

1. **Simple and integrative framework** that is easy to understand but can be applied in a complex enviroment
2. **Technology-agnostic** to provide flexibility and logical precision in assessing the trustworthiness of digital identity solutions and providers
3. **Complement existing frameworks** (security, privacy, service delivery, etc.)
4. **Provide clear links to applicable policy, regulation and legislation** (by defining conformance criteria that can be easily mapped)
5. **Normalize (standardize) key processes and capabilities** to enable cross-sector collaboration and ecosystem development.

Foundational Identity Versus Functional Identity

Public sector

Public and private sector

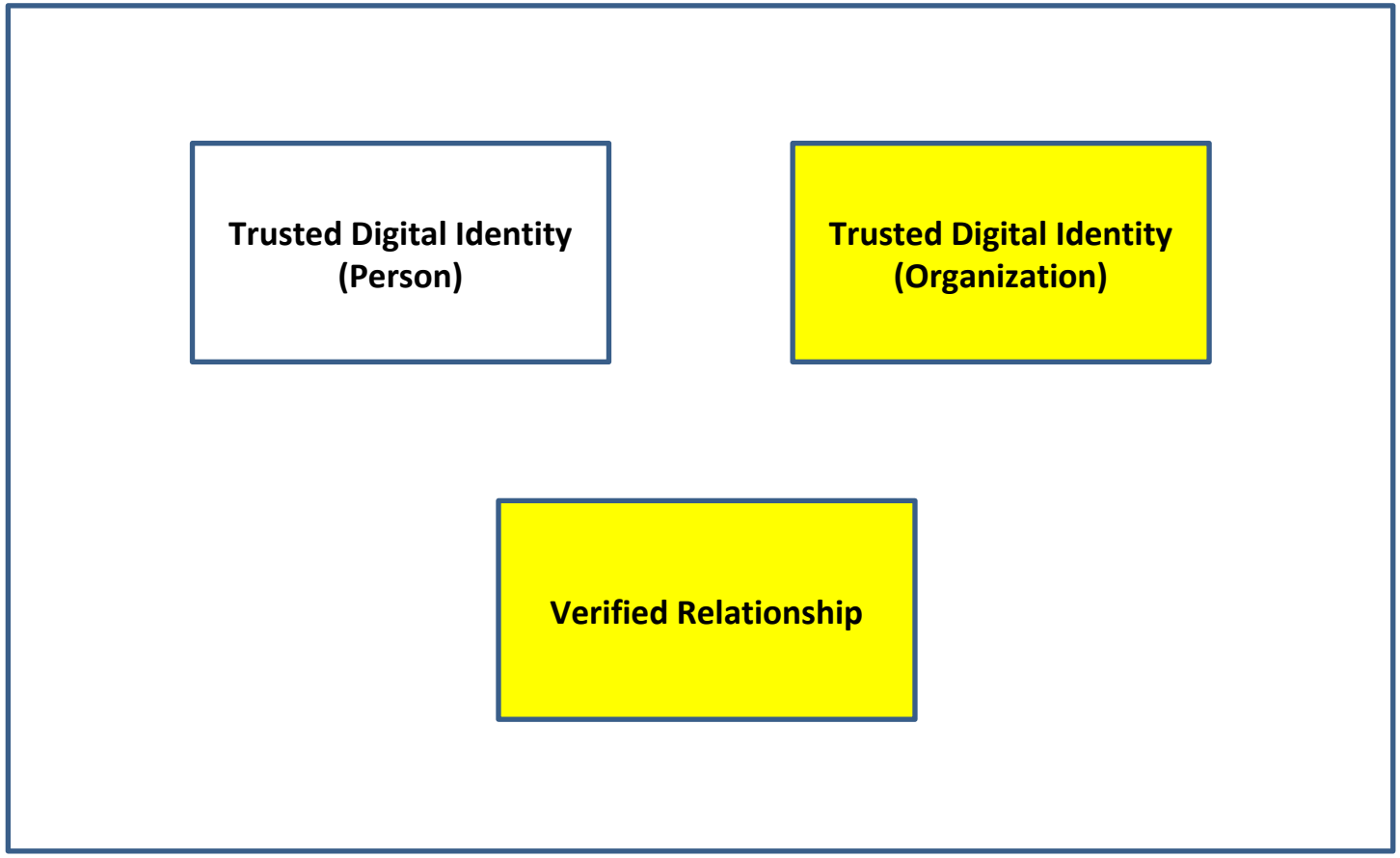


For discussion purposes only

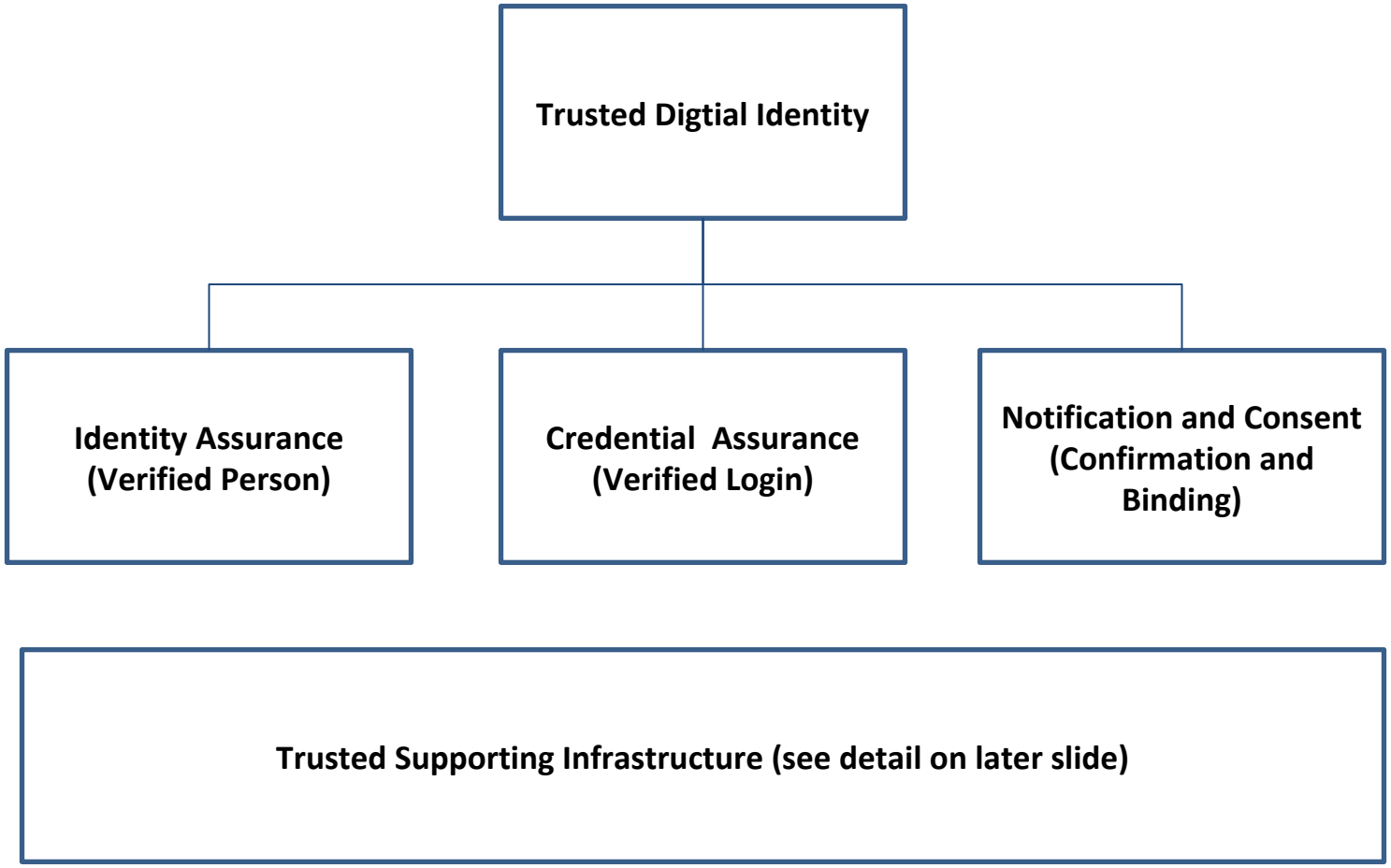
PCTF Trusted Representations and Trusted Processes

