

Human-Centric Digital Identity

Overview & State of Play

Gail Hodges

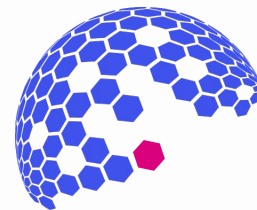
Executive Director, OpenID Foundation

director@oidf.org





Our **mission** is to lead the global community
in creating identity standards that are **secure**,
interoperable, and **privacy-preserving**.



Billions of users
Millions of applications
since 2007

login open finance open health digital ID shared signals

400 Members + Board thought leaders

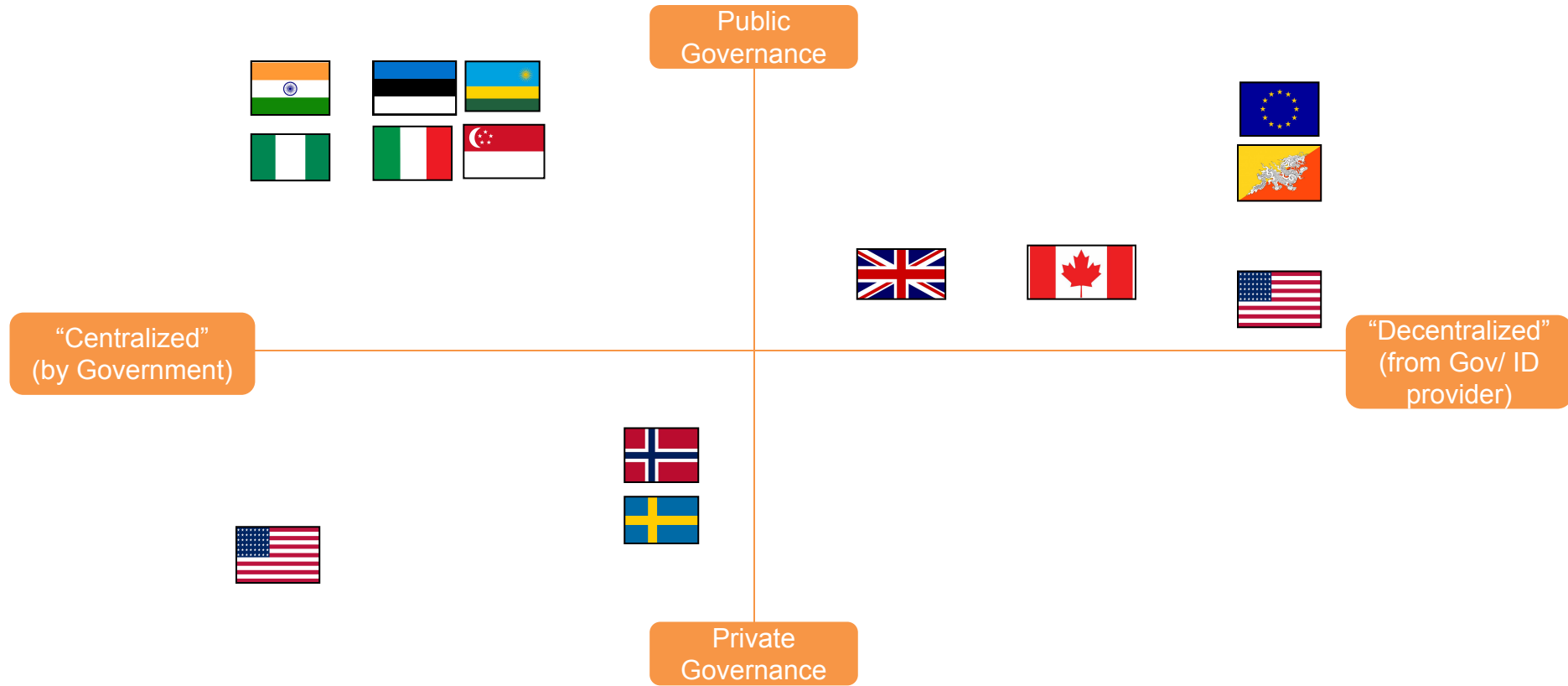


*the Foundation also has 4 community-elected representatives in addition to 2 Corporate-member
elected representative on the Board of Directors*

