



Federated Ecosystems for Digital ID: Current Approaches and Lessons

© 2022 International Bank for Reconstruction and Development/The World Bank
1818 H Street, NW, Washington, D.C., 20433
Telephone: 202-473-1000; Internet: www.worldbank.org

Some Rights Reserved

This work is a product of the staff of The World Bank with external contributions. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Nothing herein shall constitute or be considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, or of any participating organization to which such privileges and immunities may apply, all of which are specifically reserved.

Rights and Permission



This work is available under the Creative Commons Attribution 3.0 IGO license (CC BY 3.0 IGO) <http://creativecommons.org/licenses/by/3.0/igo>. Under the Creative Commons Attribution license, you are free to copy, distribute, transmit, and adapt this work, including for commercial purposes, under the following conditions:

Attribution—Please cite the work as follows: World Bank. 2022. *Federated Ecosystems for Digital ID: Current Approaches and Lessons*, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO)

Translations—If you create a translation of this work, please add the following disclaimer along with the attribution: *This translation was not created by The World Bank and should not be considered an official World Bank translation. The World Bank shall not be liable for any content or error in this translation.*

Adaptations—If you create an adaptation of this work, please add the following disclaimer along with the attribution: *This is an adaptation of an original work by The World Bank. Views and opinions expressed in the adaptation are the sole responsibility of the author or authors of the adaptation and are not endorsed by The World Bank.*

Third Party Content—The World Bank does not necessarily own each component of the content contained within the work. The World Bank therefore does not warrant that the use of any third-party-owned individual component or part contained in the work will not infringe on the rights of those third parties. The risk of claims resulting from such infringement rests solely with you. If you wish to re-use a component of the work, it is your responsibility to determine whether permission is needed for that re-use and to obtain permission from the copyright owner. Examples of components can include, but are not limited to, tables, figures, or images.

All queries on rights and licenses should be addressed to World Bank Publications, The World Bank, 1818 H Street, NW, Washington, DC, 20433; USA; email: pubrights@worldbank.org.

Cover photo: © Shutterstock/Omelchenko

Contents

- About ID4D 3**
- Acknowledgments.....4**
- Glossary 5**
- Acronyms.....7**
- Introduction 9**
 - Background.....9
 - Purpose.....9
 - Definitions and Scope.....10
 - Structure10
- What is a Federation? 11**
 - Overview of Digital ID Ecosystem Models 11
 - Basic Components of a Federation 15
 - Identity Providers (IDPs)..... 15
 - Relying Parties (RPs)..... 18
 - Identity Exchanges, Hubs, and Brokers..... 18
 - Trust Frameworks 22
 - Approaches to Federation 23
 - Federation Type 1 - Anchored by an Existing Foundational ID and Unique Identity 23
 - Federation Type 2 - Ecosystems without a National-Level Unique Identifier 26
- When is Federation a Good Choice?28**
 - Key Features and Benefits 28
 - Risks and Challenges..... 31
 - Enablers and Preconditions 33
 - Success Factors..... 34
- Conclusion.....35**

Figures

Figure 1.1: Model Comparison	13
Figure 1.2: Key Components of a Federated Digital ID Ecosystem	15
Figure 1.3: Example of an Authentication Request Flow with Double-Blind Identity Exchange	20
Figure 1.4 Example of a Cascaded Exchange/Hub/Broker	20
Figure 1.5: Trust Framework Components	22
Figure 1.6: Using Foundational Authoritative Source (A) and Digital ID Credential (B) for Issuance of Credentials Derived by Other IDPs	25
Figure 1.7: A Federation Ecosystem with Multiple Authoritative Sources (Type 2)	27

Boxes

Box 1.1: Levels of Assurance	16
Box 1.2 Different forms of electronic ID in Norway.....	17
Box 1.3 Cross-Border Authentication Flow - Estonia and Italy - EU Electronic Identification and Trust Services (eIDAS).....	21
Box 2.1 Examples of IDP and Credential Choice	29

Tables

Table 1.1: Common Ecosystem Models for Government-Recognized Digital Identification (ID)	11
Table 1.2: Potential Functions of an Identity Exchange.....	19
Table 1.3: Examples of Federation-Type 1.....	24
Table 1.4: Examples of Federation-Type 2	26

About ID4D

The World Bank Group's Identification for Development (ID4D) Initiative harnesses global and cross-sectoral knowledge, World Bank financing instruments, and partnerships to help countries realize the transformational potential of identification (ID) systems, including civil registration (CR). The aim is to enable all people to exercise their rights and access better services and economic opportunities in line with the Sustainable Development Goals. This is especially important as countries transition to digital economies, digital governments, and digital societies, and inclusive and trusted ID systems are key to ensure the benefits are realized by all as well as for safeguarding privacy.

ID4D operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, and data protection, among others. To ensure alignment with international good practices for maximizing development benefits and minimizing risks, ID4D is guided by the 10 *Principles on Identification for Sustainable Development*, which have been jointly developed and endorsed by the World Bank Group and over 30 global and regional organizations (see <http://idprinciples.org>).

ID4D makes this happen through its three pillars of work:

1. Thought leadership, research, and analytics to generate evidence and fill knowledge gaps
2. Global public goods and convening to develop and amplify good practices, foster collaboration across regional and global stakeholders, and support knowledge exchange
3. Country and regional action through financial and technical assistance to realize inclusive and trusted ID and civil registration systems

The work of ID4D is made possible through support from the Bill & Melinda Gates Foundation, the UK Government, The French Government, The Norwegian Agency for Development Cooperation (Norad), and the Omidyar Network.

To find out more about ID4D and access our other publications, visit www.id4d.worldbank.org. id4d.worldbank.org.

Acknowledgments

This paper was prepared by Anita Mittal, under the leadership of Vyjayanti Desai as part of the World Bank's Identification for Development (ID4D) Initiative. It benefitted from reviews and feedback from Julia Clark, Adam Cooper, Marie Eichholtzer, Anna Metz, Jonathan Marskell, Chris Tullis, Emmanuel Vassor, and Faher Elfayez (Communications) of the World Bank, as well as input from Sanjay Jain of iSpirit, India; Michiel van Der Veen of the National Office for Identity Data, Netherlands; Hannes Astok of the e-Governance Academy, Estonia; Thoke Graae Magnussen of the Agency for Digitisation, Denmark; Shannon Peterson of the Digital Transformation Agency, Australia; Knut Ivarson Øvregård of the Norwegian ID Centre, Norway; the OSIA team; and the Kiva protocol team.

Glossary¹

Authoritative Source

An authoritative source of identity information is a repository or system that contains attributes about an individual and is considered to be the primary or most reliable source for this information. In the case that two or more systems have mismatched or conflicting data, the data within the authoritative data source is considered the most accurate.²

Digital Identity

A set of electronically captured and stored attributes and/or credentials that uniquely identify a person.

Digital Identification (ID)

An identification system that uses digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication. For the purposes of this paper, we use digital ID to refer to *government-recognized* forms of digital identity.

Federation Administrators

Federation administrators—also referred to as trust framework providers or trust framework operators—are responsible for the governance of an ID federation. They are organizations, often set up by their constituent members, to administer the activities associated with operating an identity federation.³

Federated ID Ecosystem

As used in this paper, a federated ecosystem consists of multiple identity providers (IDPs) and relying parties (RPs) that operate under a federation trust framework to provide and use digital identity services. More broadly speaking, federation in general is a process that allows for the conveyance of authentication attributes and identity attributes across networked systems.

Federation Protocol

A protocol that allows for trusted and secure communication between IDPs and RPs across an open network by exchanging digital certificates (cryptographic techniques) to ensure the authenticity, integrity, and confidentiality of the data exchange (identity assertion). Examples include Security Assertion Markup Language (SAML) and OpenID Connect (OIDC).

1 Glossary definitions are derived from the *ID4D Practitioner's Guide* unless otherwise noted. See World Bank. 2019. "ID4D Practitioner's Guide." Washington, DC: World Bank. <http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide>.

2 United States Federal Identity Credential and Access Management (FICAM). n.d. "Streamline Identity Management Playbook." https://bnbuckler.github.io/ficam-identity/2_step-2/.

3 Adapted from Temoshok, David, and Christine Abruzzi. 2018. National Institute of Standards and Technology Internal/Interagency Report (NISTIR) 8149: "Developing Trust Frameworks to Support Identity Federations." Available at <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8149.pdf>.

Identity Assertion

A statement from an identity provider to a relying party that contains information about a user. Assertions may also contain verified attributes.⁴

Identity Exchange

An identity exchange—also known as a hub or broker—coordinates the flow of information between participants in a federation. Functional capabilities of the exchange may include identity provider (IDP) selection, blinding participants from each other, and user consent processes, among others.

Identity Provider (IDP)

An entity that registers users, performs identity proofing, manages credentials, authenticates users, and asserts user authentication status to relying parties.

Relying Party (RP)

An entity—generally a government agency or private firm—such as digital government services, banks, or healthcare providers, that relies on the credentials and authentication mechanisms provided by an identity provider (IDP), typically to process a transaction or grant access to information or a system.

User

Users are people who obtain digital identity credentials from identity providers (IDPs) and use these to access services provided by relying parties (RPs).

Trust Framework

Trust frameworks are the basis for the multilateral agreements that enable the trust and governance of a federation's operations among all of the federation's members. A trust framework stipulates adherence to agreed-upon standards, formalizes assessment processes, and defines the roles and responsibilities within multi-party arrangements.⁵

4 Grassi, P., Garcia, M., and Fenton, J., 2017. NIST Special Publication 800-63-3: "Digital Identity Guidelines." Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>

5 Temoshok, David, and Christine Abruzzi. 2018. NISTIR 8149: "Developing Trust Frameworks to Support Identity Federations." <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8149.pdf>.

Acronyms

AAL	Authentication assurance level
AS	Authoritative source
ATO	Australian Taxation Office
CDD	Customer due diligence
CIE	Carta d'identità elettronica (Italy)
CNS	Carta nazionale dei servizi (Italy)
CPR	Central Person Register (Denmark)
CR	Civil registration
CSAM	Government Gateway (Belgium)
DLT	Distributed ledger technology
eIDAS	Electronic Identification and Trust Services (EU Regulation no. 910/2014)
EU	European Union
FAL	Federation assurance level
FAS	Federal Authentication Service (Belgium)
FICAM	Federal Identity Credential and Access Management (US)
HIC	High-income country
IAL	Identity assurance level
IDP	Identity provider
KYC	Know-your-customer
LOA	Level of assurance
MNO	Mobile network operator

MOU	Memorandum of understanding
NID	National ID
NIN	National identification number
NIST	National Institute of Standards and Technology (US)
OAUTH	Open authorization
OIDC	OpenID Connect
OTP	One-time password
PBD	Privacy-by-design
PKI	Public key infrastructure
QSCD	Qualified electronic signature creation device
RIA	Republic of Estonia Information System Authority
RP	Relying party
SAML	Security assertion markup language
SIM	Subscriber identity module
SLA	Service level agreement
SPID	Sistema Pubblico di Identità Digitale (Italy)
SSI	Self-sovereign identity
SSO	Single sign-on
TARA	State Authentication Service (Riigi autentimisteenus or TARA) of Estonia
TDIF	Trusted Digital Identity Framework (Australia)

Introduction

Background

Online access to government services, such as applying for benefits, filing taxes, or registering property, typically require secure mechanisms to remotely authenticate and verify a person’s legal identity. Similarly, a variety of private sector services, including opening bank accounts or managing health records, require higher levels of assurance in a person’s identity and credentials. To provide these identification or authentication mechanisms, countries have adopted a variety of models to translate legal or official identification (ID) into forms of “digital ID.”