- Currently Identified for the PCTF:
  - 3 trusted respresentations
  - 24 *atomic* trusted processes
- Extensible approach: other trusted processes can be added as required
- Interoperable: the trusted processes can be mapped to Vectors of Trust (VoT)
- The atomic trusted processes can be divided among 3 broad categories:
  - Identity Assurance
  - Credential Assurance
  - Notification and Consent
- Various atomic trusted processes are often grouped together to form *compound* trusted processes

Trusted Digital Representations

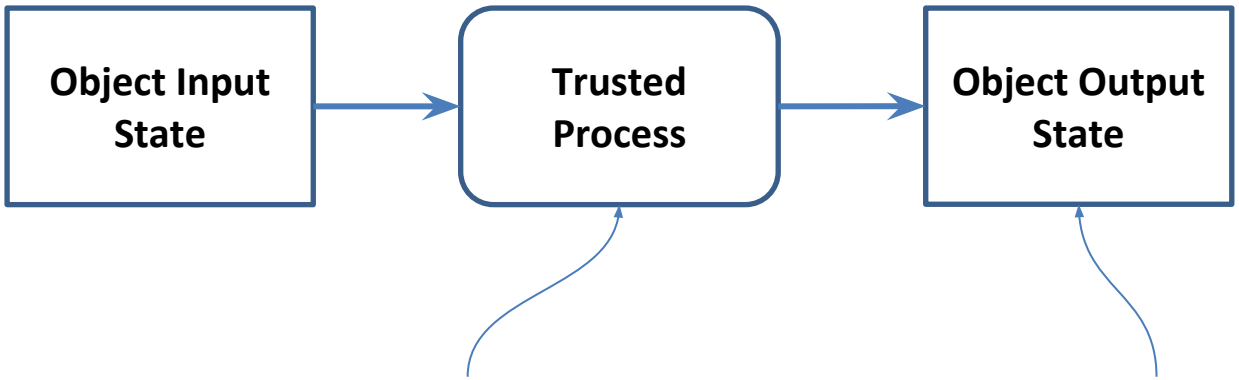


Trusted Digital Identity (Individual)



Trusted Process Model

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

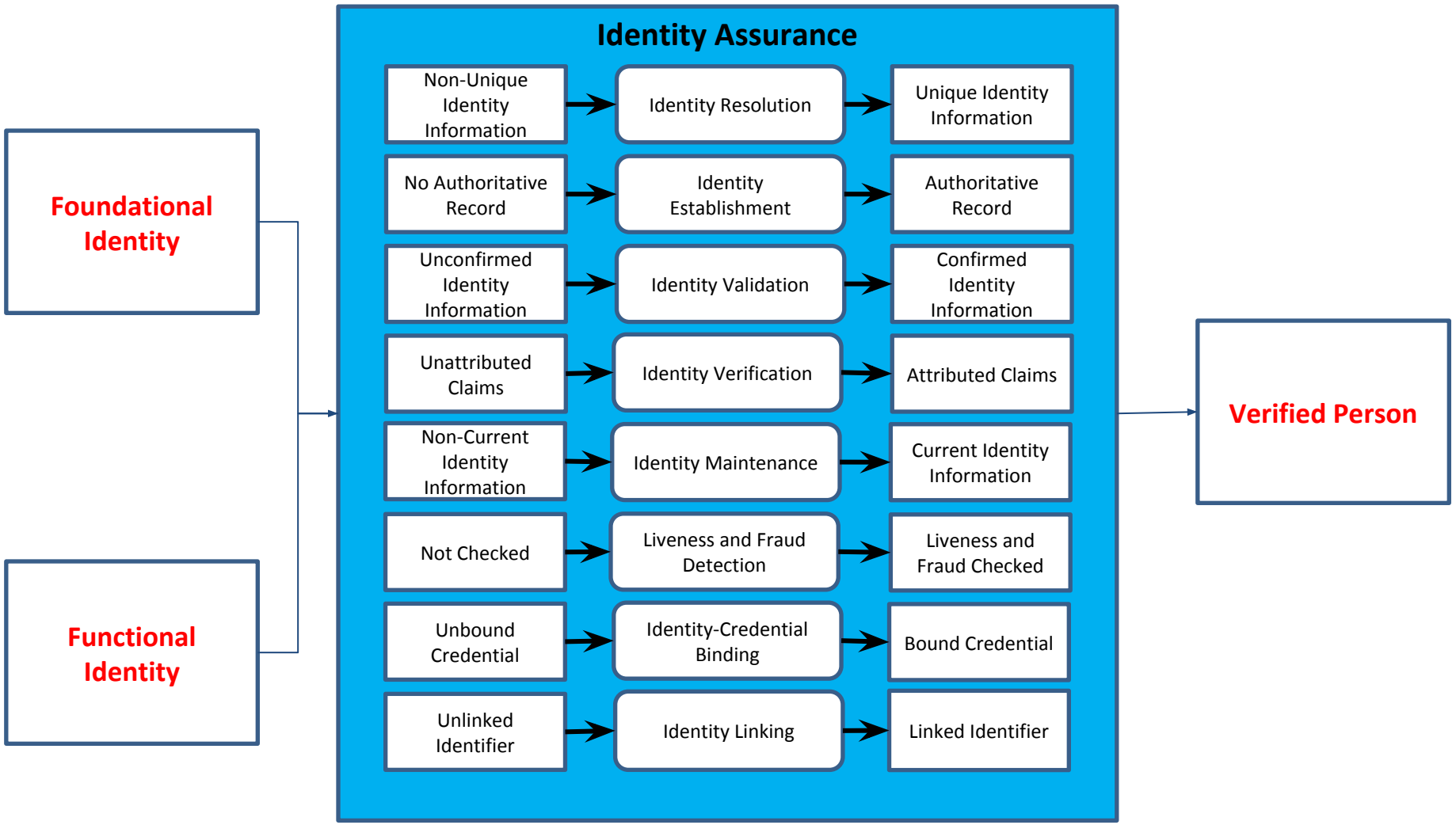


*Formalizing (and standardizing) the **trusted processes**, the **input states**, the **output states**, and the **conformance criteria**, is the essence of defining the trust framework!*