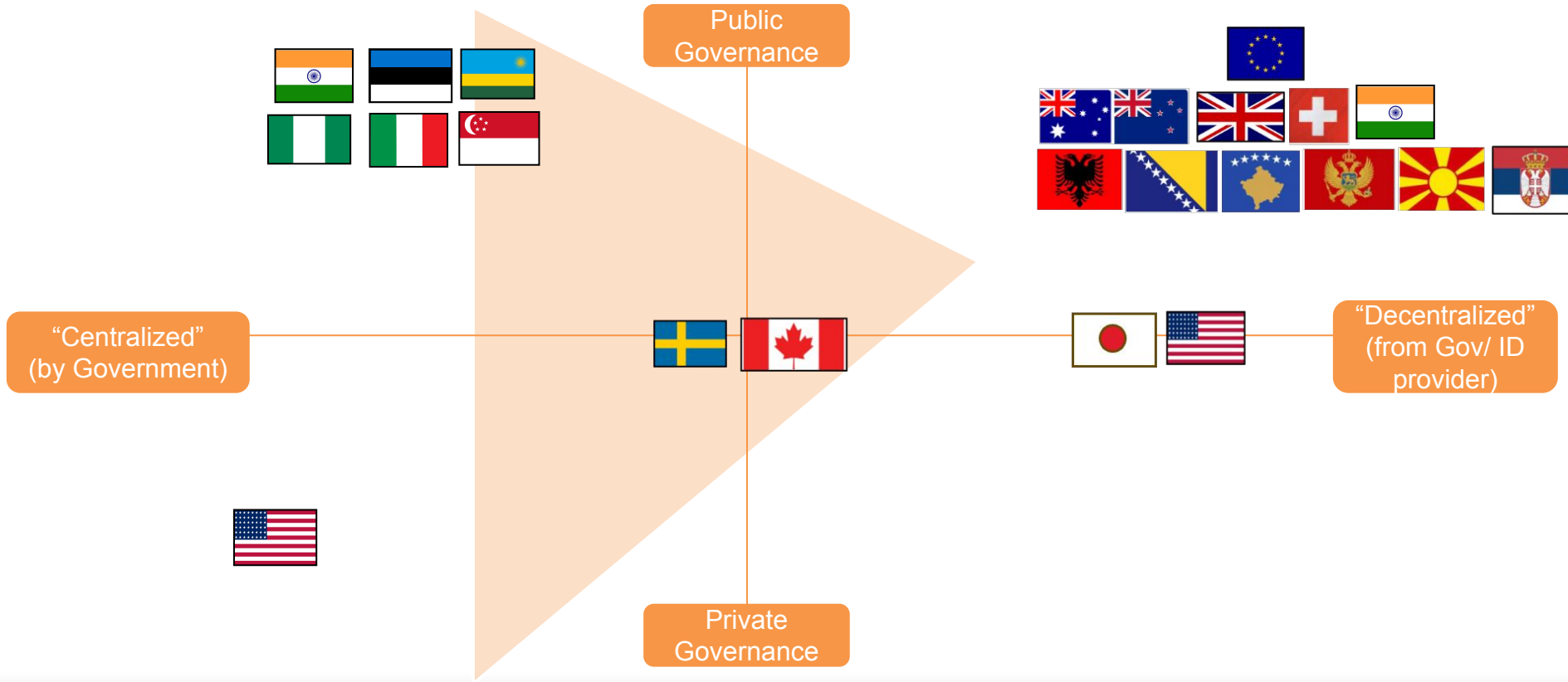
Government Partners



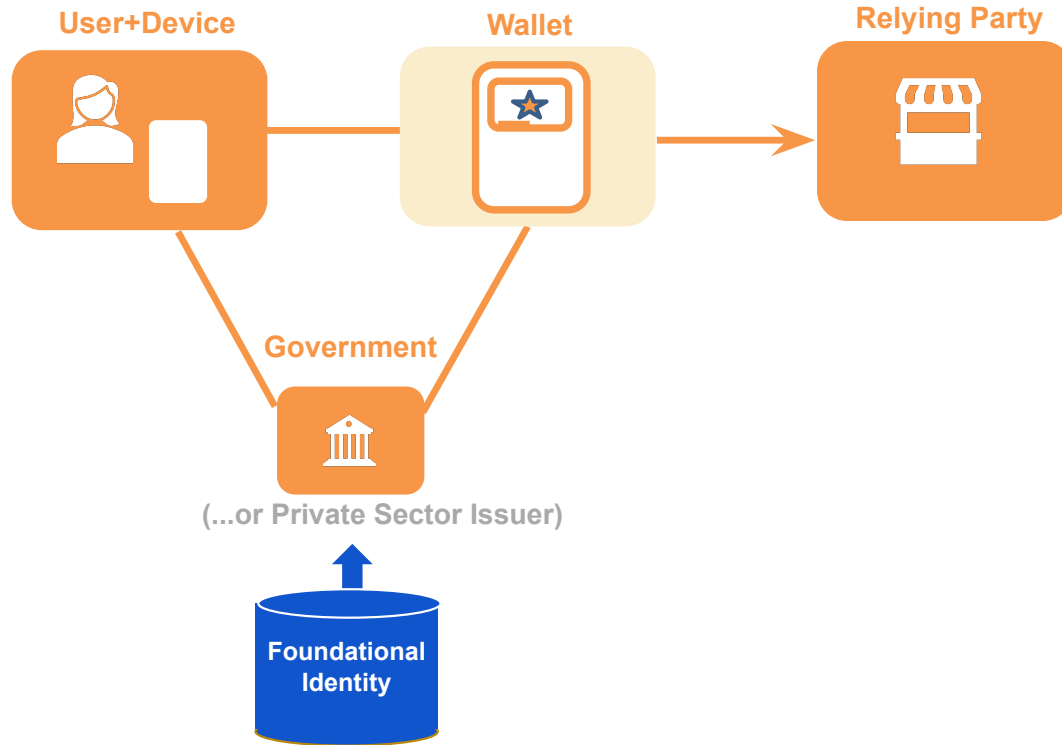
In 2023, most models were centralized, VC models emerging



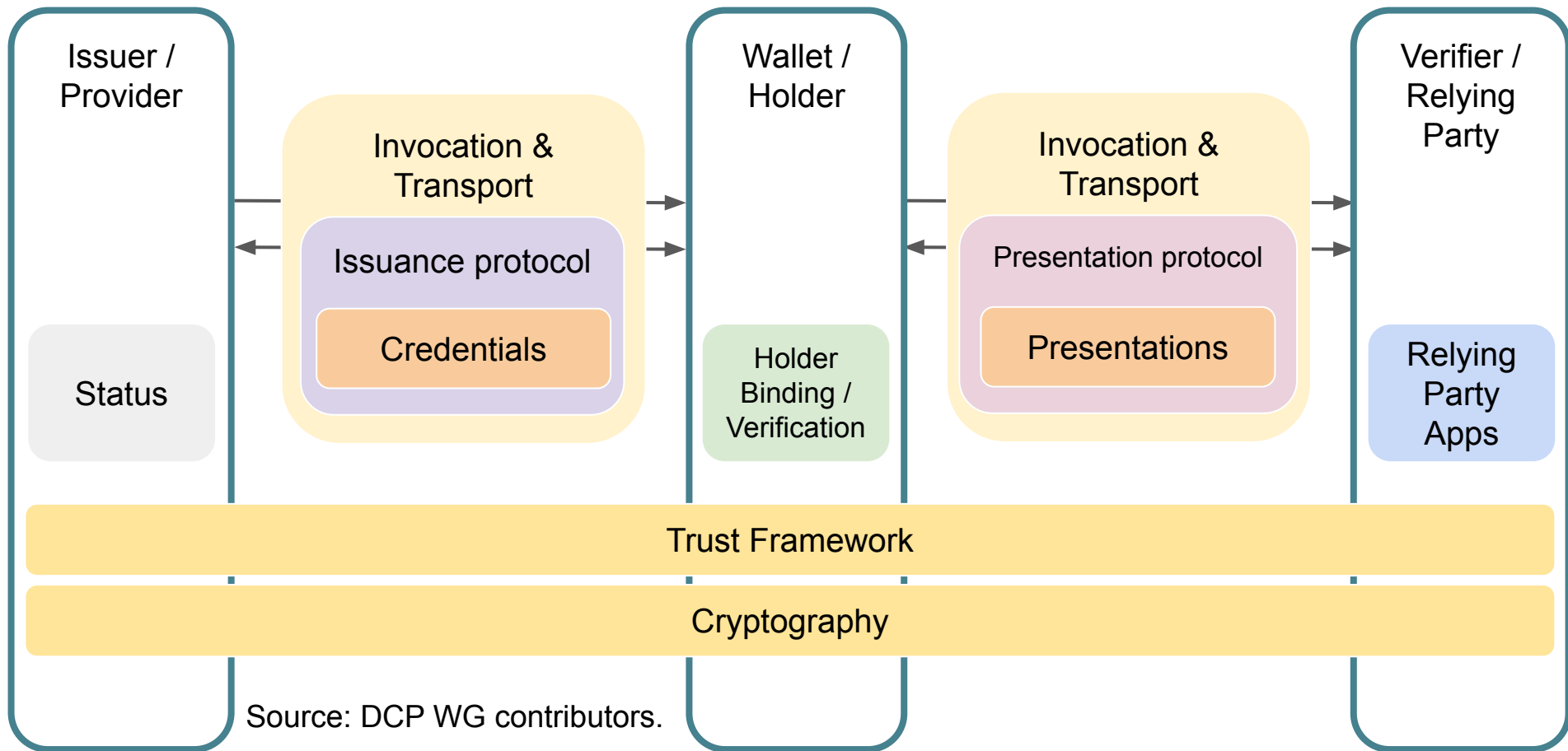
In 2026, more countries building on foundational identity with VCs



Verifiable Credential ecosystems often leverage foundational identity infrastructure



The Building Blocks for the Digital Credentials Stack



What to choose? How do I build my MVP?

Layer / Function	Standards / Choices Available					
Issuance Protocol	OpenID4VCI	ISO 23220-3	DIDComm	...	...	...
Credential Formats	W3C VCDM	SD-JWT-VC	ISO mDoc	AnonCreds	...	...
Presentation Flow	OpenID4VP	DIDComm	mDoc	QR		
Invocation	W3C DC API	QR Code	Deep Link	CHAPI	NFC (mDoc)	...
Transport	BLE (mDoc)	NFC (CTAP)	Camera(QR)	HTTP	BLE (OpenID4VP)	
Trust Framework	X.509 / Trust Lists	OIDF Federation	vLEI	DID	...	...
Status	IETF Status List		W3C Bitstring Status List		...	...

What to choose?

