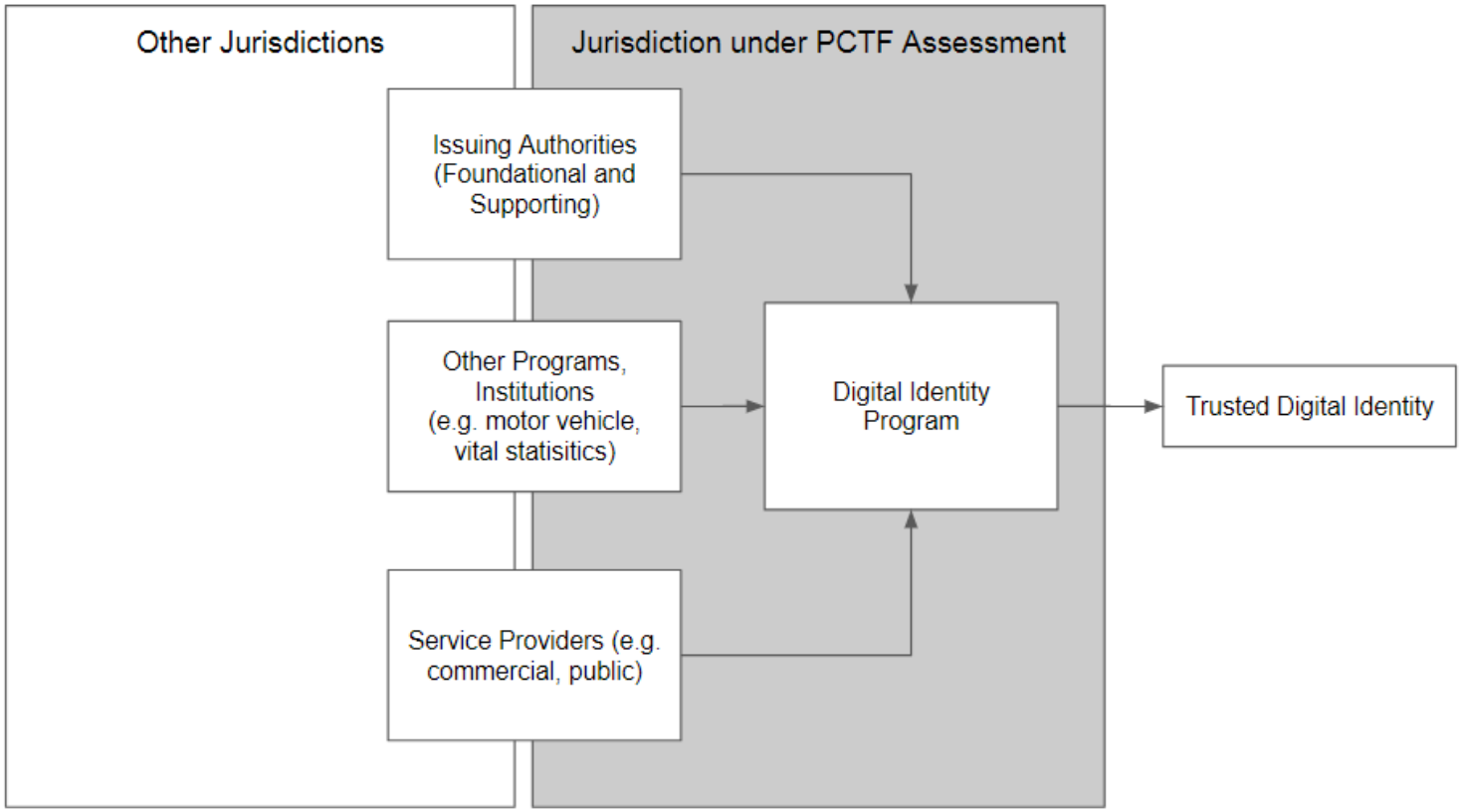
A Trusted #DigitalIdentity

I can do important stuff digitally with confidence.