In some cases, the initial architecture to offer these digital credentials involves service providers themselves performing the role of identity provider, issuing their own “functional” digital IDs to their users. In others, countries have developed a primary digital identity provider—typically the same government agency that has managed traditional forms of identification, for example, a civil registration, a national population register, or national ID authority—to facilitate verification or authentication of official identity to various relying parties. More recently, new models are emerging that involve multiple identity providers (IDPs) that provide government-recognized digital ID for online transactions to relying parties or service providers in a federation, according to an established trust framework.

Such federated digital ID ecosystems have been implemented at the national level in multiple countries in Europe— for example, Norway, Denmark, Belgium, France, the United Kingdom, and Estonia—and in others such as Australia, Thailand, and Uruguay. At the regional level, the European Union developed the Electronic Identification, Authentication, and Trust Services (eIDAS) federation to enable mutual recognition of member countries’ digital IDs across borders.

Purpose

This paper provides a primer on federated digital ID ecosystems for practitioners, development partners, and others involved in the digital ID and development space. It gives an overview of the basic types and components of a digital ID federation, as well as its specific benefits and risks based on established standards and experiences across a variety of countries. Given that most implementations of federation come from high-income countries (HICs), this paper also endeavors to translate these experiences and their limitations into the context of lower- and middle-income countries.

This paper should help governments and ID practitioners answer the following questions:

- What is a federated ecosystem and how is it different from other models of providing digital ID?
- What are the important factors to consider when evaluating if a federated ecosystem is an appropriate choice for a particular context?
- What are the basic ingredients for implementing a federated ecosystem?

Like other models of digital ID, there is no “one-size-fits-all” approach. The goal of this paper is therefore to introduce federation for those new to the approach but does not necessarily prescribe this model. The overall approach to digital ID selected by individual countries should be based on a thorough analysis of the existing identification system ecosystem and market.

Definitions and Scope

As used in this paper, federation digital ID ecosystems (henceforth referred to as “federations”) involve multiple public and/or private-sector identity providers (IDPs) that provide official digital identity services to relying parties (RPs). They operate under an explicit federation trust framework and typically implement a federation hub or exchange to facilitate communication between IDPs and RPs.⁶

The focus of this paper is on federations that provide digital ID⁷ credentials and services *recognized by governments for official purposes*, in other words, accessing government services, and may also be accepted or required for certain services in the private sector that require higher levels of assurance—for example, the opening of a bank account. Other forms of digital ID and federation provided and used only by private sector entities—such as using Facebook, Amazon, or Google accounts to log-in to other websites or services on the internet via federation protocols—are not considered here.

Notably, new models of decentralized digital ID, including through verifiable credentials and e-wallets, are gaining momentum and work to complement and supplement single IDP and federated architectures. While the following section briefly discusses these models in relation to federation, detailed discussion on decentralized systems is outside the scope of this paper and will be addressed in future work.

Structure

Section 1.1: Basic Components of a Federation, gives a brief overview of federation and how it differs from other models, while Section 1.2: Approaches to Federation outlines key features, risks, and challenges of federation, along with enablers and common success factors. Finally, Section 2: When is Federation a Good Choice? describes the various components of a federation in more detail. With this information, we hope countries and practitioners will have a solid foundation for considering the relative merits and appropriateness of federated ecosystems for digital ID.

⁶ This paper therefore uses the term federation to refer to a *narrower category of ecosystem-wide models* than the definition of a federation adopted in some standards. National Institute of Standards and Technology (NIST) Special Publication 800-63-3, for example, defines federation generally as “a process that allows the conveyance of identity and authentication information across a set of networked systems.” Under this broad definition, a single IDP—such as a national ID agency—that provides authentication services to multiple entities (relying parties, or RPs) could be considered a federation. However, for models of government-recognized digital ID, federation has come to refer to a specific type of ecosystem, where multiple IDPs and RPs develop a shared trust framework and hub to facilitate identity services. This is the type of model referred to as “federation” in this paper. See Grassi, P., Garcia, M., and Fenton, J., 2017. NIST Special Publication 800-63-3: “Digital Identity Guidelines,” p. 46. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>

⁷ In general terms, “digital ID systems” are those that use digital technologies throughout the identity lifecycle, including for enrollment, data management, credential issuance, and identity verification and authentication (see *ID4D Practitioner’s Guide*, <http://id4d.worldbank.org/guide>). While a digital ID system enables remote authentication of the individual (for example, to access online services), digital authentication and verification could also be used for in-person service delivery. However, federated ecosystems have primarily been designed to provide digital ID for online, web-based services, which are the focus of this paper. Note that throughout this paper, the term “digital ID” refers only to government-recognized digital ID.

What is a Federation?

Overview of Digital ID Ecosystem Models

Countries have developed government-recognized digital ID through different models that typically evolve over time, and federation is only one approach. Any digital ecosystem is comprised of the following general roles and components:

- **Identity providers (IDPs)** are entities that register users, perform identity proofing, manage credentials, authenticate users, and assert authentication status to relying parties.
- **Relying parties (RPs)** are entities such as digital government services or other entities, such as banks, healthcare providers, and telecom operators, that rely on the credentials and authentication mechanisms provided by an IDP, typically to process a transaction or grant access to information or a system.
- **Users**—also sometimes called ID “owners,” “subscribers,” or “data subjects”—are people who obtain digital identity credentials from IDPs and use these to access services provided by RPs.
- **Authoritative sources** are entities that hold attributes about a user and are considered the primary or most reliable source for this information, such as a civil register for birth dates, or a school to provide confirmation of graduation.
- **Trust frameworks** are the shared rules governing participants within the ecosystem.

Ecosystems generally evolve over time to meet new needs and incorporate new technologies, and each country is unique. Still, existing digital ID ecosystems can be generally classified in terms of (a) the number of IDPs that provide digital identity credentials and services; (b) the relationship and flow of information between IDPs, RPs, and individual users; (c) and how this relationship is governed and technically implemented (table 1.1).

Table 1.1: Common Ecosystem Models for Government-Recognized Digital Identification (ID)

	“Functional” ID	Single IDP	IDP Market	Federation	Decentralized
Description	Each relying party provides and manages its own ID	A single identity provider (IDP), often the foundational ID agency, serves multiple relying parties (RPs)	Multiple IDPs serve different RPs but are not coordinated	Multiple IDPs and RPs enter into an explicit trust framework	Credentials issued by IDPs or authoritative sources are managed by individual users
Number of IDPs	–	One	Multiple	Multiple	Multiple

	“Functional” ID	Single IDP	IDP Market	Federation	Decentralized
Relationship between IDPs and RPs	RP = IDP	One IDP used by all RPs	RPs and IDPs enter into bilateral arrangements	RP-IDP relationship and communication managed by federation exchange and trust framework	Linked via verifiable data registry
Identity Verification	Centralized in RP/IDP	IDP	IDP	Identity exchange forwards to RP from IDP	User
Assertion	US IRS PIN number (tax ID), bank ID, digital drivers’ license, etc.	India, Singapore, and European eID schemes, except those listed as federations, etc.	In the US: various services, such as Id.me	Nordic countries, Belgium, France, the UK, Estonia, Italy, Australia, Thailand, and Uruguay; EU Electronic Identification and Trust Services (eIDAS) 1.0 (cross-border)	EU Digital Identity Wallet (planned), ⁸ Kiva Protocol (small scale implementation)

Source: World Bank.

Table 1.1 and figure 1.1 provide a general categorization of common ecosystem models along these dimensions, including:

- **“Functional” IDPs:** Each government entity (or private sector service provider) issues its own digital ID credentials, which are used only to access its own services. Essentially, this means that each RP is its own IDP, and the identity management system is a subcomponent of other systems that provide services to the public. People cannot use the digital ID issued by one entity—for example, a credential issued by the tax administration to file tax returns online—to access services from another entity, such as an online application for a passport, which means that they must manage multiple credentials and log-ins.⁹
- **Single IDP:** Rather than issuing their own credentials, government (and potentially private sector) RPs rely on the digital ID provided by a single IDP. Oftentimes, this has been the country’s foundational ID system—for example, a civil registration or national ID system. The IDP-RP relationship may involve an implicit or explicit trust framework, such as a memorandum of understanding (MOU) and/or service level agreement (SLA), in which the IDP provides one or multiple options for authentication with different levels of assurance.
- **IDP Market:** In contrast to the single IDP model, some countries have multiple (typically two to three) IDPs issuing digital credentials that are used by various government and/or private sector RPs but are not governed or regulated under a comprehensive federation. In this case, IDPs and RPs enter into bilateral or ad hoc arrangements for identity services, where RPs choose one or more IDPs that meet their business needs. Users have a choice only if the RP they are interacting with has an agreement with multiple IDPs.
- **Federation:** Some countries have developed a trust framework to regulate and facilitate relationships between multiple IDPs and RPs. This includes an identity hub or exchange, or

⁸ Technical specifications for large-scale pilots of the EU Digital Identity Wallet will be published in October 2022.

⁹ Under some definitions, this is referred to as a “centralized” system; however, “centralized” is also used in some cases to refer to single IDP systems (i.e., where there is one centralized ID providing authentication services across applications) and/or to the technical architecture where identity assertions and verification is done by pinging the central server, rather than via decentralized credentials. To avoid this confusion, this paper uses the term “functional ID” to refer to cases in which RPs issue and manage their own IDs.

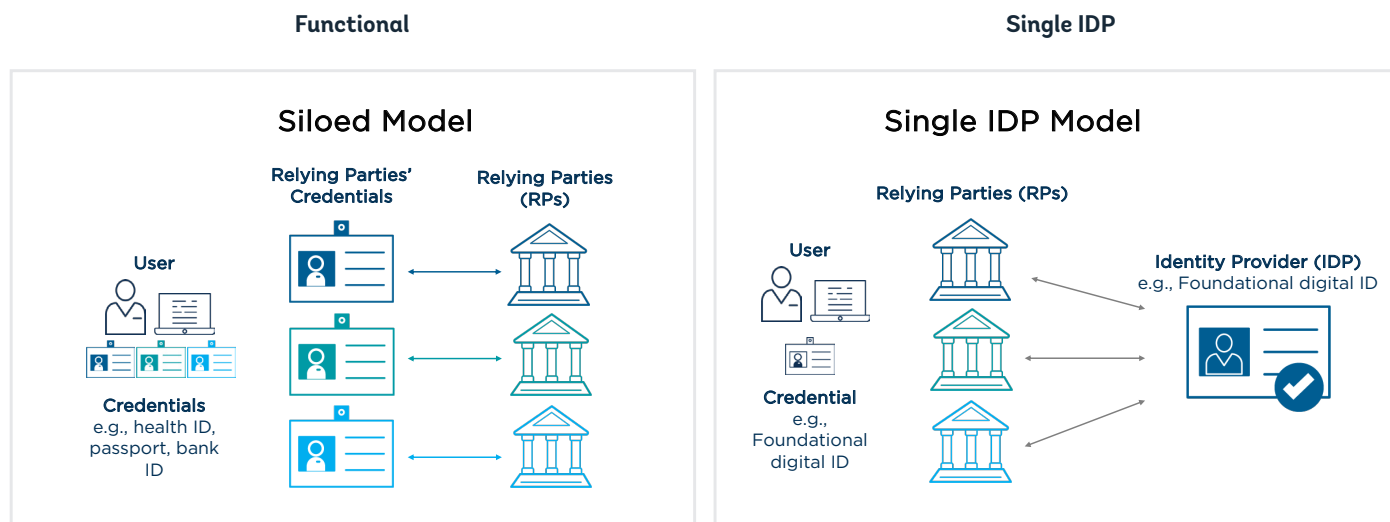
broker, that facilitates identity services among participating organizations—sometimes referred to as a “hub-and-spoke” model. This hub enables additional IDPs and RPs to be added to the federation seamlessly, and users can typically choose among the multiple IDPs for establishing their identity when accessing a service provided by the RP.