Layer / Function	Standards / Choices Available					
Issuance Protocol	OpenID4VCI	ISO 23220-3	DIDComm	...	...	
Credential Formats	W3C VCDM	SD-JWT-VC	ISO mDoc	AnonCreds	...	...
Presentation Flow	OpenID4VP	DIDComm	mDoc	QR		...
Invocation	W3C DC API	QR Code	Deep Link	CHAPI	NFC (mDoc)	
Transport	BLE (mDoc)	NFC (CTAP)	Camera(QR)	HTTP	BLE (OpenID4VP)	...
Trust Framework	X.509 / Trust Lists	OIDF Federation	vLEI	DID	...	
Credentials Status	IETF Status List	W3C Bitstring Status List		...	...	...

OIDF HAIP
Profile

Trusted by the EU and their 27 member states –
European Union Digital Identity (EUDI)
(Western Balkans, other countries emulating)

New News & Resources

- **VC/ Wallet Conformance (OIDF + linked specs: DC API, mdoc, SD-JWT, OIDC/FAPI)**
 - Open source tests available from OIDF, optional self-certification
 - New accreditation program for ecosystems (first MOU signatories: FIDO, Kantara, FIME, Raidiam, TrustID, Raidiam, Bixe Labs)
 - OIDF working with European Commission, NIST, Australian government, California on conformance
- **Specs**
 - ISO/OIDF due diligence on a joint WG to converge protocols to consider a single, presentation protocol
 - OpenID4VP, VCI, HAIP 1.1/1.2 versions backward compatible, added features
- **Adoption**
 - NIST NCCoE SP1800-42A on mDL “accelerating financial service adoption” published, informed by 11 interop events and eKYC reports
 - Four jurisdictions aligning on how to deliver FI compliance via protocols and metadata (level of assurance/proofing, authentication type) = trust framework by default
 - HL7/FHIR exploring role of VCs in Health data access

Resources: More material in deck that will be distributed

Resources: Gail Hodges – director@oidf.org

Source	Audience	Content	Link
OECD Digital Identity Recommendations (2023)	Policy leaders	Policy paper	https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491
UNDP DPI Safeguards	Policy leaders	Policy paper	https://www.dpi-safeguards.org/
FATF Guidelines (2020)	Policy leaders	Policy paper	https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity-Executive-Summary.pdf
EIDAS 2.0 resources	Lead architects & policy leaders	EU policy & architecture Architecture Reference Framework EC Launchpad event & resources Implementing Acts	https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation https://eudi.dev/ https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDI%20DIGITAL%20IDENTITY%20WALLET/pages/924975727/EUDI+Wallets+Launchpad https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16114-European-Digital-Identity-Wallet-electronic-attestations-of-attributes-update_en https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16113-European-Digital-Identity-Wallet-registration-of-wallet-relying-parties-update_en https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16112-European-Digital-Identity-Wallet-standards-and-technical-specifications-update_en
US NIST resources	Lead architects & policy leaders	SP 800-63-4 Digital identity recommendations NIST NCCoE Digital Identity project ("open a bank account", "gov access")	https://pages.nist.gov/800-63-4/ https://www.nccoe.nist.gov/projects/digital-identities-mdl
OIDF Work Group and Community Groups	Architects, thought leaders	Instructions to take part (no costs) Specs, tests, best practices	openid.net Questions: director@oidf.org
OIDF's EU Resource Hub	Lead architects	Specifications, open source tests, resources	https://openid.net/eudiw_community_page/
OIDF Ecosystem Support CG*	Lead architects & policy leaders	"Office hours" for ecosystems e.g. reference architecture, due diligence	https://openid.net/cg/ecosystem-support-community-group/
SIDI Hub: Cross Border Interoperability.	Lead architects & policy leaders	Projects and use cases to close cross border interoperability gaps	https://sidi-hub.community/

Digital Identity Landscape

Gail Hodges
Executive Director, OpenID Foundation
director@openid.org



“Human Centric Digital Identity” Whitepaper

Human-Centric Digital Identity:

for Government Officials

v1.1

Lead Editors: Elizabeth Garber, Mark Haine
October 13, 2023

Citation:

Garber, E. and Haine, M. (eds) “Human-Centric Digital Identity: for Government Officials
OpenID Foundation, (September 25, 2023)

Date	Revision
October 13, 2023	V1.1 includes additional co-brand partners and MyData Global added to Appendix D
September 25, 2023	Final v1 version published
September 18, 2023	Public comments addressed and accepted. Pre-editorial. Graphics and tables will be formatted.
July 07, 2023	Publication of Public Comment draft
April 14, 2023	Expert Review

1





Everyone
has the right to recognition
everywhere
as a person before the law

Article 6 of the Universal Declaration on Human Rights (1948)

Core UN Human Rights Frameworks

referenced in this document

Convention relating to the Status of Refugees
1951

Convention relating to the Status of Stateless Persons
1954

Declaration on the Rights of the Child
1959

International Covenant on Civil and Political Rights
1966

International Convention on the Protection of the Rights of
all Migrant Workers and Members of their Families
1990

Underpinning Role of Legal Identity

across categories of Human Rights

Right to Social Insurance
Right to Healthcare

Right to Self-
Determination

Right to Earn
a Living

Right to Privacy
Right to Own Property



Right to Birth
Registration

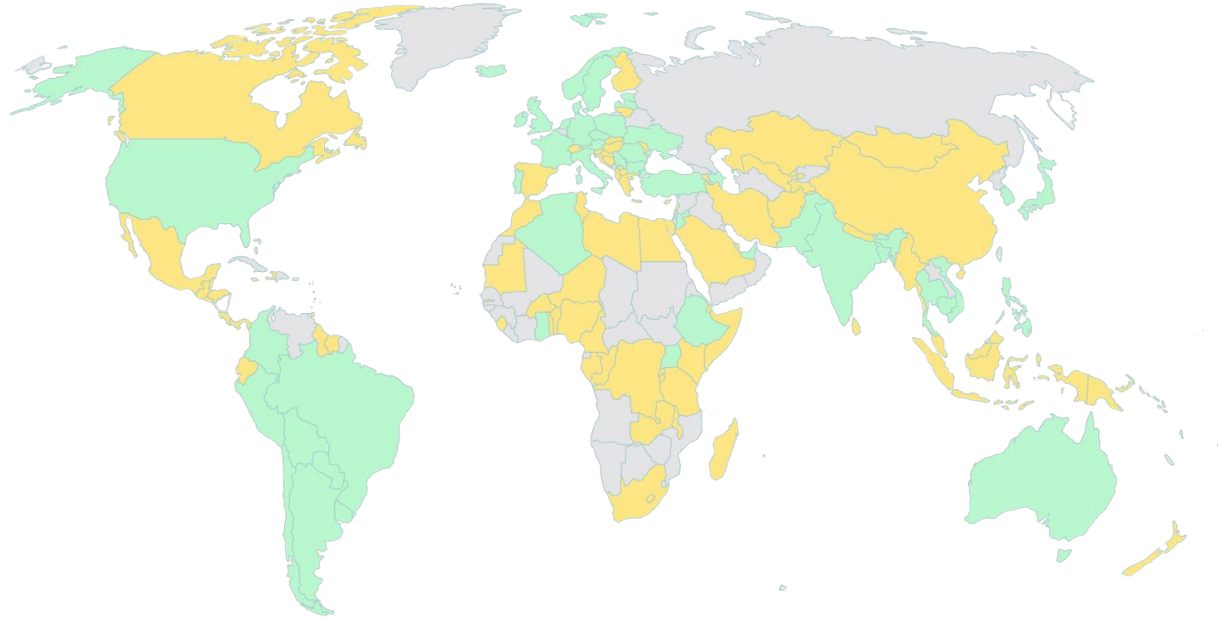
Right to
Education

Right to Leave
Right to Return

Right to Start
a Family

60+ Countries treat digital identity as critical

“Digital Public Infrastructure”