PCTF Assessment Approach



FPT/PCTF Identity Provider

Trusted Digital Identity: Conformance Criteria

Credential Assurance Level

Verified Login (PCTF)

- ❑ Credential Issuance
- ❑ Authentication
- ❑ Authentication Session Initiation
- ❑ Authentication Session Termination
- ❑ Credential Suspension
- ❑ Credential Termination
- ❑ Credential Maintenance
- ❑ Credential Revocation

Identity Assurance Level

Verified Person (PCTF)

- ❑ Identity Resolution
- ❑ Identity Establishment (Foundational/Supporting)
- ❑ Identity Issuance (Foundational/Supporting)
- ❑ Identity Validation
- ❑ Identity Verification
- ❑ Identity Maintenance

Identity Registration

Confirmation and Binding

- ❑ Verified Address
- ❑ Defined Validity Period
- ❑ Verified Binding

Notice and Consent

- ❑ Authority to disclose identity/personal information
- ❑ Notice to User
- ❑ Consent from User

Privacy & Security

Assessment & Authorization

- ❑ Privacy Impact Assessment
- ❑ Security Assessment & Authorization

Digital Service Delivery

Assessment & Authorization

- ❑ Service Level Agreements
- ❑ User Needs & Experience
- ❑ Communications

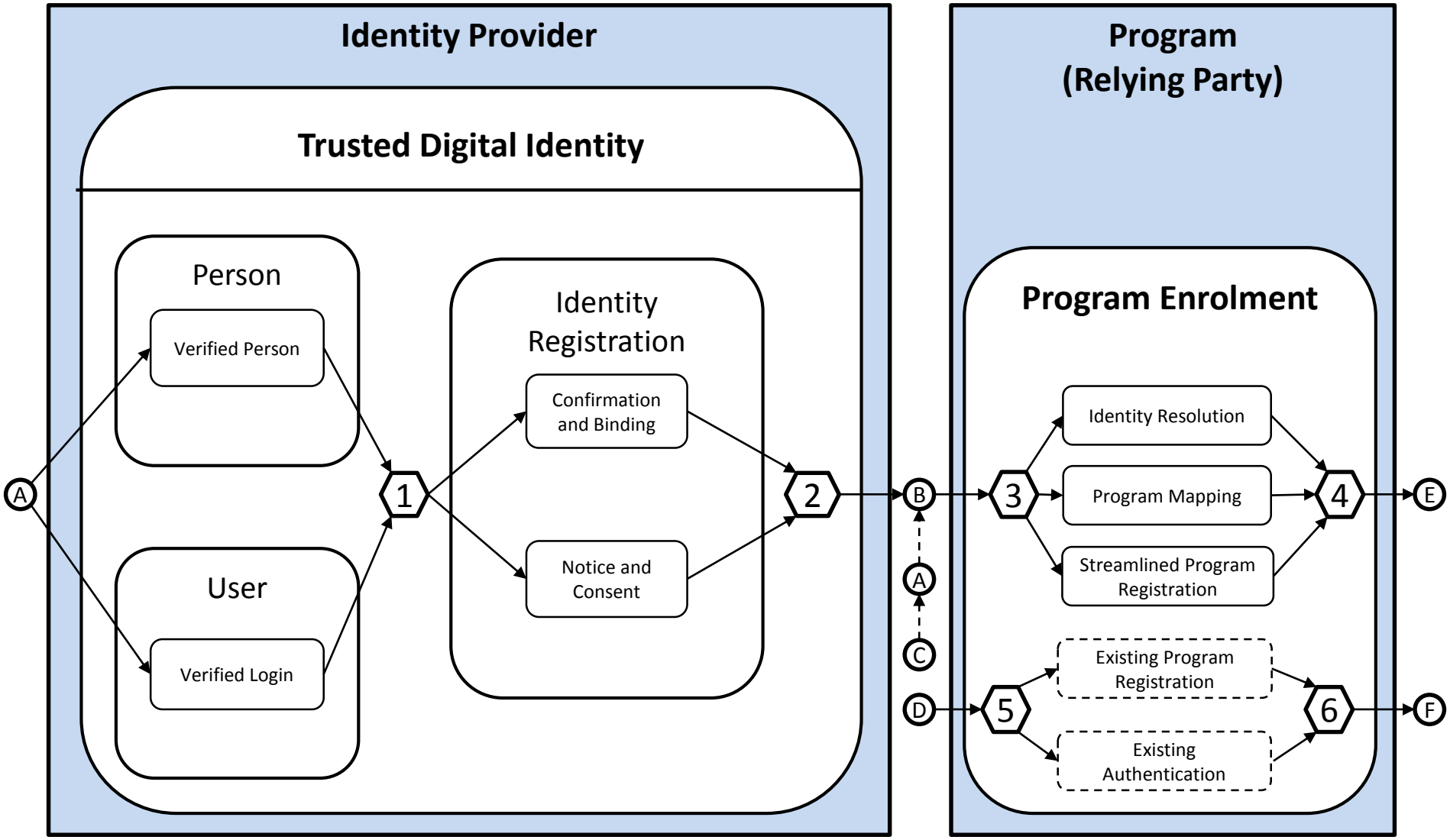
Federation / Interoperability

Standards and Specifications

- ❑ Business (Pan-Canadian IDV Standard..)
- ❑ Technical (SAML, CATS2…)

PCTF Endorsements

- ❑ Jurisdictional Endorsement (FPT-level)
- ❑ Pan-Canadian Endorsement (Joint Councils/IMSC, FPT DM Table, DIACC, etc.)