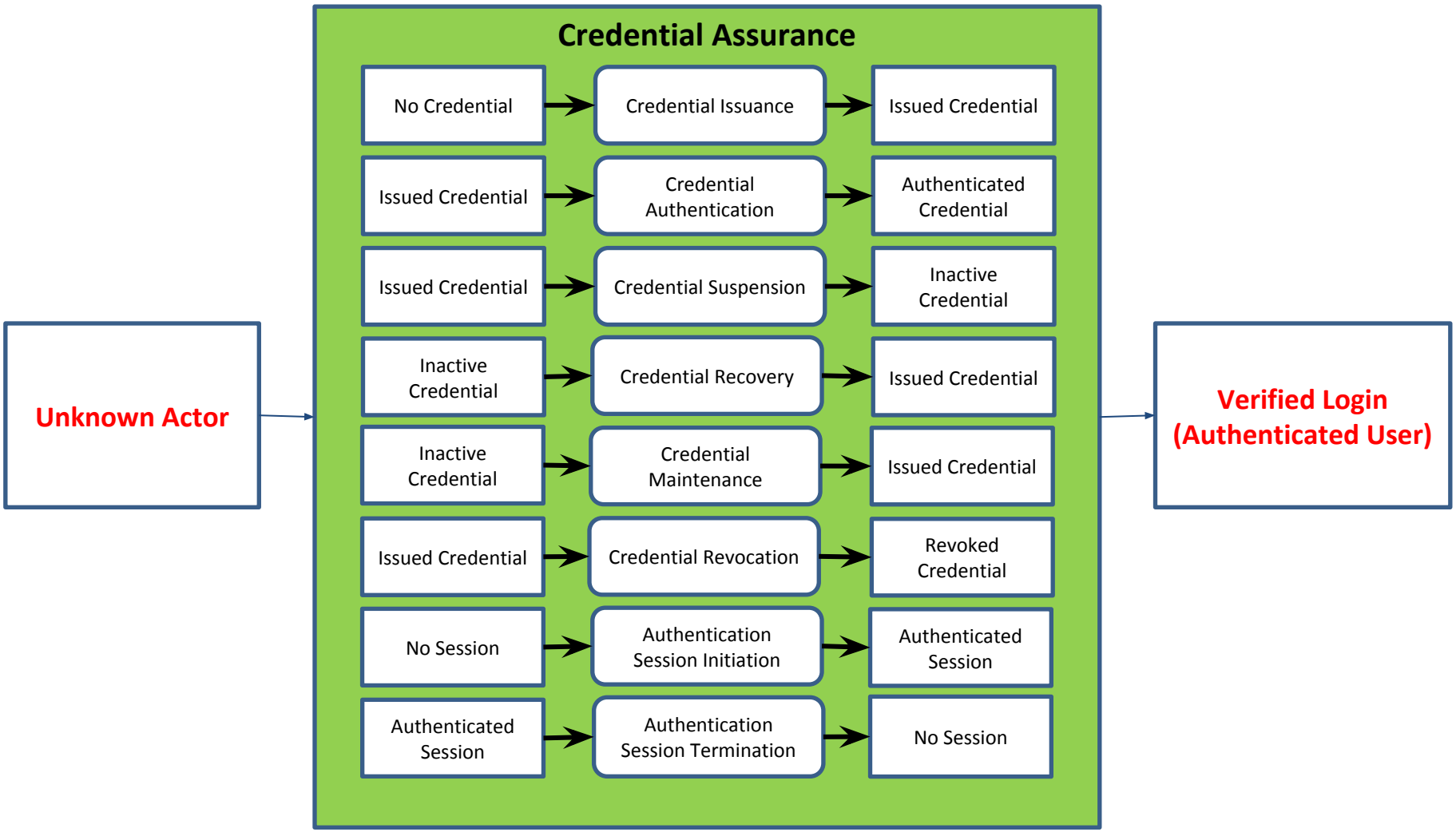
Trusted Processes (Atomic)

Identity Resolution	Credential Suspension	Identity Verification	Request Consent
Identity Establishment	Credential Recovery	Liveness and Fraud Detection	Persist Consent
Identity Validation	Credential Maintenance	Identity-Credential Binding	Consent Maintenance
Identity Maintenance	Credential Revocation	Identity Linking	Review Consent
Credential Issuance	Authentication Session Initiation	Validate Authorization for Consent	Consent Notification
Credential Authentication	Authentication Session Termination	Formulate Notification Requirements	Signature

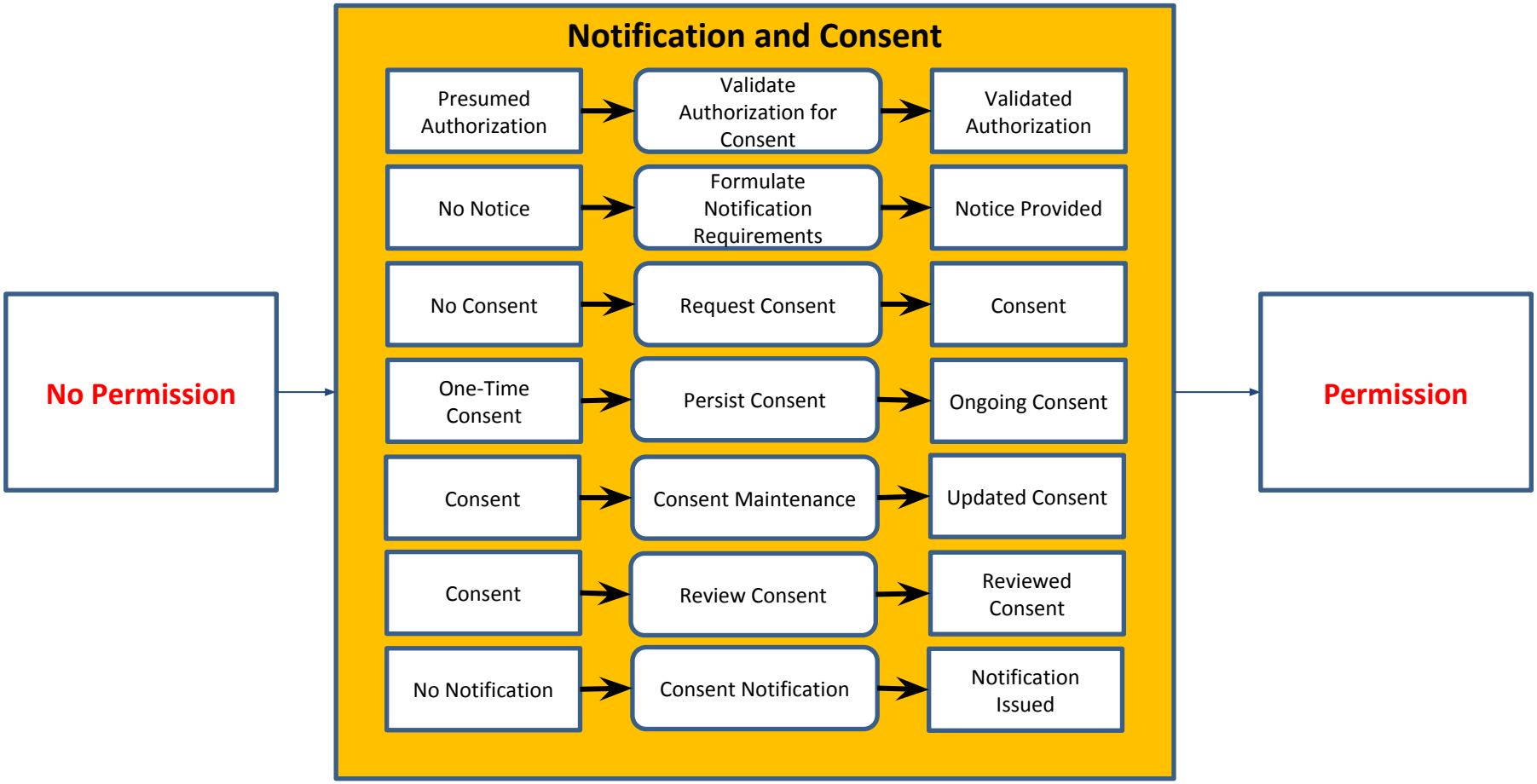
Trusted Processes (Atomic)