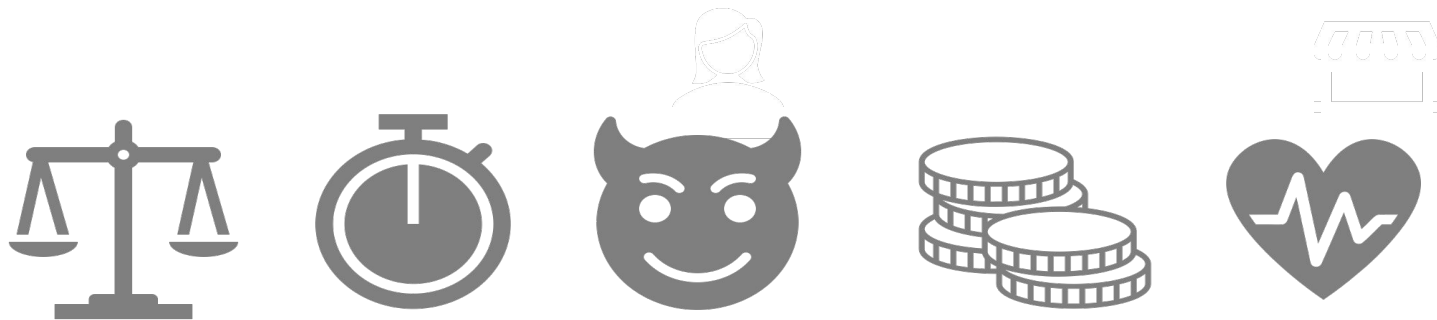
Source: [DPlmap.org](https://dplmap.org);

yellow = work in progress and green is live

Digital ID System implementation status by country



Why are 60+ Countries pursuing Digital Identity?



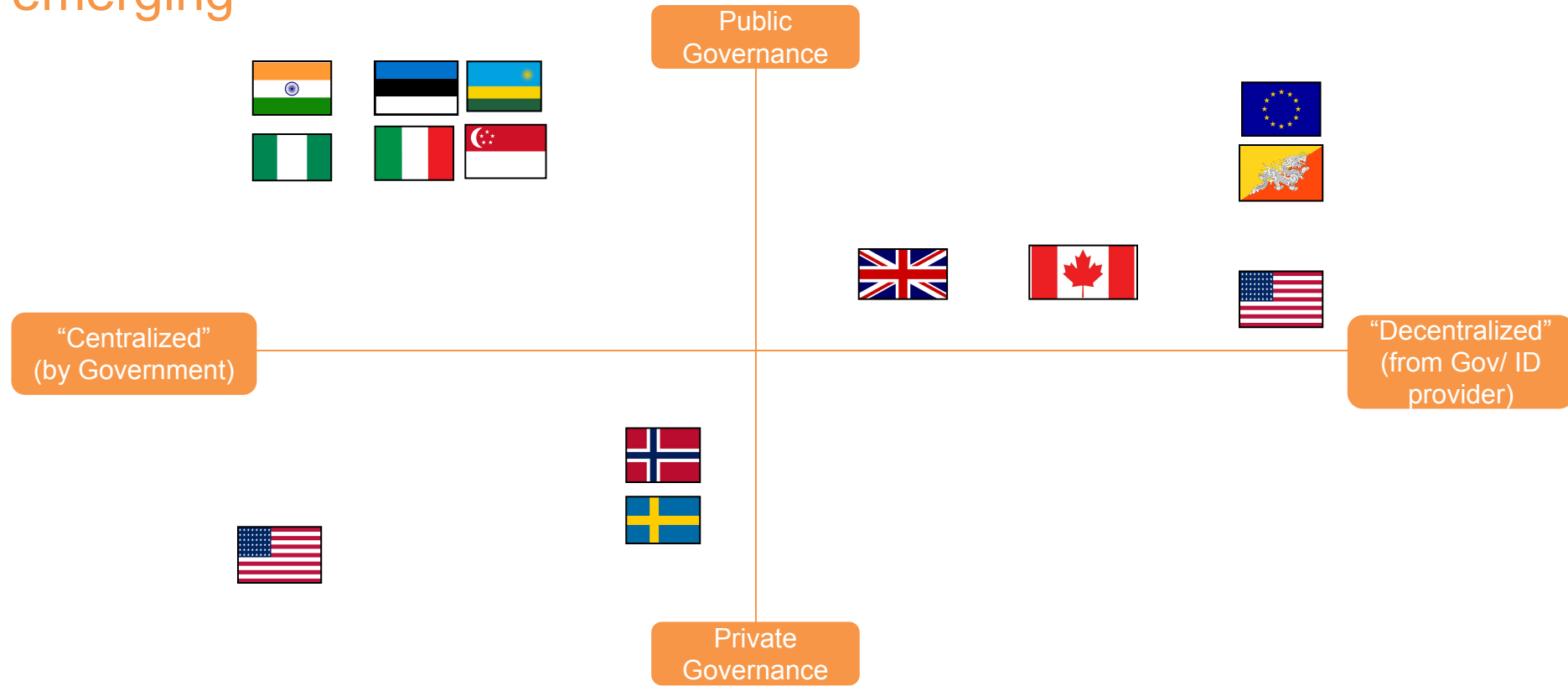
Countries share similar core problems and use cases: equity, inclusion, GDP growth, jobs, cross border trade, health, saving time and money, averting cybercrime.