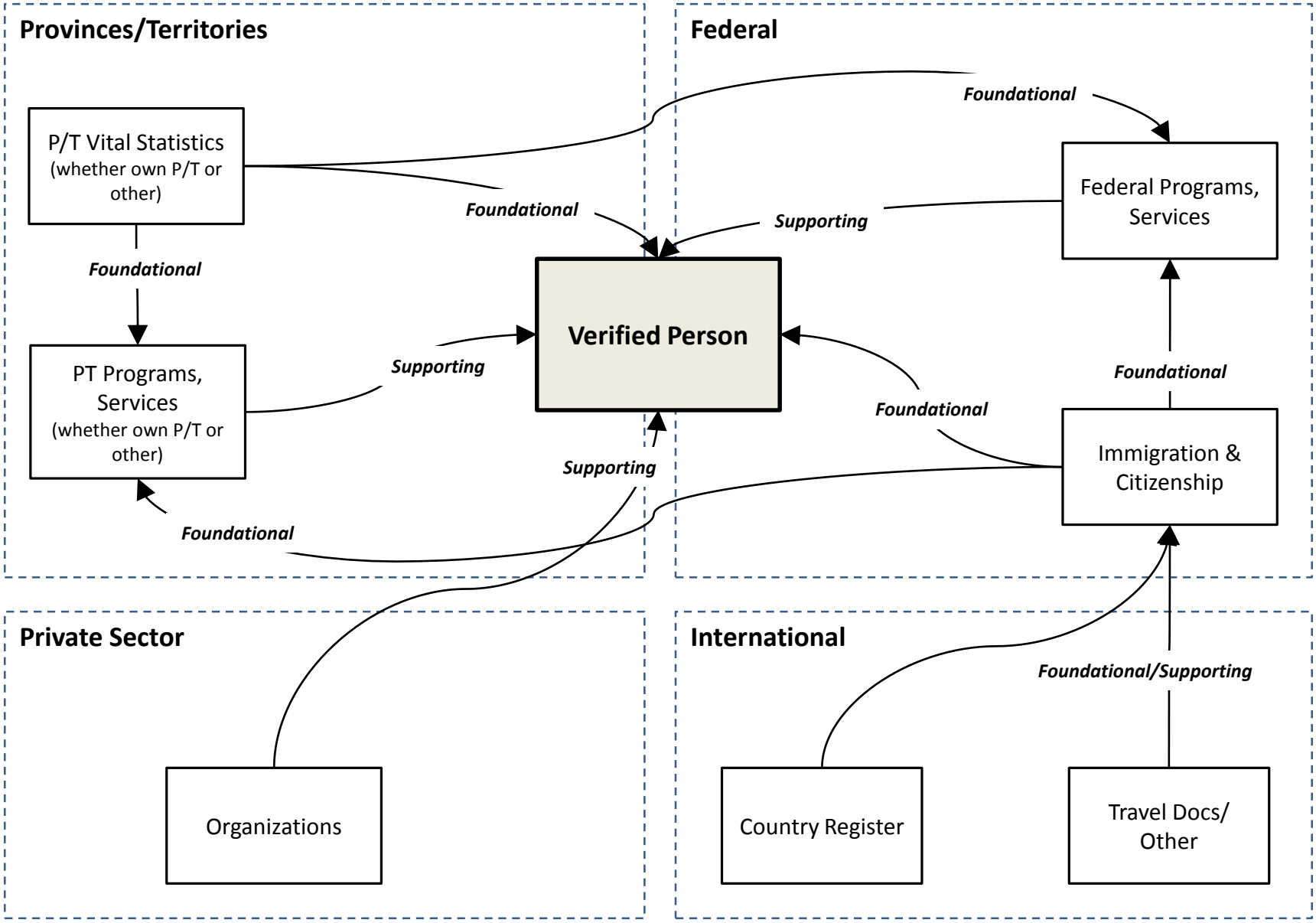


Entry/Exit States

- **A.** **Trusted Digital Identity Applicant** (not yet enroled in Program)
- **B.** **Program Applicant** using a Trusted Digital Identity
- **C.** **Program Applicant** using no Trusted Digital Identity (but intends to)
- **D.** **Program Applicant** using no Trusted Digital Identity (does not intend to)
- **E.** **Program Applicant** using a **Trusted Digital Identity**
- **F.** **Program Applicant** using no Trusted Digital Identity

Transition Criteria

1. **Verified Person** and **Verified Login** conformance criteria are met.
2. **Confirmation and Binding**, **Notice and Consent**, conformance criteria are met.
3. Program Applicant is enrolling using **Trusted Digital Identity**
4. **Identity Resolution**, **Program Mapping**, **Streamlined Program Registration** conformance criteria are met.
5. **Program Applicant** is enrolling without using Trusted Digital Identity.
6. **Program Applicant** has enroled using existing Program Registration and Authentication criteria


Provinces/Territories
Federal
P/T Vital Statistics
(whether own P/T or other)
Foundational
Foundational
Federal Programs, Services
Supporting
Foundational
Verified Person
PT Programs, Services
(whether own P/T or other)
Supporting
Foundational
Foundational
Immigration & Citizenship
Supporting
Foundational
Private Sector
International
Foundational/Supporting
Organizations
Country Register
Travel Docs/ Other

Digital Identity Cross-Border Mutual Recognition (for discussion)

US	Canada	UK	EU
IAL/AAL/FAL (SP 800 63 3)	**Trusted Digital Identity (PCTF & TB DIDM)**	**Levels of Identity Proofing (GPG-45)**	**Electronic Identification (eID)**
• **IAL**1 attributes are self-asserted • **AAL1** some assurance claimant controls authenticator registered to subscriber • **FAL1 –** permits RP to received bearer assertion signed by IDP	**Level 1:** Little confidence in the electronic representation of a person, used by that person	**Level 1** Identity is a Claimed identity with some checks that support the existence of that identity	**assurance level low** shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person,