Trusted Processes (Atomic)

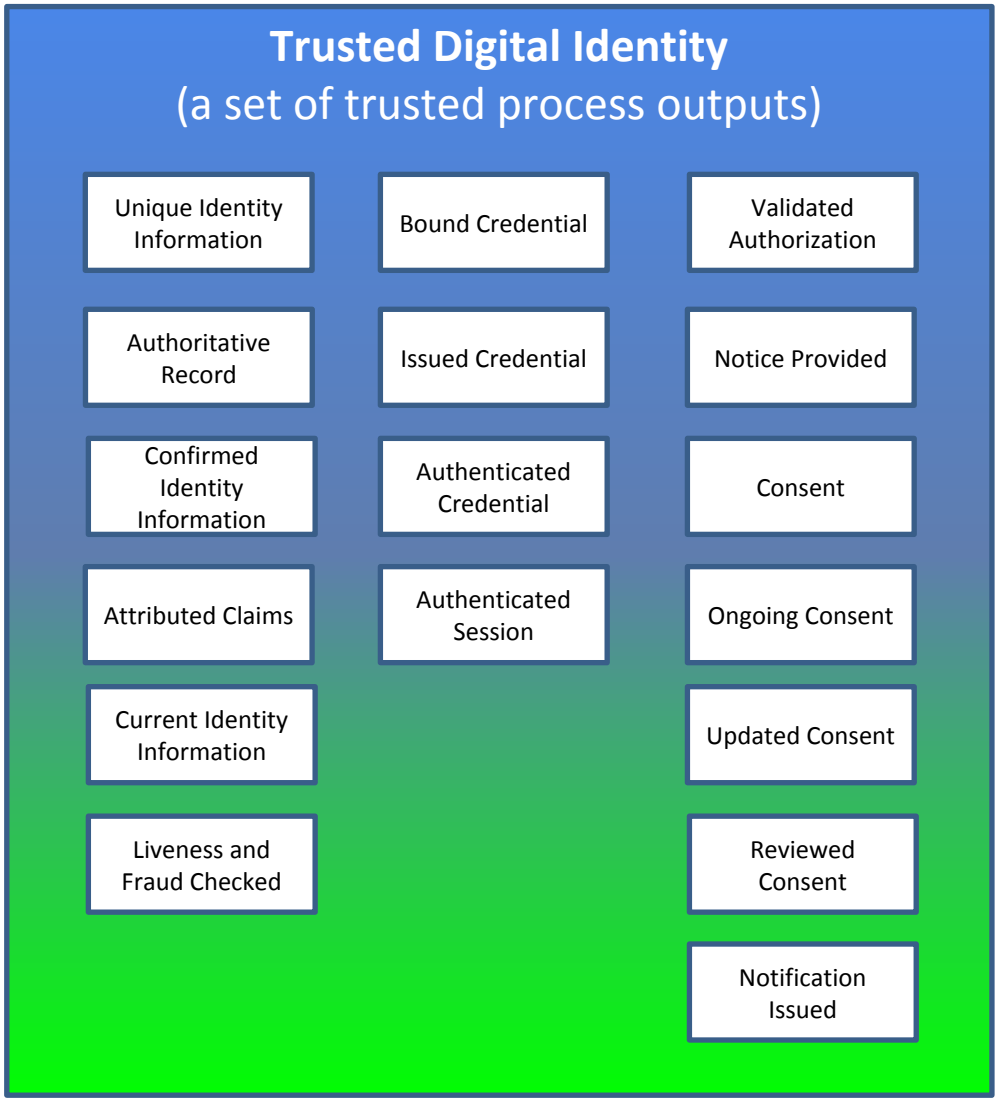


Trusted Processes (Atomic)



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

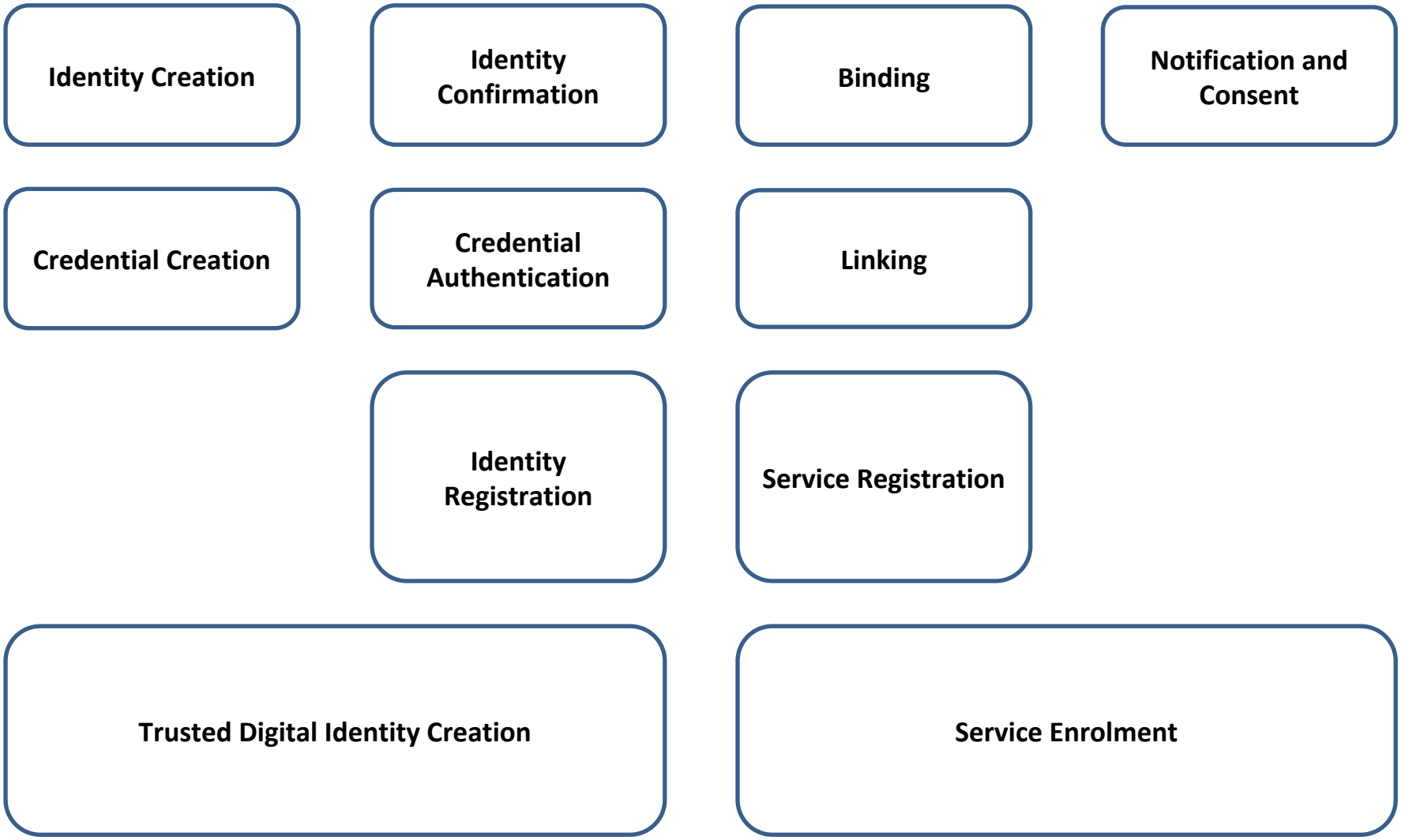
Depending on the ecosystem, some of these trusted processes may be carried out by multiple parties at different points in time .