Centralized & Decentralized Identity

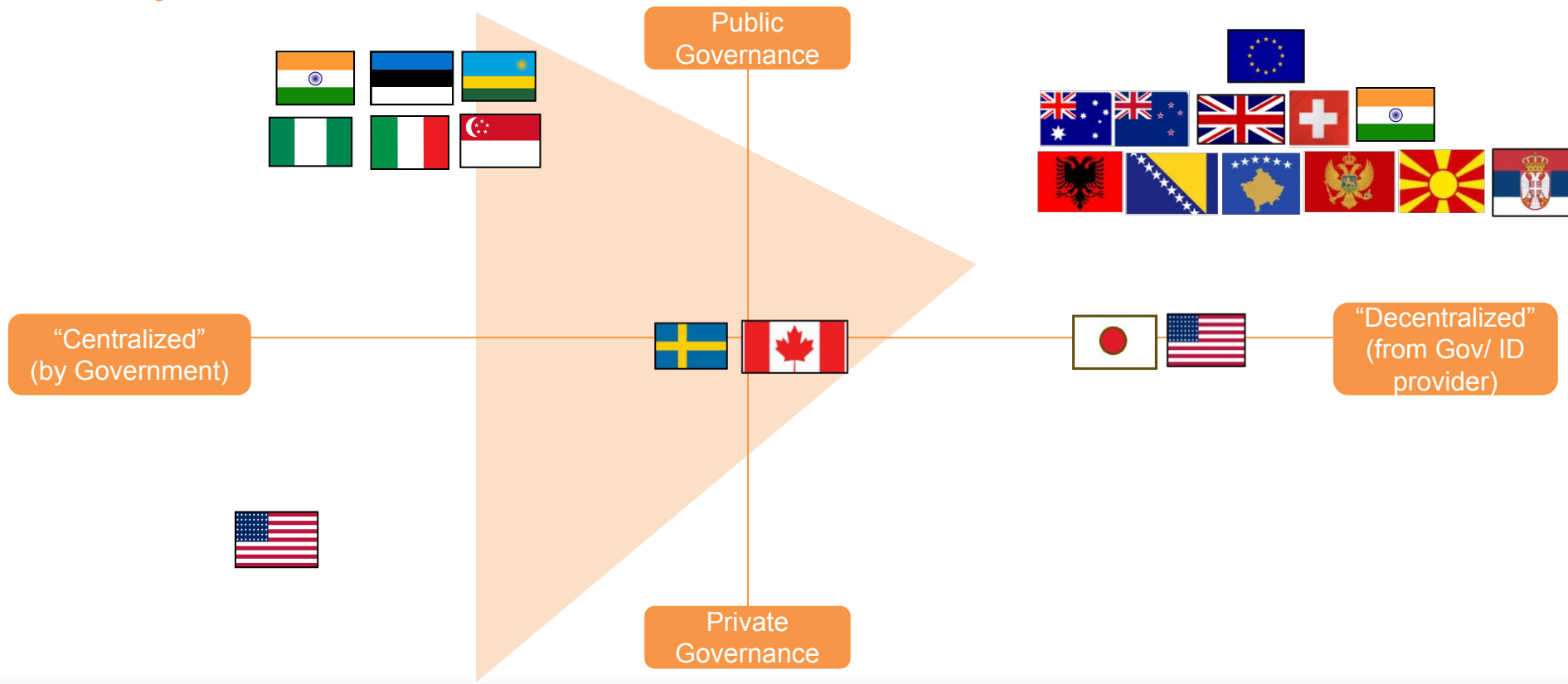


- What makes them different?
 - Cryptographic signatures
 - Privacy capabilities
 - Tamper detection by default
 - Instant verification
 - No need to call the issuer
 - Option to operate offline
 - Option to have 1 or bundle credentials

In 2023, most models were centralized with decentralized models emerging

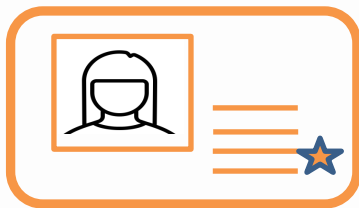


In 2026, we see a pattern of countries building on foundational identity infrastructure to issue Verifiable Credentials



Verifiable Credentials

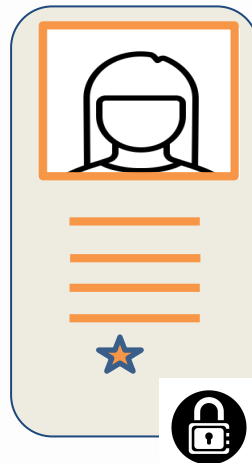
What are they?



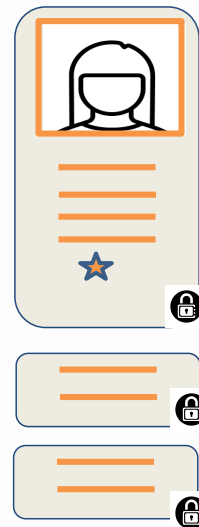
Verifiable credentials can be:



Regulated & unregulated use cases



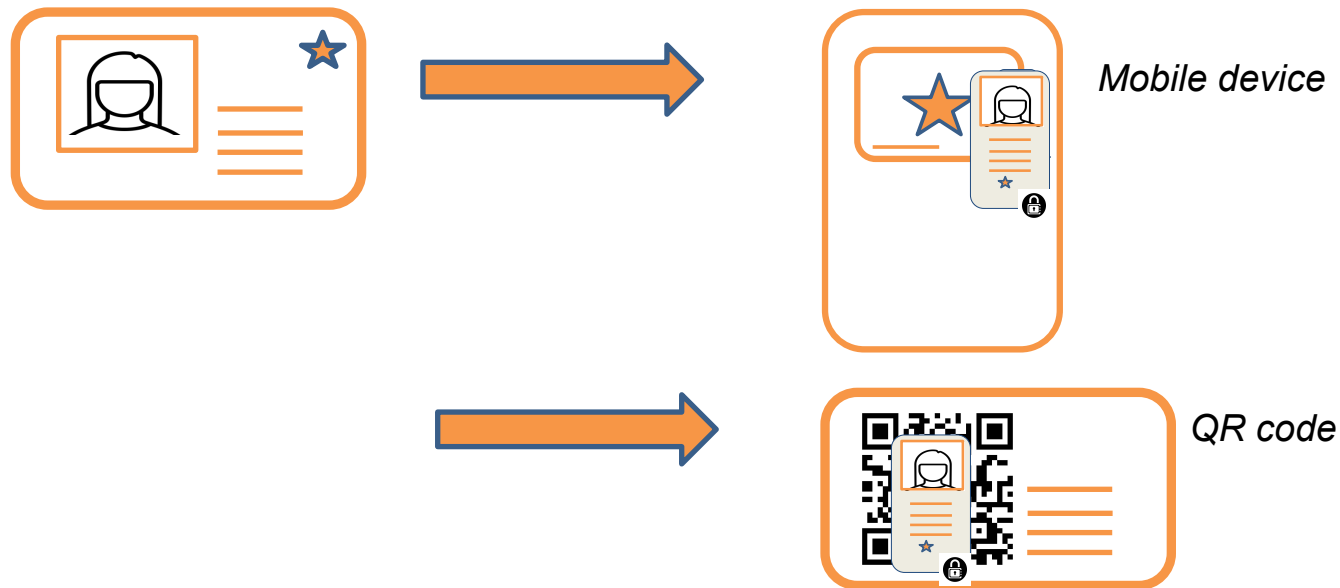
Set of data
cryptographically bound



Credentials can be
bundled together

★ = Evidence of regulatory conformance

~43 countries issuing or plan to issue Verifiable Credentials

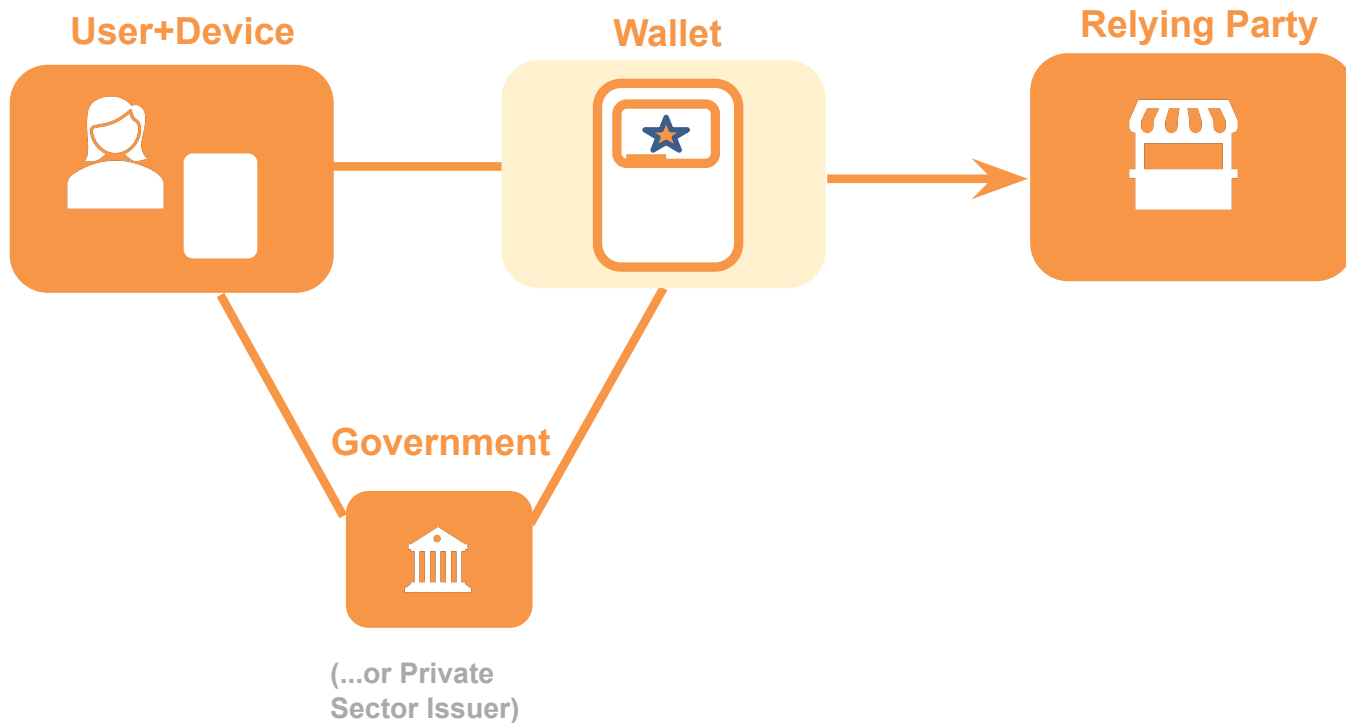


Live today in US, Japan, UK, India, Switzerland (beta). EU on track to launch by end 2026, Western Balkans to follow Global standards and open source providers are supporting jurisdiction deployments. High and lower income country deployments concurrently.

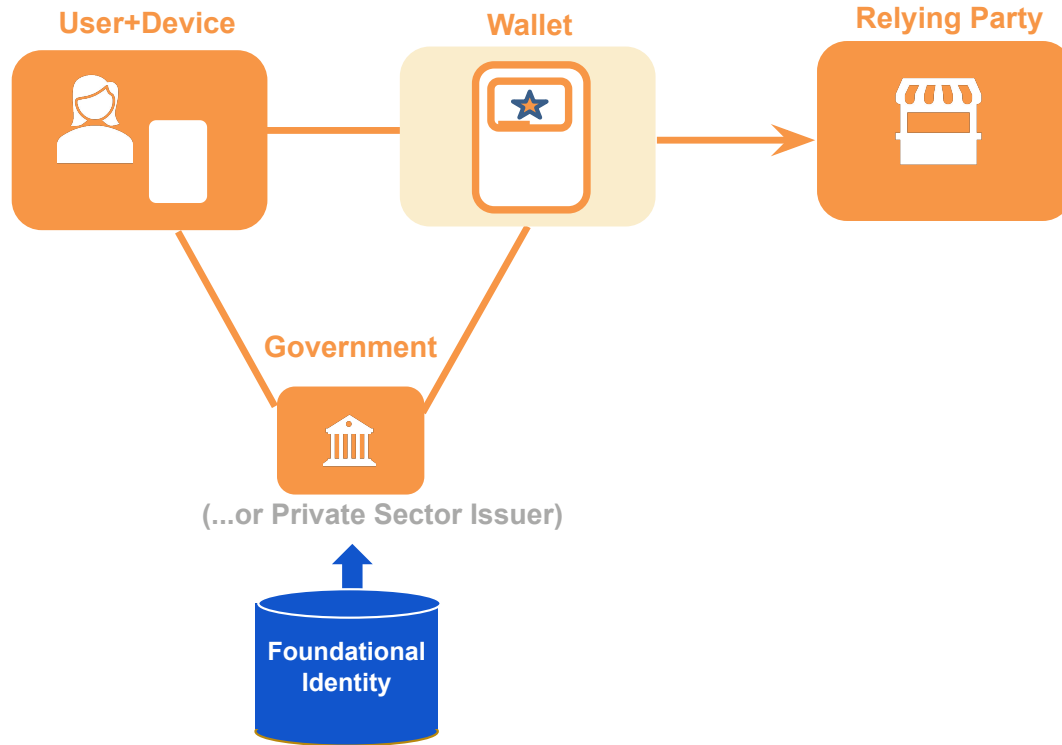
User Control and Privacy Concerns led to Interest in “Decentralized” Models



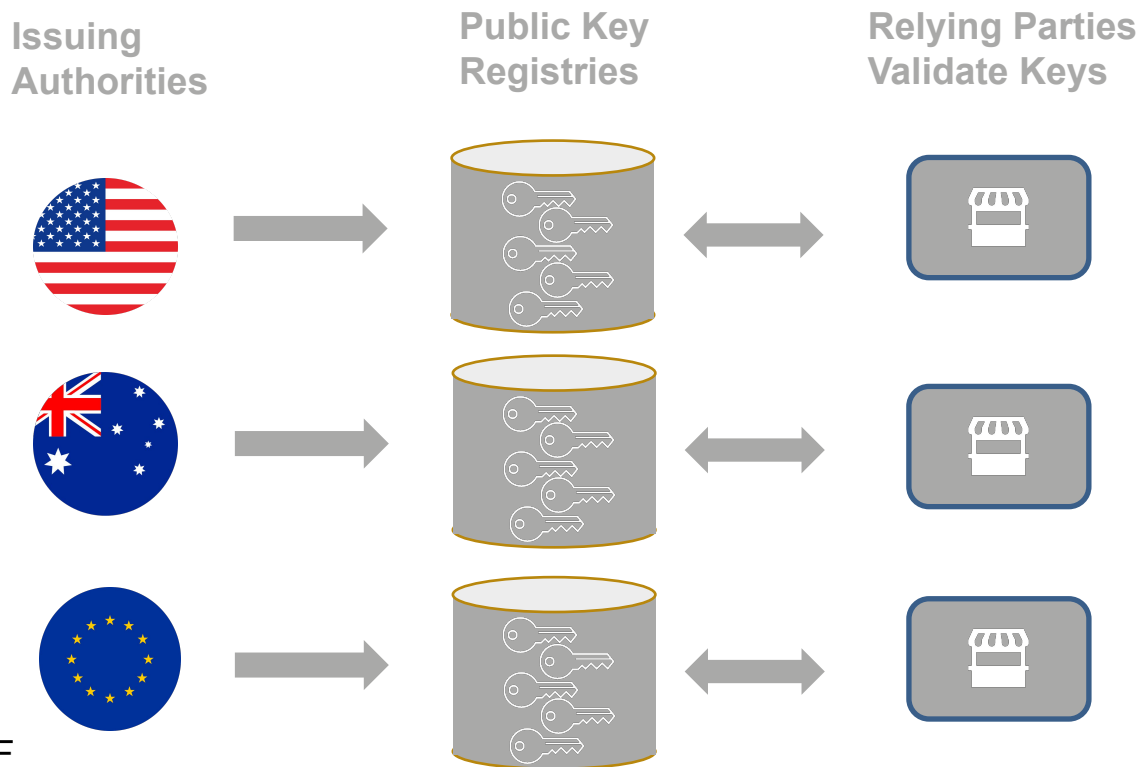
Wallets & Verifiable Credentials that Have the Potential to be Privacy Preserving by Default



Verifiable Credential ecosystems often leverage foundational identity infrastructure