• **IAL2** introduces need for remote for in-person identity proofing • **AAL2** provides high confidence claimant controls authenticators registered to subscriber. Proof of possession and control of two different authenticators through secure authentication protocol and approved crypto techniques. • **FAL2** adds requirement that the assertion be encrypted using approved cryptography, such that RP only party can decrypt.	**Level 2:** Some confidence in the electronic representation of a person, used by that person	**Level 2** Identity is a Claimed Identity with evidence that supports the real world existence and activity of that identity. On balance of probabilities, rightful owner of claim identity.	**assurance level substantial** shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person,
	Level 3: High confidence in the electronic representation of a person, used by that person	**Level 3** Identity is a Claimed Identity with evidence that supports real world existence and activity of that identity and physically identifies the identity to whom the identity belongs. Beyond reasonable doubt, the rightful owner	**assurance level high** shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial
• **IAL3** in-person identity proofing is required. Identifying attributes must be by an authorized representative of CSP through examination of physical documentation. • **AAL3** provides very high confidence that the claimant controls authenticator(s) registered to the subscriber. Based on proof of possession of a key through cryptographic protocol that requires a “hard” cryptographic authenticator that provides verifier impersonation resistance. • **FAL3** requires subscriber to present proof of possession of a cryptographic key in the assertion, signed using approved and encrypted using approved cryptography.	**Level 4:** Very high confidence in the electronic representation of a person, used by that person	**Level 4** identity is a Level 3 identity that is required to provide further evidence, subjected to additional, specific processes . Intended for high risk who may be in a position of trust where compromise could represent a danger to life.	