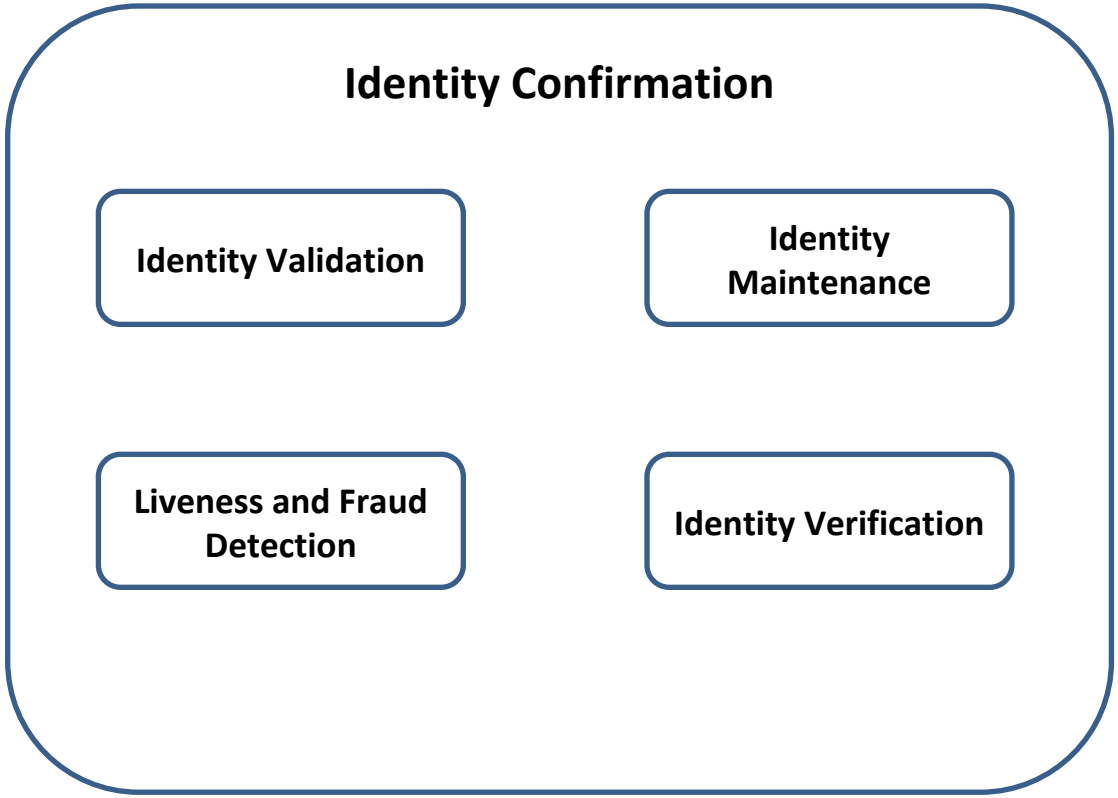
Trusted Processes can be carried out by multiple parties
(e.g., MyAlberta Digital Identity being consumed by ESDC)

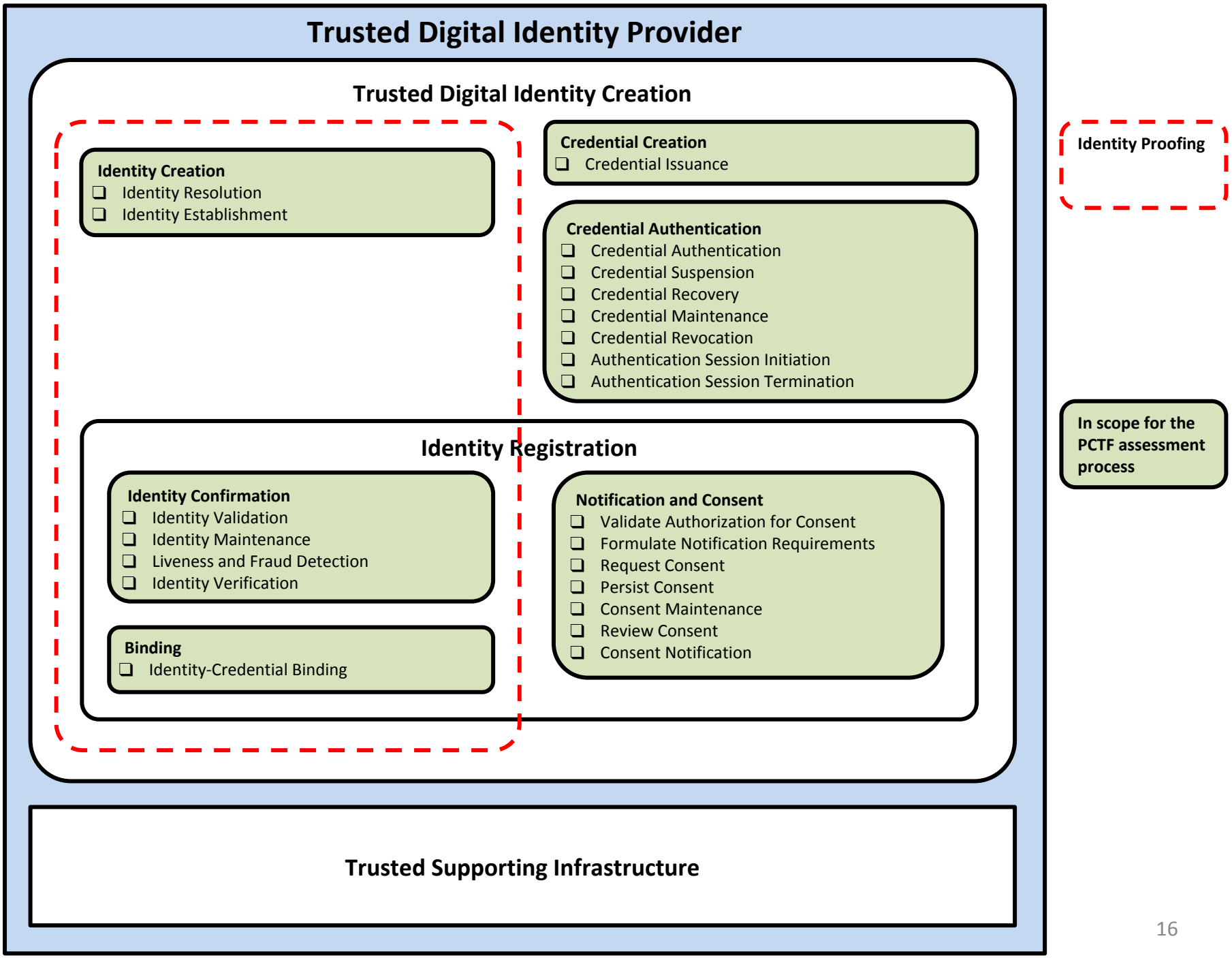
No.	Trusted Process	LOA/Vector Requirement	Trusted Digital Identity Provider	Credential Service Provider	Relying Party
1	Identity Resolution	…	MADI		ESDC
2	Identity Establishment	3	MADI		ESDC
3	Identity Validation	3	MADI		
4	Identity Verification	3	MADI		ESDC
5	Identity Maintenance	3	MADI		ESDC
6	Liveness and Fraud Detection	…	MADI		ESDC
7	Identity-Credential Binding	…	MADI		
8	Identity Linking	…			ESDC
9	Credential Issuance	2	MADI		
10	Credential Authentication	2	MADI		
11	Credential Suspension	2	MADI		
12	Credential Recovery	2	MADI		
13	Credential Maintenance	2	MADI		
14	Credential Revocation	2	MADI		
15	Authentication Session Initiation	2	MADI		
16	Authentication Session Termination	2	MADI		
17	Validate Authorization for Consent	…	MADI		ESDC
18	Formulate Notification Requirements	…	MADI		ESDC
19	Request Consent	…	MADI		ESDC
20	Persist Consent	…	MADI		ESDC
21	Consent Maintenance	…	MADI		ESDC
22	Review Consent	…	MADI		ESDC
23	Consent Notification	…	MADI		ESDC
24	Signature	…			