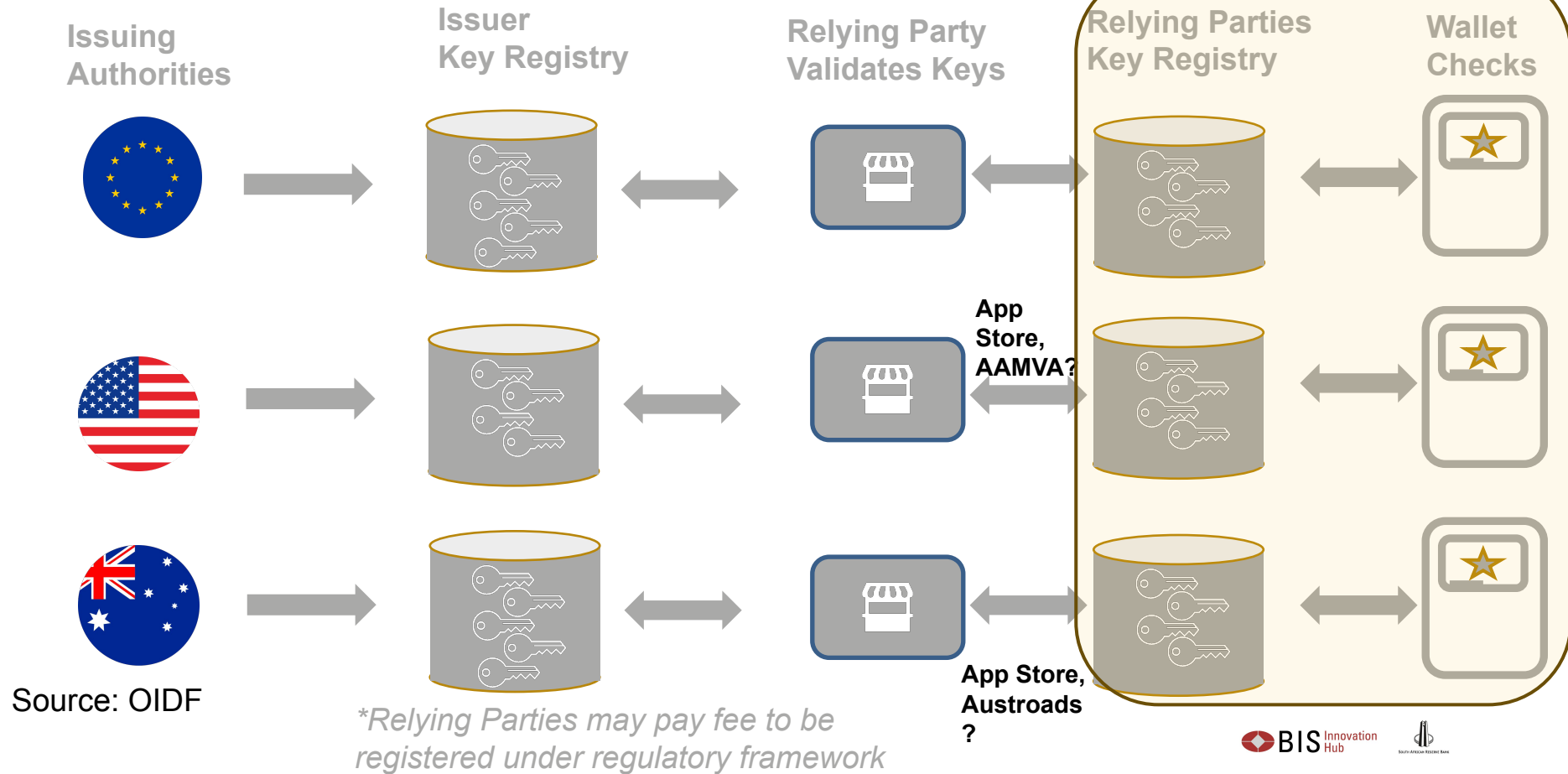
Issuer sends public key to a central registry



Source: ODF

**Relying Parties may pay fee to be registered under regulatory framework*

RP Registration - Emerging



Why are 60+ Countries pursuing Digital Identity?

Accelerating cybercrime



Ensuring resiliency in our existing systems is critical, and new verifiable credential ecosystems introduce new risks... but also new tools to mitigate attacks

Security Harms from Weak Identity Infrastructure

Threat map

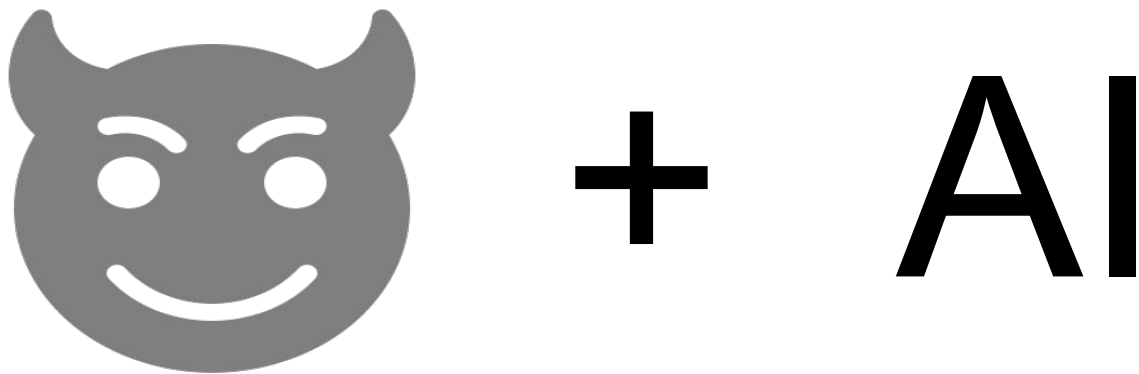
- Americas
- Asia & Pacific
- Europe
- Middle East & Africa

Microsoft Digital Defense Report (2025)

<https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/>

\$1-10 Trillion

Costs of Global Cybercrime



*...can high assurance, verifiable
credentials help avert these risks?*

Resources : Gail Hodges – director@oidf.org

Source	Audience	Content	Link
OECD Digital Identity Recommendations (2023)	Policy leaders	Policy paper	https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491
UNDP DPI Safeguards	Policy leaders	Policy paper	https://www.dpi-safeguards.org/
FATF Guidelines (2020)	Policy leaders	Policy paper	https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity-Executive-Summary.pdf
EIDAS 2.0 resources	Lead architects & policy leaders	EU policy & architecture Architecture Reference Framework EC Launchpad event & resources Implementing Acts	https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation https://eudi.dev/ https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDI+DIGITAL+IDENTITY+WALLET/pages/924975727/EUDI+Wallets+Launchpad https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16114-European-Digital-Identity-Wallet-electronic-attestations-of-attributes-update_en https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16113-European-Digital-Identity-Wallet-registration-of-wallet-relying-parties-update_en https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16112-European-Digital-Identity-Wallet-standards-and-technical-specifications-update_en
US NIST resources	Lead architects & policy leaders	SP 800-63-4 Digital identity recommendations NIST NCCoE Digital Identity project ("open a bank account", "gov access")	https://pages.nist.gov/800-63-4/ https://www.nccoe.nist.gov/projects/digital-identities-mdi
OIDF Work Group and Community Groups	Architects, thought leaders	Instructions to take part (no costs) Specs, tests, best practices	openid.net Questions: director@oidf.org
OIDF's EU Resource Hub	Lead architects	Specifications, open source tests, resources	https://openid.net/eudiw_community_page/
OIDF Ecosystem Support CG*	Lead architects & policy leaders	"Office hours" for ecosystems e.g. reference architecture, due diligence	https://openid.net/cg/ecosystem-support-community-group/
SIDI Hub: Cross Border Interoperability.	Lead architects & policy leaders	Projects and use cases to close cross border interoperability gaps	https://sidi-hub.community/

Implementer Experience & Best Practices from the “front lines”

Oliver Terbu



Start With the UX, Not the Protocol

Key design decisions:

- Who initiates the flow?
 - Issuer?
 - Wallet?
 - Verifier?
- Same-device or cross-device?
- Browser-based or native app?
- Synchronous or asynchronous issuance?
- Kiosk / proximity scenarios?