- **Decentralized:** In a decentralized model—sometimes known as “self-managed” or referred to as a “self-sovereign” identity (SSI)—various IDPs or other authoritative sources¹⁰ issue digitally verifiable credentials that are stored locally by the user, for example, in a digital wallet on a smartphone or smartcard. To authenticate or verify these credentials, the holder presents them directly to an RP, who verifies the identity and authenticity, as well as the integrity of the presented attributes through a verifiable data registry, which can be implemented using distributed ledger technology (DLT) such as blockchain, or trust lists and registries, without interacting directly with the issuer.¹¹ This model is in the nascent stages for government-recognized digital ID, but the recent adoption of the EU framework for digital wallets is likely to accelerate its growth.

If a country has a limited number of IDPs, it may be a manageable option to establish bilateral agreements with a handful of RPs in order to define their roles and responsibilities (as is the case with the single IDP and IDP market models described above). However, in most whole-of-government digital service architectures, there are typically many IDPs and RPs; users require a consistent experience, and economies of scale point toward digital identity that can be used with multiple services in the public, and in many cases, the private sector, for example: including single sign-on (SSO) e-government portals, and other “joined-up” services. For this reason, a growing number of countries have opted to create comprehensive trust frameworks to establish and govern federations that provide official digital ID services.

The remainder of this paper focuses on this specific model of a federated digital ID ecosystem, though other models will be referenced for contrast.

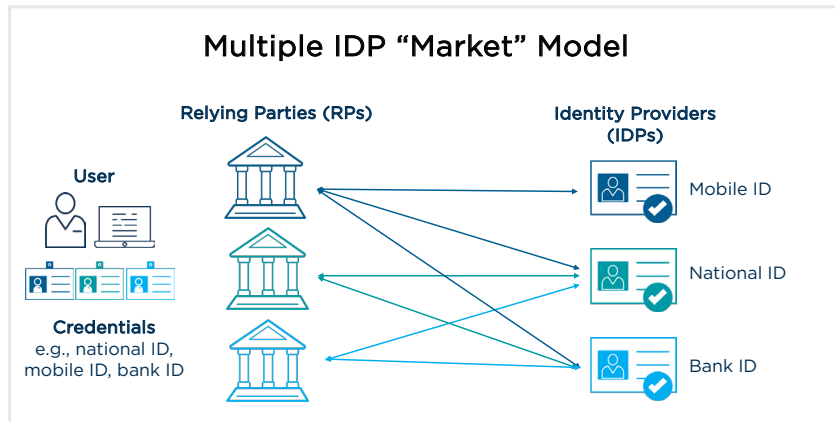
Figure 1.1: Model Comparison



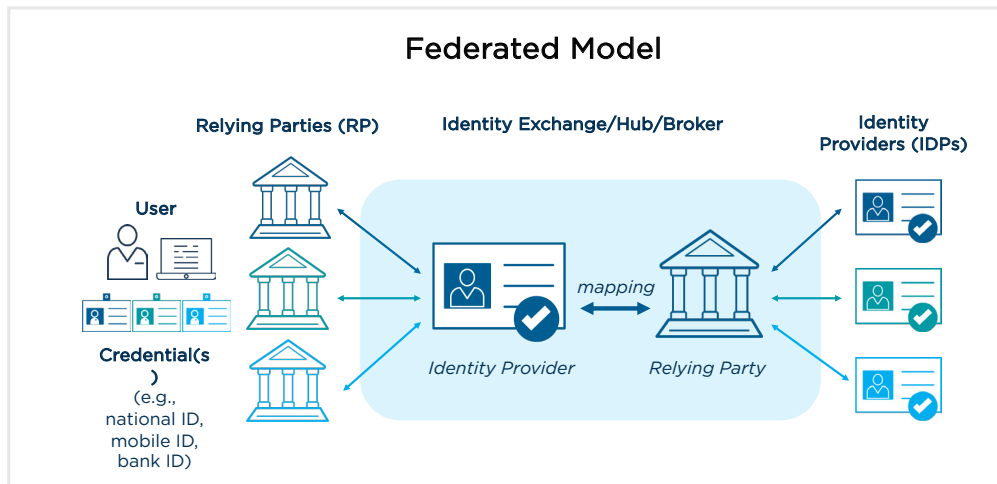
10 An authoritative source of identity information is a repository or system that contains attributes about an individual that are considered to be the primary or most reliable source for this information. In the case that two or more systems are mismatched or have conflicting data, the data within the authoritative data source is considered the most accurate. Adapted from: FICAM. n.d. “Streamline Identity Management Playbook.” United States Federal Identity, Credential, and Access Management. https://bnbuckler.github.io/ficam-identity/2_step-2/.

11 For example, see Manning, “The Basic Building Blocks of SSI.”

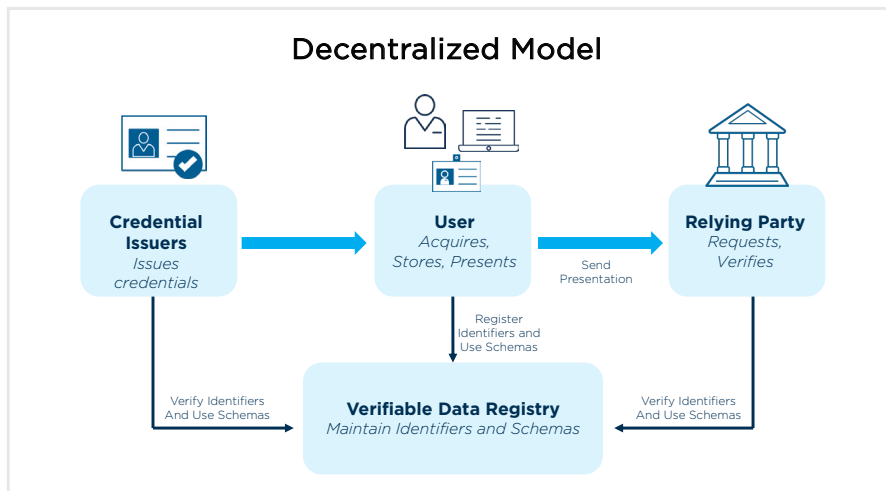
IDP Market



Federated Ecosystem



Decentralized



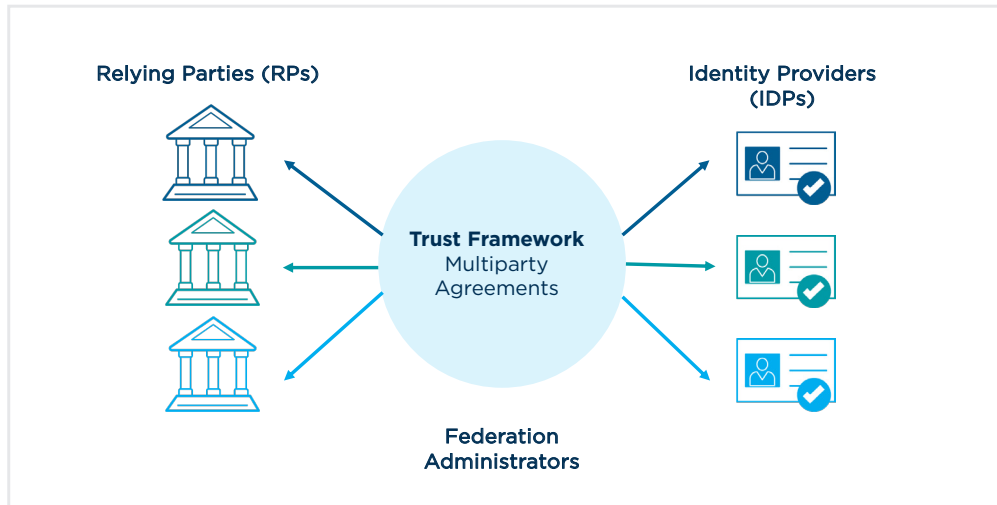
Sources: Adapted from NISTIR 8149¹² and Verifiable Credentials Data Model v1.1-<https://www.w3.org/TR/vc-data-model/>

12 Temoshok, David, and Christine Abruzzi. 2018. NISTIR 8149: “Developing Trust Frameworks to Support Identity Federations.” <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8149.pdf>.

Basic Components of a Federation

Federations enable a relying party (RP) to trust the identity assertions provided by other entities according to a defined trust framework. As shown in figure 1.2, federations consist of identity providers (IDPs) and RPs that have agreed to participate in an identity federation arrangement under a trust framework. This section provides an overview of each of these components and roles.

Figure 1.2: Key Components of a Federated Digital ID Ecosystem



Source: Adapted from NISTIR 8149¹³

Identity Providers (IDPs)

Each IDP within a federation is a digital ID system that registers individuals, issues credentials, and provides authentication and identity assertions to relying parties (RPs). IDPs can be entities who already manage foundational or functional ID systems,¹⁴ or new entities created to provide services under the federation. IDPs can include government entities—for example, a national or digital ID agency, tax authority, social insurance agency, civil registration system, or public postal service—or private firms, such as a bank, mobile network operator (MNO), or private postal service. The IDP could also be a broker/hub delegating identity assertion to other IDPs based on the trust framework. IDP activities throughout the identity lifecycle¹⁵ are described below.

Registration: IDPs register new users and verify their identities in a process known as “identity proofing” before issuing digital credentials. This process generally relies on pre-existing ID systems and/or other authoritative sources of identity information to verify identity attributes and associate or “bind” the credential to the identity. As a result, the registration process depends heavily on the landscape of existing ID systems in the country, as described in more detail under Section 1.2: Approaches to Federation.

¹³ Temoshok and Abruzzi. 2018. NISTIR 8149: “Developing Trust Frameworks to Support Identity Federations.”

¹⁴ See the ID4D Practitioner’s guide glossary for definitions of foundational and functional ID systems and other terms.

¹⁵ See <https://id4d.worldbank.org/guide/identity-lifecycle> for more information on the identity lifecycle.