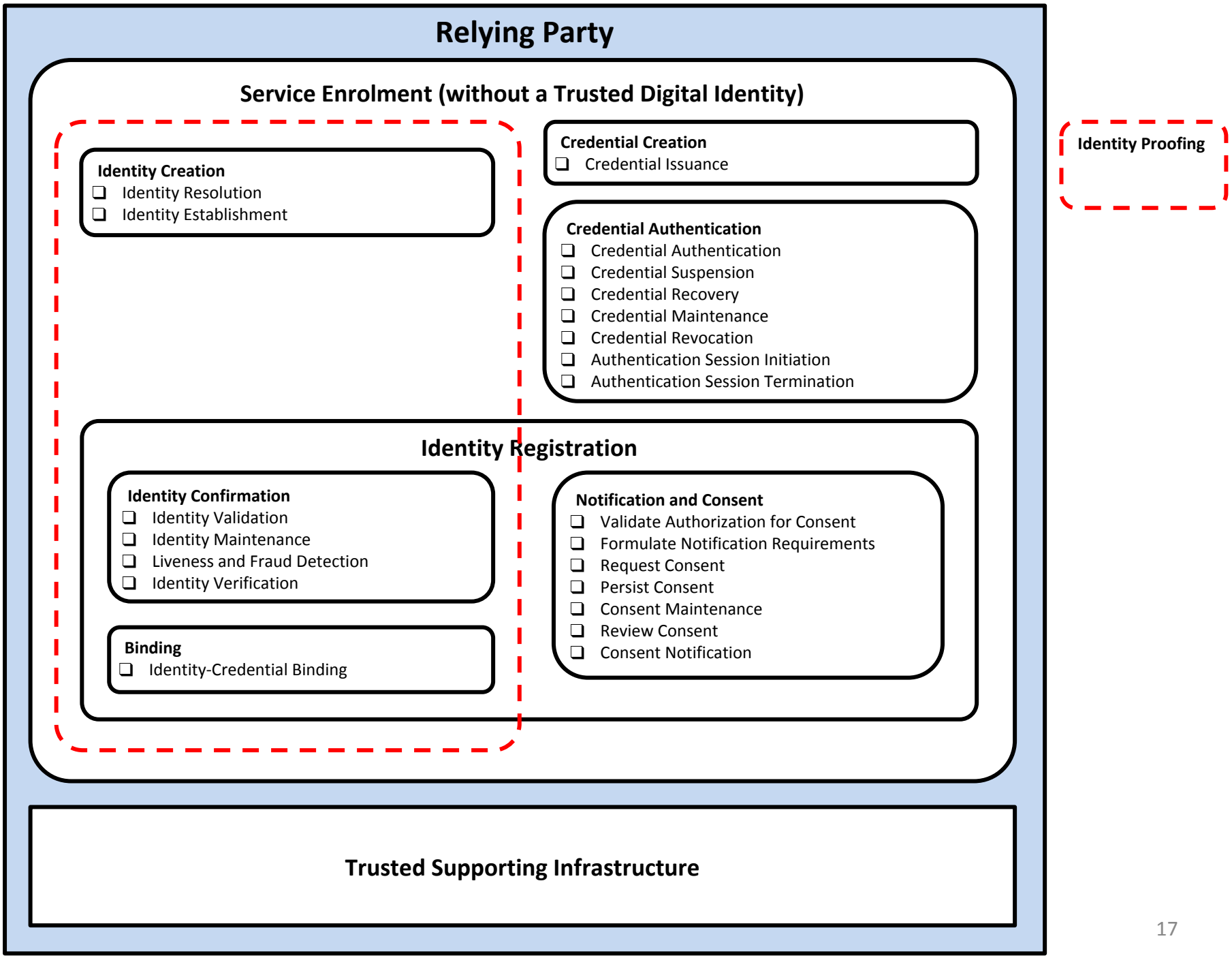
Compound Trusted Processes

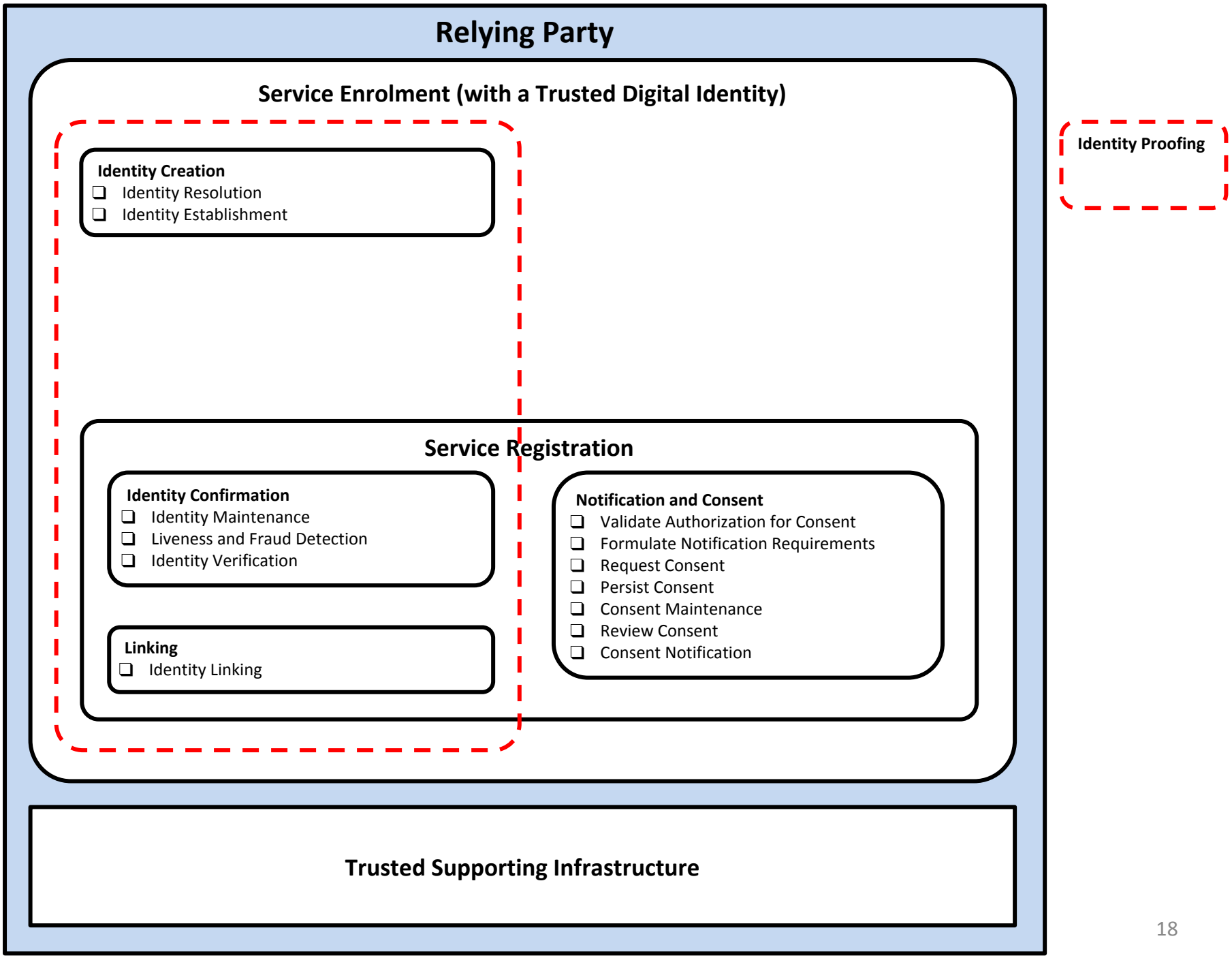


Example of a Compound Trusted Process: *Identity Confirmation*




Trusted Digital Identity Provider
Trusted Digital Identity Creation
Identity Creation
❑ Identity Resolution
❑ Identity Establishment
Credential Creation
❑ Credential Issuance
Credential Authentication
❑ Credential Authentication
❑ Credential Suspension
❑ Credential Recovery
❑ Credential Maintenance
❑ Credential Revocation
❑ Authentication Session Initiation
❑ Authentication Session Termination
Identity Registration
Identity Confirmation
❑ Identity Validation
❑ Identity Maintenance
❑ Liveness and Fraud Detection
❑ Identity Verification
Binding
❑ Identity-Credential Binding
Notification and Consent
❑ Validate Authorization for Consent
❑ Formulate Notification Requirements
❑ Request Consent
❑ Persist Consent
❑ Consent Maintenance
❑ Review Consent
❑ Consent Notification
Trusted Supporting Infrastructure
Identity Proofing
In scope for the PCTF assessment process

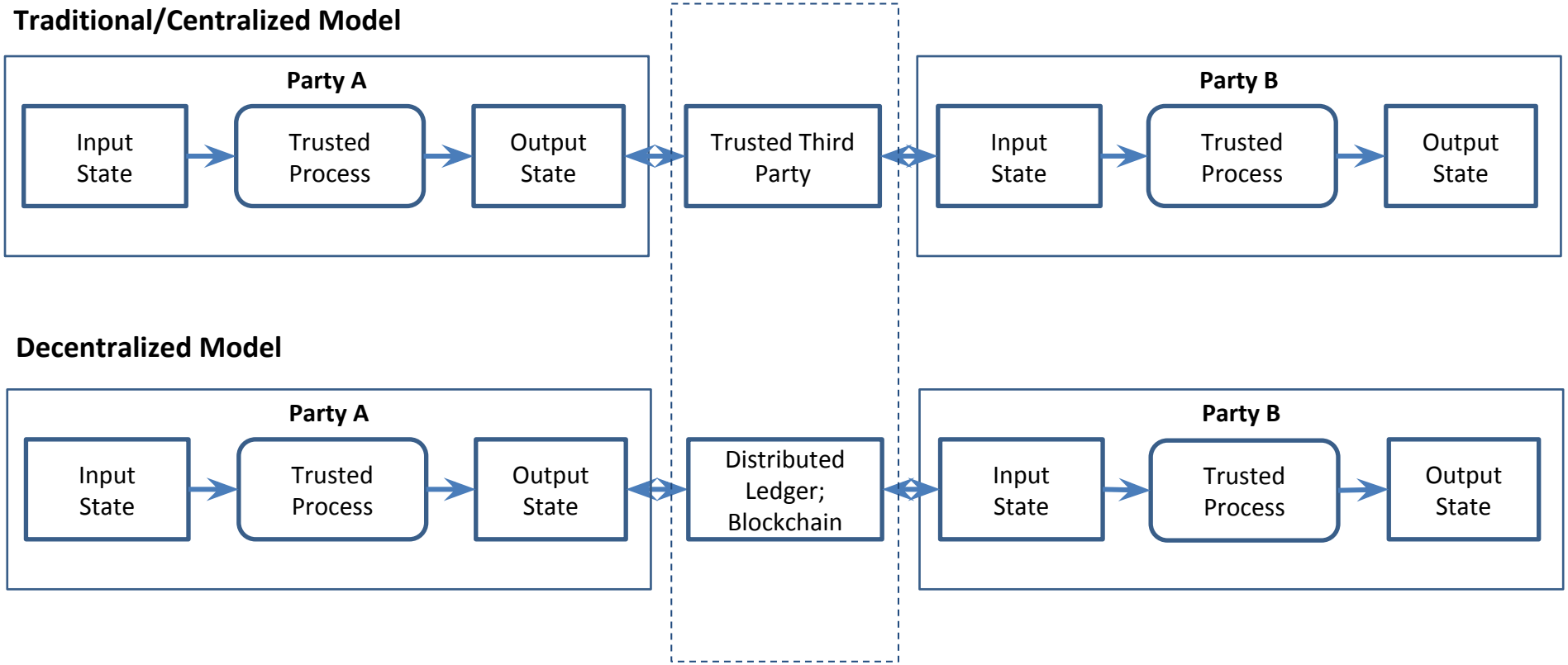

Relying Party
Service Enrolment (without a Trusted Digital Identity)
Identity Creation
Identity Resolution
Identity Establishment
Credential Creation
Credential Issuance
Credential Authentication
Credential Authentication
Credential Suspension
Credential Recovery
Credential Maintenance
Credential Revocation
Authentication Session Initiation
Authentication Session Termination
Identity Registration
Identity Confirmation
Identity Validation
Identity Maintenance
Liveness and Fraud Detection
Identity Verification
Binding
Identity-Credential Binding
Notification and Consent
Validate Authorization for Consent
Formulate Notification Requirements
Request Consent
Persist Consent
Consent Maintenance
Review Consent
Consent Notification
Trusted Supporting Infrastructure
Identity Proofing


Relying Party
Service Enrolment (with a Trusted Digital Identity)
Identity Creation
❑ Identity Resolution
❑ Identity Establishment
Service Registration
Identity Confirmation
❑ Identity Maintenance
❑ Liveness and Fraud Detection
❑ Identity Verification
Linking
❑ Identity Linking
Notification and Consent
❑ Validate Authorization for Consent
❑ Formulate Notification Requirements
❑ Request Consent
❑ Persist Consent
❑ Consent Maintenance
❑ Review Consent
❑ Consent Notification
Trusted Supporting Infrastructure
Identity Proofing