Credentials: The credentials issued and/or used by an IDP to verify or authenticate an individual vary by context. Examples include a mobile cryptographic subscriber identity module (SIM); a mobile app; biometrics; smart cards; a mobile number; a cryptographic token, such as FIDO security keys; a password; PIN; or combination of these factors. In conjunction with the identity proofing process, the types of credentials used enable authentication at different levels of assurance (see box 1.1).

Box 1.1: Levels of Assurance

The level of assurance (LOA) reflects the relying party (RP)'s trust that an identity assertion provided by an identity provider (IDP) is the person's "true" identity. Higher levels of assurance reduce the risk of a fraudulent identity and increase the security of transactions, but also can increase the cost and inconvenience to users and RPs. Therefore, the assurance level required by an RP for a particular transaction must be carefully evaluated to mitigate security risks while maintaining the inclusivity and user-friendliness of the system.

The overall assurance level provided during a transaction depends on the strength of:

1. **The identity proofing process (identity assurance level, or IAL)** based on the method of identification during enrollment, such as in-person vs. remote; the attributes collected; and the degree of certainty with which those attributes are verified against authoritative sources, for example, a civil registration or national ID system.
2. **The authentication mechanisms (authentication assurance level, or AAL)** based on the type of credential(s), the number of authentication factors used—in other words, one vs. multiple—and the cryptographic strength of the transaction.
3. **The federation protocols (federation assurance level, or FAL)** based on the type and strength of cryptography used to establish the authenticity of the identity assertion.

Source: Adapted from NIST Special Publication 800-63-3. See also ID4D Practitioner's Guide: <https://id4d.worldbank.org/guide/levels-assurance-loas>.

Frequently, different IDPs offer varying levels of assurance, and may issue different types of credentials and authenticators, such as a smartcard, mobile ID, or biometric-based authentication, so that users have a choice of which IDPs and credentials to use for a given service. In **Norway**, for example, people can choose between six different electronic IDs to access over 1000 digital services from Norwegian public authorities (see box 1.2 below).

Box 1.2 Different forms of electronic ID in Norway

The following graphic and table illustrate various sign-in options available at <https://idporten.difi.no/>, as well as levels of security associated with different credentials.

ARBEIDS- OG VELFERDSETATEN

SELECT AN ELECTRONIC ID

- MinID**
MINID
Use codes from SMS or PIN code letter
- BANKID**
BANKID
Use BankID app, code chip or BankID on mobile
- BUYPASS ID**
BUYPASS ID
Use Buypass ID on smart card or mobile
- COMMFIDES**
COMMFIDES
Use smart card

FOREIGN USERS
Login and registration for new users with passport

[How to obtain an electronic ID](#)

EID – Security Level (SL)	Login Credentials	No. of Users (2014)
MinID (SL-3)	National identity number, password + single-use code from SMS or PIN code letter	>3.1m
BankID (SL-4)	National identity number, password + code from the security token issued by the bank	>3.1m
BankID on mobile (SL-4)	Mobile number + date of birth, crypto SIM, and PIN code	425,000
BuyPass ID on Card (SL-3 and 4)	National identity number, smart card + PIN for smart card	>2 million at level 3 card and 350,000 at level 4
BuyPass ID on Mobile (SL-4)	National identity number, Mobile SIM + PIN code	
Commfides (SL-4)	Smart cards/USB drives and PIN	Small actor

Source: information obtained from <https://eid.difi.no/en/id-porten/what-electronic-id-e-id> and a presentation by Norwegian authorities.

Authentication and verification services: When requested, IDPs provide an “identity assertion” to RPs. The identity assertion includes the level of assurance achieved (see box 1.1) and the user’s attributes, which are either pre-specified in the trust framework, or those which the user has consented to share as part of the transaction. With federated ecosystems, the federation assurance levels required by an RP and provided by an IDP are mutually agreed upon based on the risk level of the transaction being completed, along with identity proofing and authentication levels of assurance.

Relying Parties (RPs)

RPs consume identity assertions provided by the IDPs and use the information to authorize access to users for services and applications. RPs may be public or private organizations that offer services, applications, and information that require restricted access, such as certain government benefits and services, online banking services, or online healthcare provider services.

Relying parties rely upon and utilize identity assertions from IDPs, rather than operating separate identity management systems of their own. In this way, RPs can achieve their goals of providing online services without bearing the cost of managing identity services that are neither core to their business nor their core competency. RPs may still create and manage accounts for their users and customers (for example, to track applications), but this information is separate from the identity and access management function.

RPs must be able to trust the identity information they receive from IDPs to make risk-based decisions related to beneficiary or customer identity, such as for enrollment into programs or account opening. To do this, RPs and IDPs use federation protocols like security assertion markup language (SAML) and OpenID Connect to establish secure connections across an open network for transmitting identity assertions

RPs also define the levels of assurance required for access to a service, as well as the identity attributes required from identity providers. For some RPs, like financial institutions, the LOA and attributes may be defined through governmental regulation, such as know-your-customer (KYC) or customer due diligence (CDD) regulations.

Identity Exchanges, Hubs, and Brokers

An identity exchange, hub, or broker (henceforth referred to as an “exchange”) serves as the intermediary between IDPs and RPs in a federated architecture. This exchange enables additional IDPs and RPs to be added to the federation seamlessly, and for the user to choose among multiple IDPs to establish their identity in order to access a service provided by the relying party.

As summarized below in table 1.2, an exchange can perform multiple functions to increase convenience, streamline services, and enhance data protection and privacy for users. For example, it can pseudonymize or tokenize user identities to make the IDP and RP blind¹⁶ to each other, obtain and manage user consent for sharing attributes, and maintain audit logs. It can also perform functions to enhance user experience by filtering which identity providers provide the level of assurance required by the relying party, remembering user choice of IDP for subsequent logins and providing a dashboard for transactions.

16 A single blind involves blinding relying parties from identity providers, so that the IDP is not aware of which RP is making the request. In a double blind, the identity of the IDP is also concealed from the RP, so that the RP only knows the level of assurance provided and cryptographic proof that the identity assertion is authentic. Triple blind is the same as double—with the additional feature that the identity exchange itself is also blinded from transactions.

Table 1.2: Potential Functions of an Identity Exchange

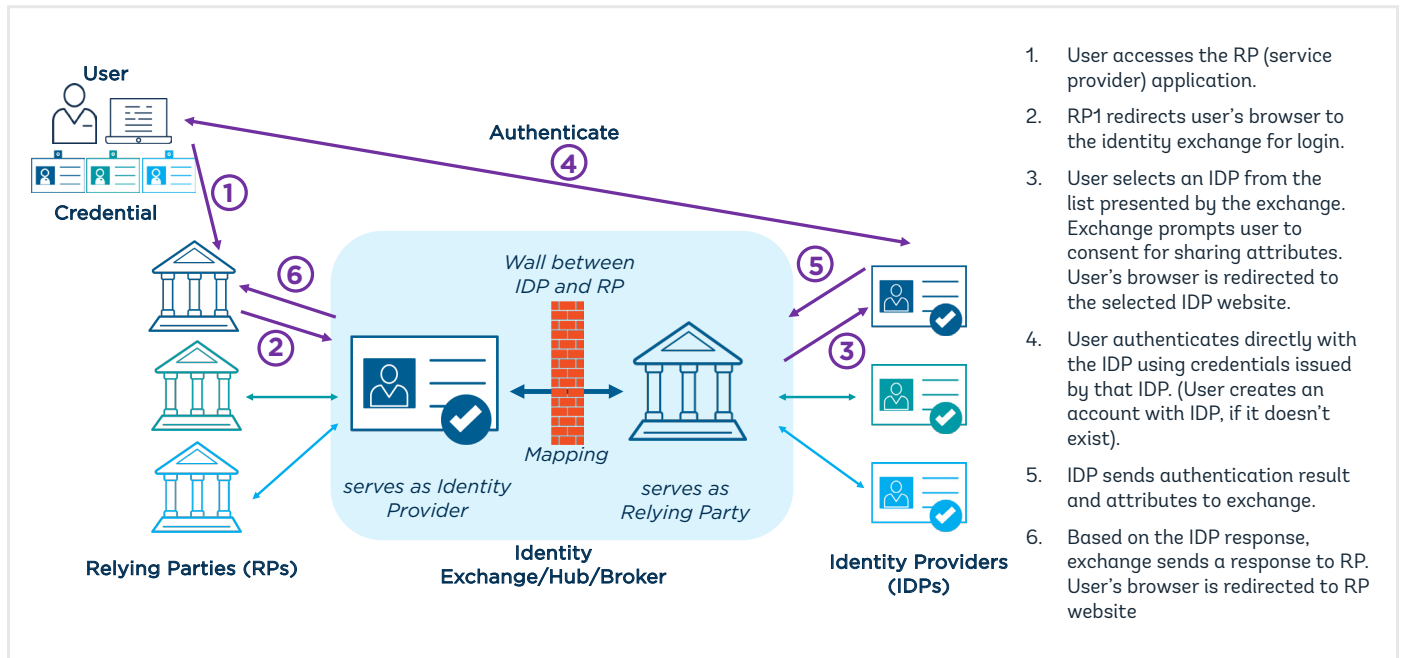
Functionality	Description
Identity Provider (IDP) Selection	<ul style="list-style-type: none"> • IDP filtering: selecting IDP which meets the level of assurance required by a relying party (RP) • Remember user choice of IDP for subsequent login • User interaction for IDP selection
User Consent	<ul style="list-style-type: none"> • Interaction with user for consent • Remember user consent for reuse
Identity Resolution and Blinding	<ul style="list-style-type: none"> • Mapping identifiers for an identity from IDP to RP and thus enhancing privacy by building a wall between IDPs and RPs. The exchange tokenizes¹⁷ or maps the identifier issued by an IDP for a user and issues different unique identifiers to each RP for that user.
Protocol Support	<ul style="list-style-type: none"> • Implementation of the federation protocols: security assertion markup language (SAML), Open ID Connect + open authorization (OAUTH) to support choice and legacy applications.
Attribute Enrichment	<ul style="list-style-type: none"> • Integration with additional attribute providers to provide further verified attributes to relying parties
Auditing	<ul style="list-style-type: none"> • Maintains logs for forensic and non-repudiation requirements, as only the exchange has the complete visibility and traceability of authentication and attribute requests. It is necessary for the logs to be anonymized or pseudonymized so as to ensure that the hub does not become an entity with a 360-degree view of an individual.
User Dashboard	<ul style="list-style-type: none"> • Provides user with their transaction history and also manages their consent preferences

Source: Trusted Digital Identity Framework (TDIF) of Australia. n.d. <https://www.dta.gov.au/our-projects/digital-identity/digital-identity-system>.

Figure 1.3 illustrates an authentication request workflow via an identity exchange that uses **double blinding**. In this example, the IDP sends the identity verification response to the exchange and does not know—that is, “It is blind”—to the identity of the RP requesting the service. Similarly, the RP interacts only with the exchange and does not know which IDP provided the assertion. The exchange is responsible for mapping the tokens between the IDP and RP, thus ensuring that (a) a user’s identifier is different for each RP for a given IDP, and (b) that the identifier is different for the same RP when the IDPs are different for the same user. This model provides increased privacy to users by positioning the identity exchange as a wall between IDPs and RPs. However, for RPs that require uniqueness of users, a mechanism is also necessary to resolve the identity of a user when they are using multiple IDPs.

17 See ID4D “Privacy by Design” and “The ID4D Practitioner’s Guide.”

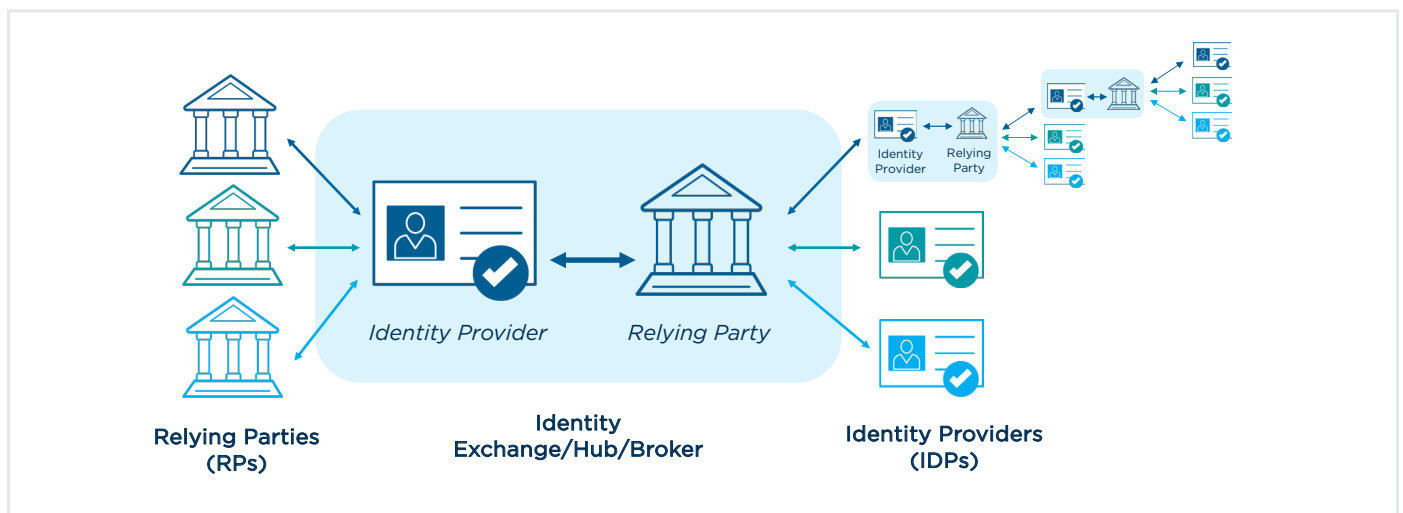
Figure 1.3: Example of an Authentication Request Flow with Double-Blind Identity Exchange



Source: Author

As shown in figure 1.4 and box 1.3, the exchange can be **cascaded and exist at multiple levels** of IDP federations, wherein one identity provider is an exchange, and further stages follow it. This exists in the EU eIDAS federated architecture, where the eIDAS nodes are connected to national exchanges—such as the State Authentication Service (*Riigi autentimisteenus* or TARA) of Estonia or CSAM of Belgium—and may perform the role of an IDP when accessing a service at an RP. However, these eIDAS nodes also become hubs, brokers, or exchanges for access to cross-border services, prompting the user to choose the IDP of their choice in another EU country.

Figure 1.4 Example of a Cascaded Exchange/Hub/Broker

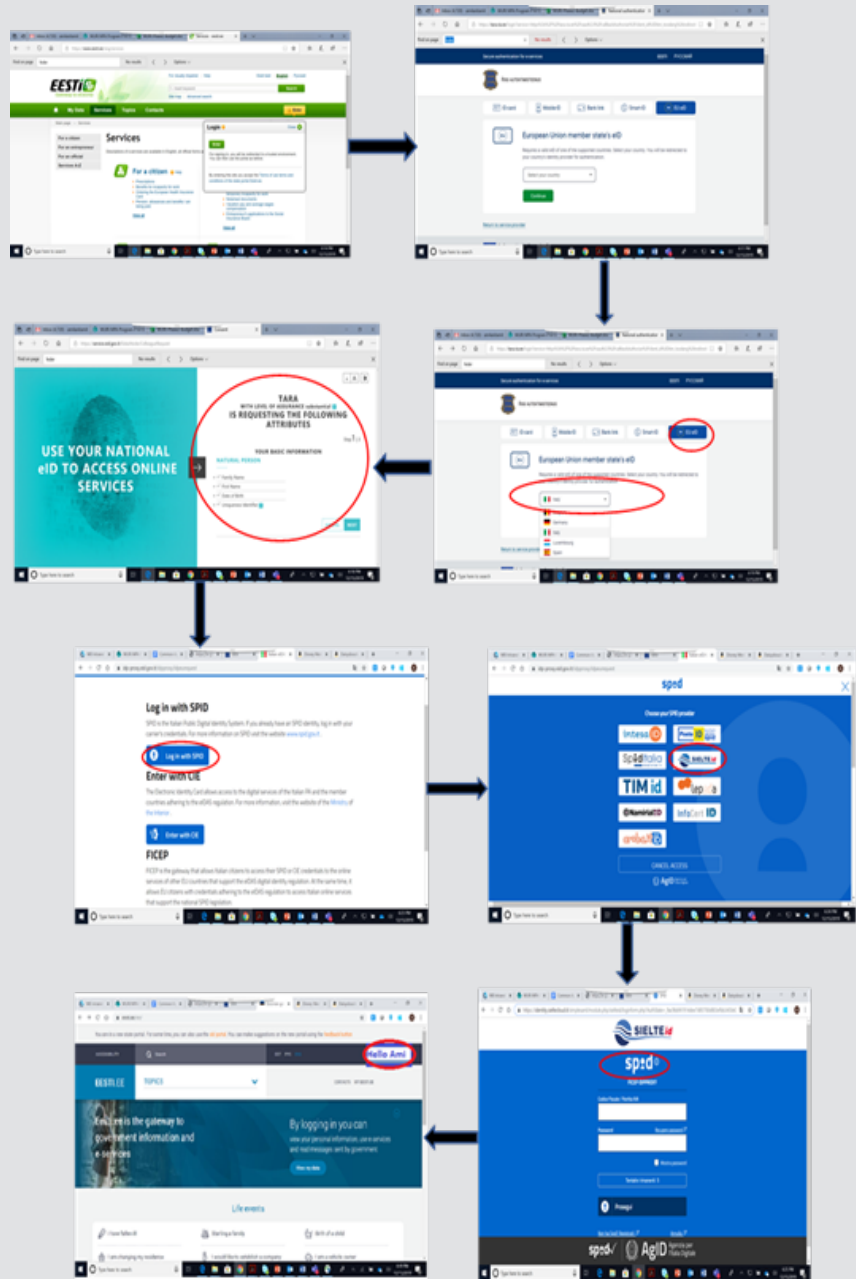


Source: Author

Box 1.3 Cross-Border Authentication Flow – Estonia and Italy – EU Electronic Identification and Trust Services (eIDAS)

The below sequence of screenshots shows the user experience with a cascaded identity exchange for cross-border authentication. In this illustrative example, the user is accessing a service on Estonia’s portal using credentials issued by an Italian identity provider (IDP). As such, the user could be physically present in any country.

1. User visits Estonia’s portal for accessing public services and clicks the “login” button
2. User’s browser is redirected to the exchange hub TARA (Estonia) webpage, wherein the user chooses the “EU eID” option
3. User is prompted to choose the ID country; user chooses Italy
4. The Italian exchange requests user consent for sharing of attributes with TARA; on obtaining consent, exchange redirects user’s browser to the options for selecting an IDP
5. User selects Sistema Pubblico di Identità Digitale (SPID) from available IDP options, and user’s browser is redirected to SPID login page
6. SPID provides another list of IDP options; user selects “SielteID”
7. User’s browser is redirected to the SielteID webpage, where the user enters the credentials for authentication
8. The user will be redirected back to the Estonia public portal and logged in to the website if authentication is successful



Source: Screenshots of the flow from https://tara.ria.ee/auth/init?login_challenge=b6d8cfe6d7a9466a8ac859362e9815ef&lang=en

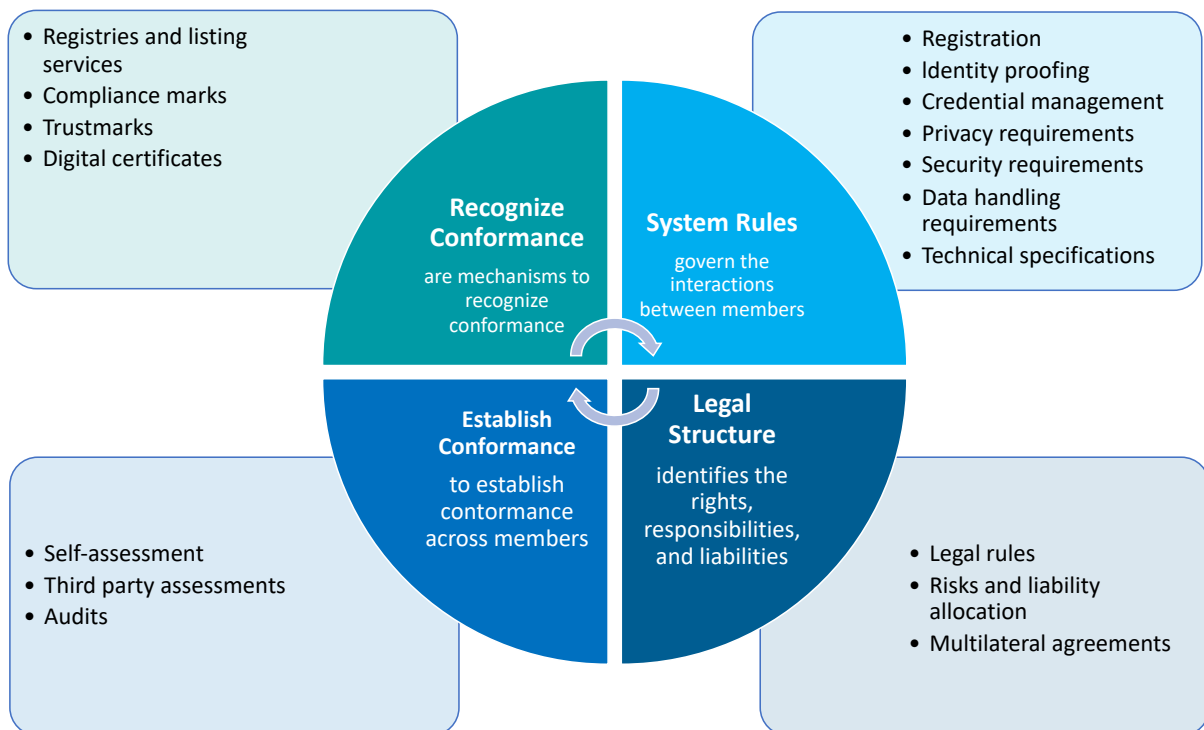
Trust Frameworks

Trust frameworks are a set of agreements and associated rules among IDPs and RPs that are part of the federation. Trust frameworks stipulate standards, protocols, roles, and responsibilities, and serve as the basis for the multilateral agreements that enable the trust and governance of a federation's operations among its members. These include:

- Conducting identity management responsibilities (registration/enrollment, identity proofing, and credential management, among others)
- Sharing identity information
- Using identity information that has been shared with the trust framework
- Protecting and securing identity information
- Performing specific roles within the federation
- Managing liability and legal issues¹⁸

Four key components that characterize an identity trust framework according to the NIST framework are shown below in figure 1.5.