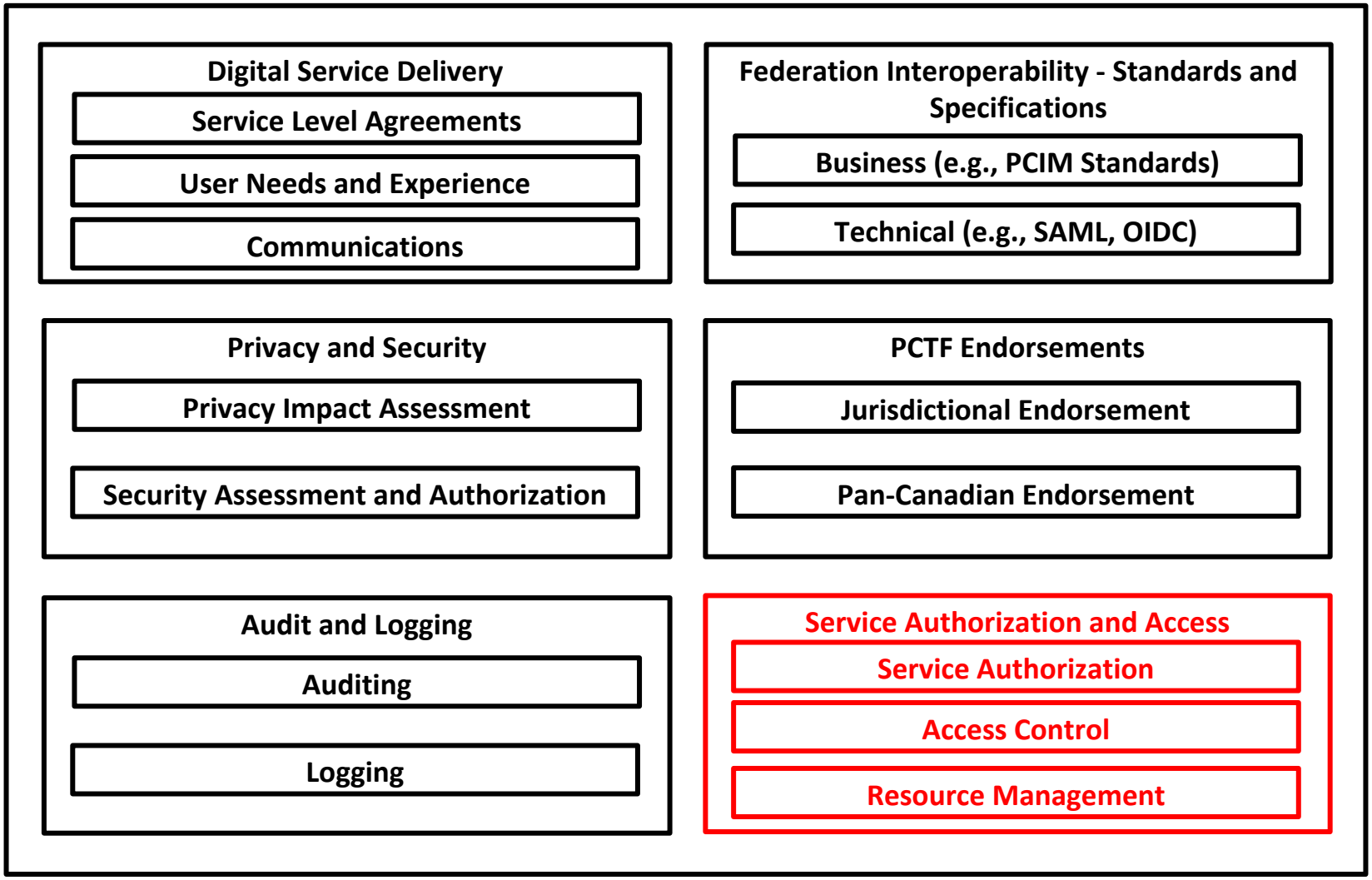
Trusted Processes and Conveyance

*Trusted process outputs (i.e., proofs) are **independent** of conveyance model. The proofs (output states) can be conveyed using a **traditional/centralized model** (e.g., a trusted third party) or a **decentralized model** (e.g., a distributed ledger, a blockchain) – or both.*

Conveying a proof from one party to another party



Trusted Supporting Infrastructure

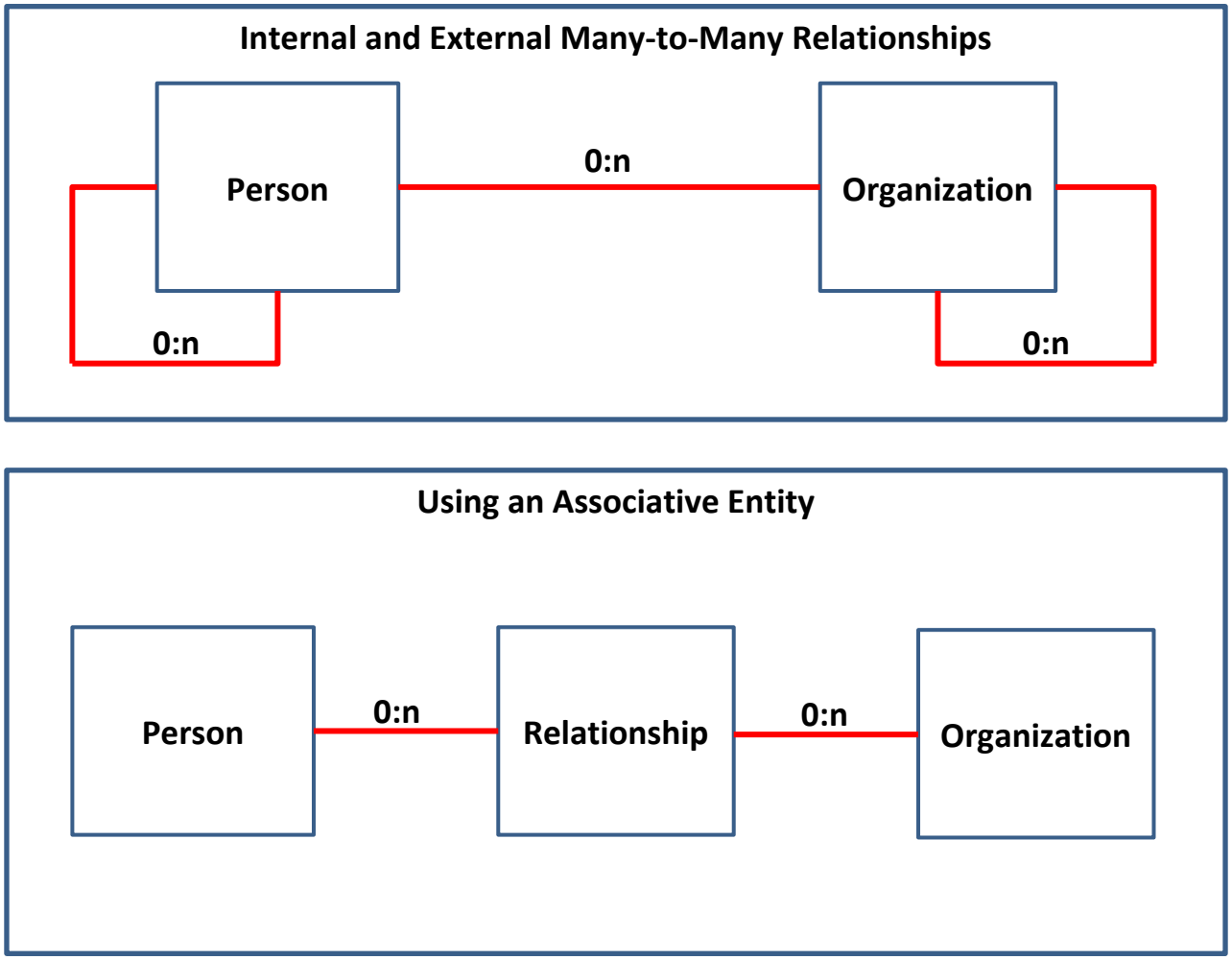


For discussion purposes only

Vectors of Trust

- A proposed IETF standard (RFC 8485, October 2018)
- Currently consists of 4 components:
  - **Identity Proofing (P)**: describes how likely it is that a given digital identity transaction corresponds to a particular, real-world identity subject
  - **Primary Credential Usage (C)**: defines how strongly the primary credential can be verified by the TDIP
  - **Primary Credential Management (M)**: conveys information about the expected lifecycle of the primary credential in use, including its binding, rotation, and revocation
  - **Assertion Presentation (A)**: defines how well the TDI can be communicated across the network without information leaking to unintended parties and without spoofing

Entities and Relationships



Government of Canada Digital Standards

A Set of Guiding Principles