Figure 1.5: Trust Framework Components



Source: Adapted from Temoshok, David, and Christine Abruzzi. 2018. NISTIR 8149: "Developing Trust Frameworks to Support Identity Federations." <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8149.pdf>

¹⁸ Temoshok, David, and Christine Abruzzi. 2018. NISTIR 8149: "Developing Trust Frameworks to Support Identity Federations." <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8149.pdf>; and Makaay, E, Smedinghoff, T. and Thibeau, D. 2017. OIX White Paper: "Trust Frameworks for Identity Systems." <https://www.oixnet.org/news-whitepaper/>.

Developing a trust framework for a federation involves many stakeholders and requires clear leadership and coordination. In addition, federated ecosystems require administrators to actively govern the federation and oversee implementation of the trust framework in practice. According to NIST¹⁹, potential roles for federation administrators include:

- Establishing the trust framework rules and requirements
- Developing and managing documentation
- Managing membership and participation
- Managing member conformance to the trust framework’s rules
- Maintaining, promoting, and evolving the federation
- Overseeing the smooth operation of the federation, including undertaking fraud and security investigations

Approaches to Federation

Identity federation architectures can be separated into two broad types based on their relationship with existing official ID systems and the types of authoritative sources they use. The first category consists of cases in which the digital IDs provided by the federation are anchored in an existing foundational ID system that provides a unique identity, such as those of Estonia, Belgium, Norway, Denmark, Thailand, and Uruguay. Countries without foundational unique identifiers, such as the UK and Australia, have developed a second model of federation. These general differences are discussed below.

Federation Type 1 – Anchored by an Existing Foundational ID and Unique Identity

Historically, most countries with longstanding foundational ID registries have chosen to issue official digital IDs through these systems, often in the form of “electronic ID” or eID smart cards, whereas in more recent cases, such as in India or the Philippines, foundational ID systems have been built with digital authentication capability from the onset. However, other countries—including **Estonia, Belgium, Norway, Denmark, Uruguay, and Thailand**—have leveraged existing foundational ID systems and registries to develop new federated ecosystems with multiple IDPs to facilitate access to online public services, and in some cases, private sector transactions and services as well.

While each of these systems is distinct, they share some key characteristics:

- **Type 1 - A: Reliance on a foundational register as an authoritative source for identity proofing:** Each of these countries has a well-established ID database, population register, or centralized civil registration system that issues a unique identity, which serves as an authoritative source for identity verification during registration/onboarding by IDPs. In each case, birth registration and foundational ID coverage are close to universal, and (digital) administrative records are generated about the individual continuously from birth, such as a school record, health records, etc., minimizing the risk of identity fraud or duplicate identities (fig 1.6).

19 Temoshok, David, and Christine Abruzzi. 2018. NISTIR 8149: “Developing Trust Frameworks to Support Identity Federations.” <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8149.pdf>

- Type 1 - B: Foundational digital ID serves as an “anchor” to bootstrap IDP in the federation:** These countries each have a digital credential—for example, a smart card in **Estonia** and **Belgium** or a password and code in **Denmark** and **Norway**—issued to all citizens and legal residents. This credential is bound to the unique identifier issued by the foundational ID register or system, which acts as an “anchor” IDP. In this manner, foundational ID enables remote/presenceless online identity proofing, credential binding, and issuance of derived²⁰ credentials, generally in real time, by other IDPs in the federation. In **Belgium**, for example, people can obtain the federated itsme® mobile ID in real time using their smart card national ID for identity verification. They can also receive alternate digital ID or credentials, known as digital keys, which consist of a username, password, and a token code. The token code can be set up online through mobile authenticator apps or as a one-time password (OTP) through SMS. All of these processes are managed by online authentication with the smart card eID via the central ID portal (table 1.3).
- Adoption of single sign-on (SSO)²¹:** Each of the countries in this example has a central identity exchange/hub that connects IDPs and implements SSO for public sector services; RPs then connect to this platform for identity assurance services. The identifiers—such as username or user ID—used across different IDPs for authentication, are linked to the unique national level identifier and enable single sign-on when accessing services from different service providers. The European countries also follow the “once only” principle, under which the user is not expected to provide the same data twice to the government. Government services are expected to retrieve the required attributes or data from the authoritative sources for providing service, as per the requirements for delivering that service, which is enforced through authorization-based access control policies.

Table 1.3: Examples of Federation–Type 1

Feature	Belgium	Estonia	Norway	Denmark
Foundational System/ Authoritative Source	Population register	Population register	Norwegian National Registry	Central person register (CPR) – Civil Register
Unique ID Number Used by All Identity Providers (IDPs)	National identification number (NIN) -11-digit code, based on birth date and gender	Personal identification code -11-digit code, based on birth date and gender ²²	NIN number -11-digit code consisting of the date of birth, xx, gender, and control digits -Example: ddmmyyxxgcc (g-even for women and odd for men)	CPR number -10 digits -Example: Ddmmyyxxxg (g-even for women and odd for men)
Hub, Broker, or Exchange	CSAM	TARA	ID-porten	NemID /MitID ²³

20 As defined in NIST SP800-63-3, “binding” is the technical process of associating a user with a credential, while a “derived credential” is one that is “issued based on proof of possession and control of an authenticator associated with a previously issued credential, so as not to duplicate the identity proofing process (See <https://pages.nist.gov/800-63-3/sp800-63-3.html>).

21 Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (such as a username and password) to access multiple applications. The service authenticates the end user for all the applications the user has been given rights to and eliminates further prompts when the user switches applications during the same session.

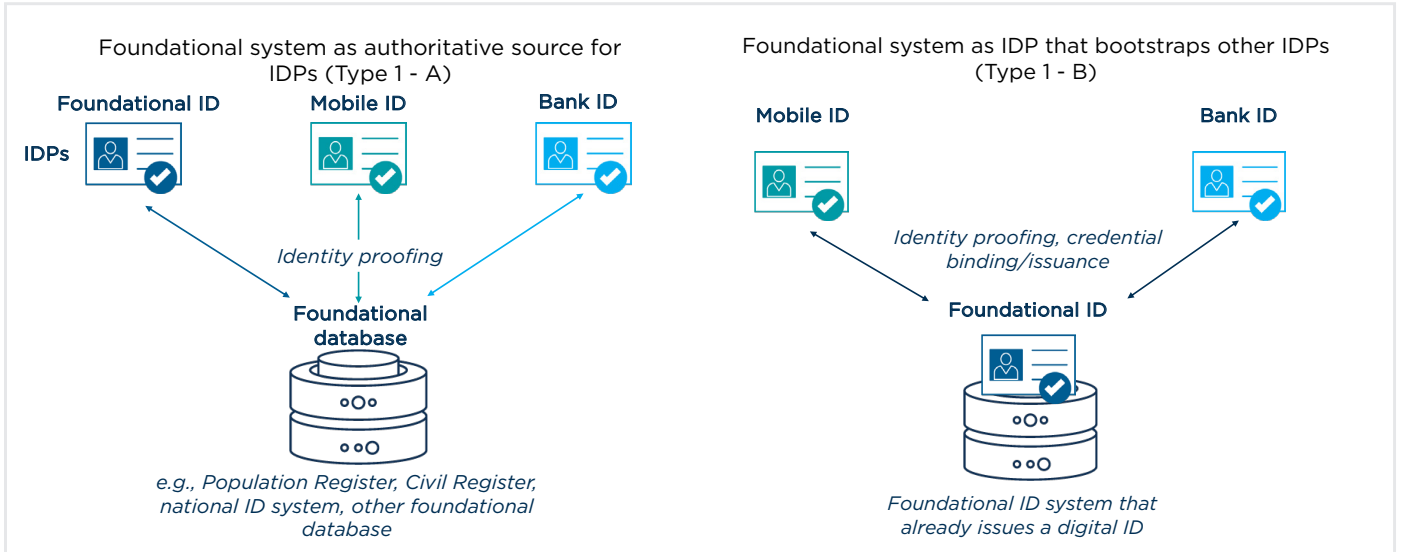
22 A “gyymmddxxxc” code consists of: “g” for century counter + gender—odd for men and even for women; “yyymmdd” for date of birth; “xxx” for registry number at a given date; and “c” for control number.

23 MitID has stronger authentication factors than NemID and may replace NemID by the end of 2022.

<p>IDPs and Credentials</p> <p>(examples in bold indicate government-provided anchor IDP)</p>	<ol style="list-style-type: none"> eID card (smart card) Mobile ID(itsme®) Digital keys (username, password + one-time password (OTP) code app) Digital keys (username, password +OTP on SMS) Username+password EU-Electronic Identification and Trust services (eIDAS) 	<ol style="list-style-type: none"> ID Card (smart card) Mobile ID (public key infrastructure, or PKI, SIM card) Smart ID (mobile app + remote qualified electronic signature creation device, or QSCD) EU-eIDAS 	<ol style="list-style-type: none"> MinID (national ID number, password+code) Bank ID – smart card Bank ID on mobile app Buypass – smart card Buypass on mobile Commfides – smartcard/USB EU-eIDAS 	<ol style="list-style-type: none"> User ID, password+token code card Password+token code mobile app Password+hardware token Password+token on IVR Mobile app EID gateway for EU- eIDAS
<p>Relying Parties (RPs)</p>	<p>All public service providers connected to the Federal Authentication Service (FAS)</p>	<p>All public service providers</p> <p>–Authentication service for private sector services as well</p>	<p>All public service providers for Single Sign-On</p> <p>–Authentication service for private sector services as well</p>	<p>All public service providers for single sign-on(SSO)</p> <p>–Authentication service for private sector services as well</p>
<p>Trust Framework Administration</p>	<p>Joint responsibility of government member institutions</p>	<p>Republic of Estonia Information System Authority (RIA) for “State Authentication Service” hub solution</p> <p>–Other hub solutions used by many portals/e-services, including tax and customs system, Ministry of Justice system, and BankLink</p>	<p>Norwegian Digitalisation Agency</p>	<p>Agency for Digitisation</p>

Source: Author

Figure 1.6: Using Foundational Authoritative Source (A) and Digital ID Credential (B) for Issuance of Credentials Derived by Other IDPs



Source: Author's Analysis

Federation Type 2 – Ecosystems without a National-Level Unique Identifier

A second set of countries, including the **UK** and **Australia**, have built federated ID ecosystems without the anchor of an existing (digital) foundational ID system or national-level unique identifier. Again, each country’s model is distinct, though they share some common characteristics:

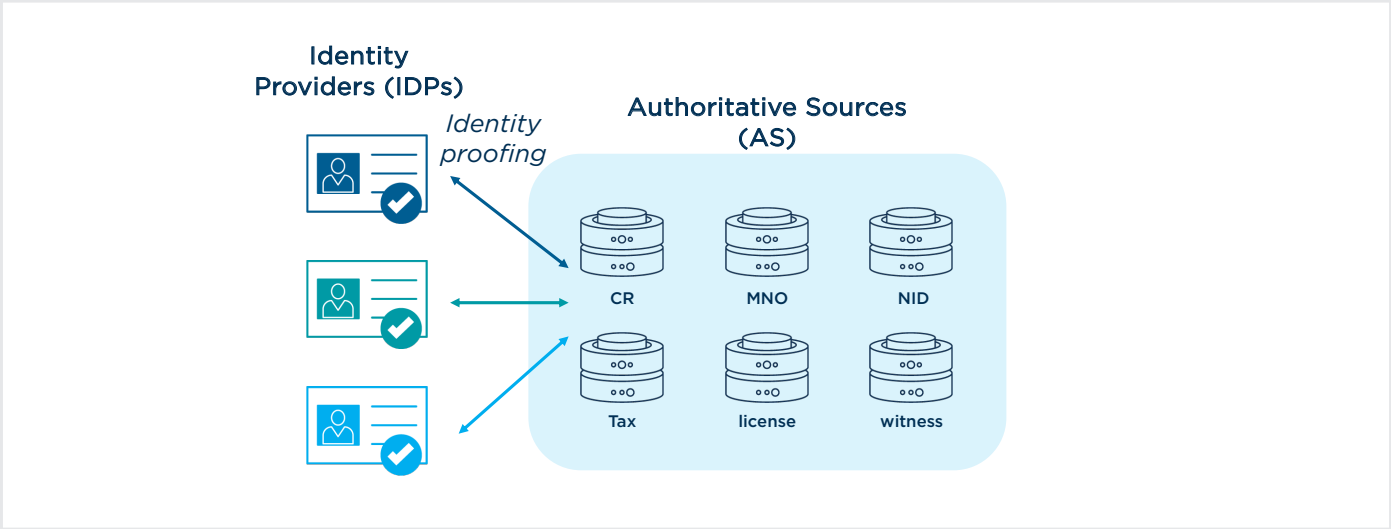
- **Identity-proofing based on multiple authoritative sources:** Because birth registration in these countries is very high, this provides an authoritative source for identity information. However, because civil registry records are managed locally rather than centrally, they do not provide unique, population-wide identities like the population registers in Type 1. As a result, IDPs in these countries have also relied on a variety of functional ID systems and databases for identity proofing, including passports, driving licenses, mobile network operators, and utility agencies (see table 1.4 and figure 1.7).
- **Each IDP generally follows its own identity proofing process and issues IDP-specific identities:** Each IDP follows its own process of identity proofing based on evidence provided in alignment with the defined procedures of the trust framework for identity proofing at the desired or required assurance level. Identity proofing is generally done by using two to three different authoritative sources, such as a driving license and passport, to validate or verify identity and credential binding. Because there is no unique identity at the national level, IDPs independently issue unique identifiers to each person who has enrolled in their system, which are not linked. Therefore, a person can have multiple identifiers—one from each IDP.
- **Interoperability for joined-up services or orchestration of services can be challenging, as the identifiers are not the same for a user across RPs:** Because users have different identifiers across RPs, implementation of services requiring matching of records across RPs has been more complex in these countries; resolving records across databases involves matching on biographic attributes, such as name and date of birth, which may have inconsistencies across systems .

Table 1.4 Examples of Federation–Type 2

Feature	UK	Australia
Authoritative sources used for identity proofing	Mobile phone providers, credit agencies, passport, driver and vehicle licenses	Driver licence, Medicare card, birth certificate, citizenship certificate, or passport.
Hub, broker, or exchange	GOV.UK Verify	Exchange and Connect ID
IDPs	<ol style="list-style-type: none"> 1. Digidentity 2. Post office *Experian, Barclays, and Security Identity are former IDPs	<ol style="list-style-type: none"> 1. Australian Taxation Office (ATO)-myGovID mobile app 2. Australia Post-Digital ID mobile app 3. OCR labs (one-off based on biometrics)
RPs	Public sector	Public and private sector
Trust Framework	GOV.UK Verify	Trusted Digital Identity Framework (TDIF)

Source: World Bank.

Figure 1.7: IDPs use multiple strong authoritative sources (Type 2)



Source: Author.

When is Federation a Good Choice?

The factors that influence the development and model of digital ID in a given country are varied and highly dependent on context, legacy systems, potential use cases, and demand—there is no one-size-fits-all solution.²⁴ This section aims to help practitioners evaluate the appropriateness of a federated model by outlining the key features of a federated ecosystem, potential risks and challenges, and common enablers and success factors based on global experiences.²⁵

Key Features and Benefits

Some features and potential benefits are common to any federated ecosystem model, while others are specific to the precise architecture adopted for federation. This section highlights key characteristics of federated systems across multiple dimensions, including:

- **Choice of identity provider (IDP):** By their nature, federations provide users with more choice over which digital identity provider to use than single IDP or functional ID-driven models. People may already have digital IDs with certain IDPs—for example, a national ID or bank—that they can then use to easily access multiple services through the identity federation without having to obtain a functional ID for that service.
- **Choice of credentials:** While single IDP models can offer a choice of credentials, such as the same IDP issuing multiple types of credentials in different authentication factors, this has been less common in practice. Federations of multiple IDPs with varying credential form factors can therefore increase the number and types of credentials people can choose from as they provide credentials to meet different levels of assurance. See box 1.2 and box 2.1 for examples.

24 See the ID4D Practitioner’s Guide for further discussion on drivers influencing ID system design. <https://id4d.worldbank.org/guide/section-ii-designing-id-system>.


25 In this section, federated systems are contrasted on key dimensions with functional ID, single IDP, and IDP market models described above; given the limited number of national-level deployments of decentralized models to date, these are not compared in detail here. For an example of detailed analysis of the potential benefits of federated ecosystems in specific cases, see the publications of National Institute of Standards and Technology (NIST Special Publication 800-63 Digital Identity Guidelines), the Canadian trust framework (Trust Framework | Digital ID & Authentication Council of Canada) and Australian trust framework (<https://www.dta.gov.au/our-projects/digital-identity/digital-identity-system>).

Box 2.1 Examples of IDP and Credential Choice

People may choose an IDP based on pre-existing trust in the institution, or their preferred type of credential, such as a preference for smart phone-based credentials, or for smart cards or biometric-based authentication.

In **Sweden** and **Norway**—where the average person interacts with their bank far more often than the government—there is a high saturation of strong credentials used for BankID, which is now part of a digital ID federation. It has been natural for people to use digital BankID credentials as a means of identification for online government services, as they were accustomed to using these credentials for banking; trust in banking translated to trust in authentication for other services with the same credential.

In Italy, the Sistema Pubblico di Identità Digitale (SPID) ecosystem offers a variety of credential forms and factors for users to choose from, as listed in the image below.

IDENTITY PROVIDER	SECURITY LEVELS	GEOGRAPHICAL AREA	RECOGNITION IN PERSON	REMOTE RECOGNITION	RECOGNITION CIE*, CNS	Sending the OTP code also via sms	RAO
	①②③	IT EU	✓	Via webcam (paid service)	✓	YES Free service	Discover more 
	①②③	IT EU	✓	Via webcam (paid service)	✓	YES Free service	Discover more 
	①②③	IT EU	✓	Identifica App with CIE (free) or via Webcam (free)	✓	Yes Free service	✓ Discover more 
	①②③	IT EU	✓	PosteID App with CIE and PIN (free of charge) PosteID App with electronic document without PIN or bank transfer (subject to charge)	✓	YES Free service	✓ Discover more 
	①②③	IT EU	✓	Via webcam (paid service)	✓	YES Free service	Discover more 
	①②③	IT EU	✓	Via webcam (paid service) Audio-video with bank transfer (payment to charity)	✓	YES Free service	Discover more 
	①②③	IT EU	✓	Via webcam (paid service)		YES Free service	Discover more 
	①②③	IT EU	✓	via webcam	✓	YES paid service	Discover more 
	①②③	IT EU		Via webcam (paid service)	✓	No	Discover more 

Source: <https://www.spid.gov.it/en/what-is-spid/how-to-choose-between-digital-identity-providers/>

- **Reuse and portability of credentials:** In contrast with a functional ID model—in which each service provider issues and manages their own ID—single IDPs, IDP markets, federated ecosystems, and decentralized models provide for “reuse” and portability of credentials across systems. An individual can be identity-proofed once and issued an identity and a credential bound to that identity, which can be used by multiple RPs. Compared with market models where IDPs are not coordinated, federations and single IDP models can make this process seamless. In federated models, an identity issued from one IDP can also make it easy to establish or prove identity and subsequently obtain identity credentials from other identity providers.
- **Minimizing data sharing with relying parties (RPs):** Under a functional ID model, each provider would have access to a person’s identity proofing documents, which generally shares more data than needed by the RP for the service delivery. In contrast, federated and decentralized models can enable sharing of a minimal set of pre-agreed attributes with the RP based on the user’s consent, as well as options to pre-define different combinations of approvals for different attributes and/or RPs for a better user experience. The same is also possible in single IDP models, although few have implemented this in practice. In contrast, it is standard with federated identity exchange and decentralized models.
- **Reducing visibility of transactions:** When authentication is performed by a single IDP across multiple RPs, it creates the possibility of developing a complete, 360-degree view of an individual’s data and transactions.²⁶ While certain controls and privacy-by-design (PBD) features can help prevent this type of profiling in single IDP systems, federation offers another approach by using multiple IDPs and an identity exchange as an intermediary so that no single IDP has a holistic view, as in most implementations, the hub blinds the IDP and RP from each other during an identity verification. However, particularly for Type 1 federations that use a common identity across IDPs and RPs, there is still the possibility that the identity exchange itself could potentially aggregate a user’s data and transaction information. In addition to standard controls applied in other systems, identity exchanges can be designed to blind the exchange from transactions.
- **Incentives for innovation:** Under multiple IDP models, including federation, the private sector is encouraged to provide an enhanced user experience with authentication options to attract users to their service offering. For instance, a smartphone-based mobile ID provided by a bank, that is simple and easy to use, could be accepted for online banking as well as providing a proof of identity to access other services. In federated (or IDP market) models, the private sector may be able to charge a fee for providing identity and authentication services to other service providers/RPs. Some private sector providers may be able to offer innovative credential form factors with enhanced usability, security, privacy, or mix of features to meet varying needs of different population groups with innovative business models.
- **Reduced cost and risk associated with RP-managed credentials:** Federated models, as well as single IDP and decentralized models, enable reusability of credentials across different RPs, allowing RPs to outsource identity management to IDPs; for example, RPs do not need to set up a forgotten password or lost card helpdesk. Compared to functional ID models, in which RPs are managing identities themselves, this can reduce the replication of users’ personal data across the internet and alleviate the need for users to manage multiple credentials or logins that may be vulnerable to loss or attack.

²⁶ Legal, technical, and operational controls and privacy-by-design features can reduce the risk of a single IDP having a 360-degree view or aggregation of data about an individual. This could include tokenization of identifiers to limit linking of data across databases and individual profiling, as well as auditing, tamper-proof logs, personal data monitors, robust security practices, and access controls. For more information, see Mittal, Anita, and Ridhee Malhotra. 2018. “Privacy by Design: Current Practices in Estonia, India, and Austria. Identification for Development Washington, D.C.: World Bank Group. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/546691543847931842/privacy-by-design-current-practices-in-estonia-india-and-austria>

- **Ability to scale and expand user bases:** Compared with functional ID models where each RP needs to perform identity proofing and credential issuance for the users during onboarding, federated models (as well as single IDP models) allow RPs to expand their user base more quickly by relying on the identity proofing and credentials of third party IDPs. For federated ecosystems, the RP can enable the addition of additional IDPs and, subsequently, their users, with minimal configuration changes to the hub as compared to the onboarding process of single IDP with a new RP. With a federation, there are clear and transparent rules for new RPs and IDPs to join the federation, making it easier to scale more quickly than IDP markets without federation infrastructure and trust frameworks in place. Federation provides access to greater capacity over multiple IDPs and familiarity for users as they reuse their credentials to access multiple RPs.
- **Ability to streamline services and logins.** If the digital ID ecosystem is linked with other digital public infrastructure, such as payment gateways or electronic signatures, then the RP can leverage all the shared resources and services in a plug-and-play model. Typically, this is easier with a single IDP or federated model Type 1, and more difficult in the case of Type 2 federation. In many EU countries, a digital ID provided by a single IDP or federated ecosystem with single sign-on (SSO) is a key component of the whole of government architecture, enabling sharing of data across multiple service provider systems for decision-making based on business rules.

Risks and Challenges

Federated ID ecosystems can also have specific risks and challenges. As previously discussed, the precise issues can vary based on the specific federation architecture, and some risks can be mitigated through specific approaches, as noted below.

- **Complex multiparty protocols and governance:** Federation requires relatively complex multiparty protocols that have subtle security and privacy constraints and necessitate careful consideration. Commercial aspects linked to business models and liability also need to be taken into account. Additionally, developing and governing a multi-party trust framework requires effective stakeholder coordination and leadership. Efficient regulation and governance of the trust framework governing these interactions is crucial for the successful operation of the federation and could be challenging in a low-capacity environment.
 - **Mitigation:** Technical risks can be managed through adoption of common, industry supported protocols, such as security assertion markup language (SAML), Open ID Connect, and Open Authorization (OAuth). Transitions to newer protocols can be done via a managed process. Additionally, capacity building through training and hiring of experts can help mitigate governance challenges. Financial viability analyses may also be required to determine commercial models.
- **Potential lack of user-friendliness due to multiple redirects, especially on mobile devices:** The involvement of multiple parties may create an additional burden for users, due to redirections and IDP selection. In the case of the EU Electronic Identification and Trust Services (eIDAS) federation, for example, users may first have to select the country of their IDP, and then select again a specific IDP within the national scheme if the latter is itself a federation. Browser redirects can be a particular problem with mobile devices and applications due to the lack of Open Authorization (OAuth) use in mobile apps. However, most of these issues are caused by SAML implementations, whereas OpenID Connect (OIDC) is far more effective at providing app-based user experiences.
 - **Mitigation:** Work on enhancements to federation protocols in open forums, such as the Open Identity Foundation, and sharing of best practices by countries working to address these

issues—for example, the **Netherlands'** work on the user experience and user flow to reduce or hide the number of redirections by making changes (such as displaying a blank page instead of flashing different interfaces) to help improve the user experience in such scenarios, especially on mobile devices.

- **Reduced—but not eliminated—risk for 360-degree profiling:** As noted above, communication between the RPs and an IDP in a federation—and particularly those that use a single identifier across RPs—could reveal to the IDP where the individual is conducting a transaction and allow the identity exchange to build a profile of transactions across multiple IP addresses unless additional controls are in place. This is a similar risk to a single IDP model; in a functional ID, IDP market, or decentralized model, this risk is mitigated to some extent, as the IDPs are independent, and the individual can distribute their activity across different IDPs.
 - **Mitigation:** This risk is higher in federation Type 1 due to the use of common identities across IDPs, when compared with Type 2. Implementation of blinding (single, double, or triple) within the identity hub can help mitigate these risks to varying degrees by hiding information from IDPs and RPs.
- **Dependence on IDPs:** Compared with functional ID models, RPs that rely on external IDPs for identity claims, forensics, and record retention may have limited visibility, monitoring, and control over the activities of IDPs. RPs need to be able to ensure that IDPs adopt the requisite processes and practices in identity management that meet the risk or assurance level needed. If an IDP leaves the federated system, the RP must be able to deal with such contingencies.
 - **Mitigation:** Development of a trust framework and adherence to the rules under the framework can mitigate this risk to some extent. In cases where a specific IDP leaves, the continuation of services for RPs and the migration of user identities to a new IDP could be achieved with relative ease in federation Type 1 but would be more complex in federation Type 2, given the lack of a unique identity.
- **Relatively new concept for official ID outside of high-income countries:** Federation for government-recognized digital ID is a relatively new concept in many low- and middle-income countries and has only become common in high-income countries (HICs) in the last 10-15 years. As a result, the understanding and availability of skilled resources on this topic is also not sufficiently available in all countries. Some earlier implementations have also faced growing pains, as in the case of user-redirects, but there has also been significant ongoing work to improve usability aspects for browser redirects—especially in mobile apps—which is essential for the overall success of the federated authentication model.
 - **Mitigation:** The lack of resources can be managed through development of training material in conjunction with end-to-end user journeys and service maps. Independent accessibility assessments and adherence to trust framework rules that relate to usability and accessibility may also alleviate this risk.

Enablers and Preconditions

Based on global experiences, a federated ecosystem may be appropriate to consider in contexts that have the following characteristics:

- **There is a high and increasing demand for digital ID in online services²⁷ at multiple levels of assurance.** Although some ID credentials provided by IDPs in a federated ecosystem could also be used for face-to-face transactions, most implementations of federated ecosystems are intended exclusively for remote, online use. A high volume of transactions is required to sustain a business model for multiple IDPs. For this reason, a federated model may be most appropriate in countries that already have many end-to-end digital services and a growing digital economy. In contexts with a high potential demand for digital ID at various levels of assurance, a federated ecosystem has the potential to offer greater choice and inclusivity over the types of credentials issued than some other models.
- **There is already a strong foundational ID system and/or other authoritative sources that IDPs can use for identity proofing at a high level of assurance.** The existence of high quality, high coverage foundational ID systems or registers—such as civil registration, national ID, or national population register systems—or other authoritative sources, provides an enabling environment for other IDPs to issue identity credentials with low onboarding costs. For multiple IDPs to sustainably provide services in the federated system, apart from demand for their services, enrollment and identity proofing processes should be efficient in terms of cost, time, and complexity for both individuals and IDPs. In many EU countries, for example, banks are well equipped to join a federation as IDPs because their customers are already onboarded to financial services via foundational systems for internet banking and can seamlessly use their banking ID to access other services.
- **There are already multiple IDPs (including service providers) that provide digital credentials.** In some countries, a variety of service providers and agencies—for example, the national ID, tax administration, social programs, or election administration—as well as banks and other firms, may already provide digital ID credentials. In such cases, a core set of stakeholders already exists, and developing common standards for federation (or decentralized ID) may be faster and/or more feasible than creating a new digital ID system driven by a single provider.
- **There is a need to develop a system that allows for cross-border interoperability and mutual recognition.** Federation enables RPs to service users from different identity silos or jurisdictions. This is especially useful for cross-border service access when users may have digital IDs issued by other countries, as evidenced by the EU eIDAS federation. This can also be useful in federal countries where individual states are often the identity providers.

²⁷ Increased acceptance and use of private sector digital services similar to that of Grab and Gojek in Southeast Asia, also have the potential to drive demand for similarly easy to use digital services in the public sector.

Success Factors

While the previously discussed conditions are conducive to federated ecosystems, factors that are important for successful implementation and sustainability over time include:

- **Demand-driven use cases for digital identity services:** As noted above, there should be sufficient need and capacity for identity assertions in a digital environment to drive demand for IDP services. The utility of digital identity depends on compelling, impactful use cases and services—in other words, frequently used online services that require identity verification/authentication for their business processes—without these, demand for IDP services will be low. In some cases, online services may exist but have low usage levels due to poor internet penetration and availability for a substantial portion of the population, low levels of digital literacy or awareness of online services, or services that are not customer friendly and are difficult to use. In the case of cross-border federation, the need for people to access foreign services should also be carefully assessed. Focusing on the real needs of people and other uses, as well as ensuring that the application of digital identity addresses those needs in a way that is inclusive, secure and does not impose additional cost or inconvenience, is essential.
- **A clear understanding and application of required levels of assurance:** An assessment of the required level of assurance needed for the online services can inform the role of different IDPs in the federated system. This is essential for developing the trust framework but also for enduring demand. For example, the number of services that require a higher level of assurance provided by a government-recognized digital ID may be few or limited to infrequent transactions, such as purchasing property, or specialized users.
- **Strong trust framework development, administration, and oversight:** Development of a trust framework and its administration is a complex task, yet essential to ensure smooth operation of the federation and trusted identity services. Maintenance and change requests to the technical specifications and attributes profiles are an ongoing task that will ensure the long-term success and relevance of the federation. Data protection laws and subsequent implementation through an independent data protection authority are also essential to mitigate risks associated with processing personal data and potential misuse or data breaches.
- **A sustainable business model that is attractive to IDPs but does not create barriers to adoption or use by people and RPs:** Financial models and fees should be based on various factors, including the volume of transactions, types of IDPs and RPs (public or private) and the specific services, the cost of identity management to IDP, the savings to RPs by using IDP services in the federated model, the costs incurred by the provider of the exchange, and the trust framework and federation administration activities. In some cases, government IDPs may assume some of the costs to provide basic identification services as a free public service.²⁸

²⁸ See, for example, “ID4D Practitioner Note on Identity Authentication and Verification Fees: Overview of Current Practices.” <http://documents1.worldbank.org/curated/en/945201555946417898/pdf/Identity-Authentication-and-Verification-Fees-Overview-of-Current-Practices.pdf>.

Conclusion

Federated ecosystems present a new model for countries to develop government-recognized digital ID services, either in addition to existing digital ID provided by foundational systems (in the case of the Type 1 model) or in place of it (in the case of Type 2). For countries with high demand for online authentication and verification at various levels of assurance, federation has the potential to increase the availability and scalability of these services and offer increased choice to users and relying parties. When designed with privacy-protecting features and architecture, it also offers multiple benefits, including reducing the potential of a single identity provider (IDP) to gain a full picture of an individual's transactions.

At the same time, federated ecosystems require strong existing forms of official identification with wide coverage to provide sufficient identity proofing for IDPs in an online environment, as well as significant governance and technical capacity to design, run, and provide oversight for the federation. As such, it may be a better fit for countries well on their way to digital transformation, rather than those just beginning to move online. Countries implementing single IDPs models can plan for a potential future federated model by focusing first on achieving a trusted and inclusive digital ID to meet initial demands for both remote and in-person authentication, then scaling to increase IDPs through a federation as the demand for online services increases.

As decentralized models gain traction with the new EU digital wallet ecosystems, these may also provide an alternative digital authentication layer that can build on existing systems while providing users with more choice and control. Future work will explore these models and their benefits compared with federated and single IDP models in more detail.

id4d.worldbank.org