These choices directly affect:

- Security posture
- Drop-off rates
- Accessibility
- Operational complexity

Design the journey first. Then choose the protocol.

Successful implementations start with the real user interaction.

Security Is a Function of Architecture

Examples:

- Cross-device flows → higher phishing surface
- Same-device flows → stronger session binding
- Browser-based issuance → different threat model than native-to-native

Critical decisions:

- Are credentials device-bound?
- Where are keys stored? (platform key store / secure enclave)
- Is hardware-backed protection required?
- Are platform attestations necessary?

Security must be:

- Proportionate to credential value
- Aligned with regulatory expectations
- Usable in practice

Avoid both under-securing and over-engineering

Different UX flows create different risk profiles

Trust Is More Than a Valid Signature

Verification must check:

1. Cryptographic validity
2. Issuer authorisation under a trust framework

Questions to resolve:

- Is there an existing PKI or trust list?
- Is the issuer accredited for this credential type?
- What assurance level applies?
- Is revocation/status checking required?

Trust is:

- Technical (cryptography, security controls, protocols etc.)
- Institutional (governance, accreditation)

Both must align

Build for Interoperability & Start Small

Avoid fragmentation:

- Choose a stack that is already widely adopted
- Ensure open-source or professional SDK support
- Prefer profiles that have undergone security review

Start with a simple MVP use case comprising:

- Issuer → Web app
- Verifier → Web app
- Wallet → Mobile app

A myriad of open-source products available that allow branding

And:

- Participate in interoperability events
- Use official conformance test suites

This helps with detecting bugs early

**Interoperability is not automatic
it must be validated.**

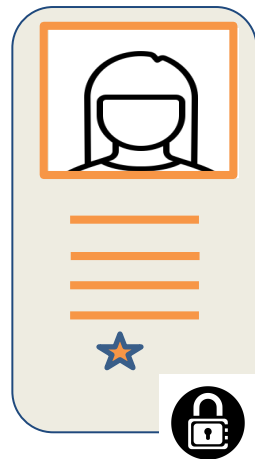
What are the Super Powers of Verifiable Credentials? Who does what?

Oliver Terbu



Verifiable credentials are digitally signed, tamper-evident digital statements

- They allow someone to prove ...
 - Identity
 - Age
 - Qualification
 - Income
 - Affiliation
- What makes them different?
 - Cryptographic signatures
 - Tamper detection by default
 - Instant verification
 - No need to call the issuer – “no phone home”
 - Option to operate offline



The authenticity is embedded in the credential itself.
Trust becomes deterministic, not probabilistic.

Verifiable credentials invert the traditional trust model

Instead of ...

- Asking a central authority each time
- Uploading full documents
- Exposing excessive personal data

Privacy improves because less data is shared and no central party is involved when data is shared.

Trust moves with the data - not locked inside central systems.

They enable ...

- Direct presentation from the Holder to the Relying Party
- Independent cryptographic verification
 - Issuer authenticity
 - Device binding
 - Revocation and status checks
- Selective disclosure (e.g. "name" without revealing "birthdate")
- Holder control
- Reduced data exposure
- Zero-Knowledge proofs (e.g. prove "over-18" without revealing "birthdate")

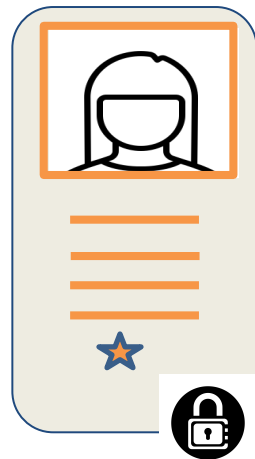
A verifiable credential is a digitally signed container of claims about a subject issued by an issuer to a holder

It includes ...

- **Issuer** (who issued it)
- **Subject** (who it is about)
- **Type** (what type of attestation)
- **Claims** (what is being asserted)
- **Digital signature** (cryptographic proof) from the issuer
- **Optional device keys** of the holder

Example:

- **Issuer:** Ministry of Transport
- **Subject:** Alice
- **Type:** mobile Driving Licence
- **Claims:**
 - Date of birth: 1995-04-12
 - Licence class: B
 - Expiry: 2029-06-01



A Presentation is what the Holder shares with a Verifier

It can ...

- Contain **one or more Verifiable Digital Credentials**
- Contain **selected claims only**
- Be **bound to a verification request** (challenge/nonce-response)
- **Digital signature** (cryptographic proof) from the holder

Example:

- Instead of sharing full driving license → share “over 18: Yes”
- Instead of full diploma → share “Degree awarded: Yes”

The presentation proves:

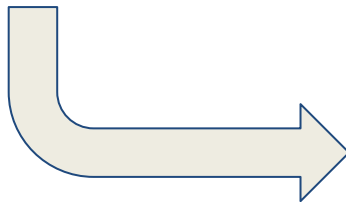
- The presentation is authentic
- It has not been altered
- The holder controls it

A holder is typically realized
via a mobile wallet
application that can securely
store cryptographic keys

Example: Verifiable credential in the SD-JWT VC format

```
{
  "vct": "https://credentials.example.com/identity_credential",
  "given_name": "John",
  "family_name": "Doe",
  "email": "johndoe@example.com",
  "phone_number": "+1-202-555-0101",
  "address": {
    "street_address": "123 Main St",
    "locality": "Anytown",
    "region": "Anystate",
    "country": "US"
  },
  "birthdate": "1940-01-01",
  "is_over_18": true,
  "is_over_21": true,
  "is_over_65": true
}
```

unsecured payload



```
{
  "_sd": [
    "09vKrJM0lyTWm0sjpu_pd0BVBQ2M1y3KhpH515nXkpY",
    "2rsjGbaC0ky8mT0pJrPioWTq0_daw1sX76poUlgCwbI",
    "Ek08dhW0dHEJbvUHLE_VCeuC9uREL0ielZhh7XbUTtA",
    "lDzIKeiZdDwpqpK6ZfbyphFvz5FgnWa-sN6wqQXCiw",
    "JzYjH4svliH0R3PyEMfeZu6Jt69u5qehZo7F7EPYlSE",
    "PorFbpKuVu6xymJagvkFsFXAbRoc2JGLAU2BA4o7cI",
    "TGf4oLbgwd5JQaHyKVQZU9UdGE0w5rtDsrZzfUaomLo",
    "jdrTE8YcbY4EifugihiAe_BPekxJQZICeiUQwY9QqxI",
    "jsu9yVulwQQlhFlM_3JlzMASFzgLhQG0DpfayQwLUK4"
  ],
  "iss": "https://example.com/issuer",
  "iat": 1683000000,
  "exp": 1883000000,
  "vct": "https://credentials.example.com/identity_credential",
  "_sd_alg": "sha-256",
  "cnf": {
    "jwk": {
      "kty": "EC",
      "crv": "P-256",
      "x": "TCAER19Zvu30HF4j4W4vfSVoHIP1ILiLdls7vCeGemc",
      "y": "ZxjiWWbZMQGHVWVKVQ4hbSIrsVfuecCE6t4jT9F2HZQ"
    }
  }
}
```

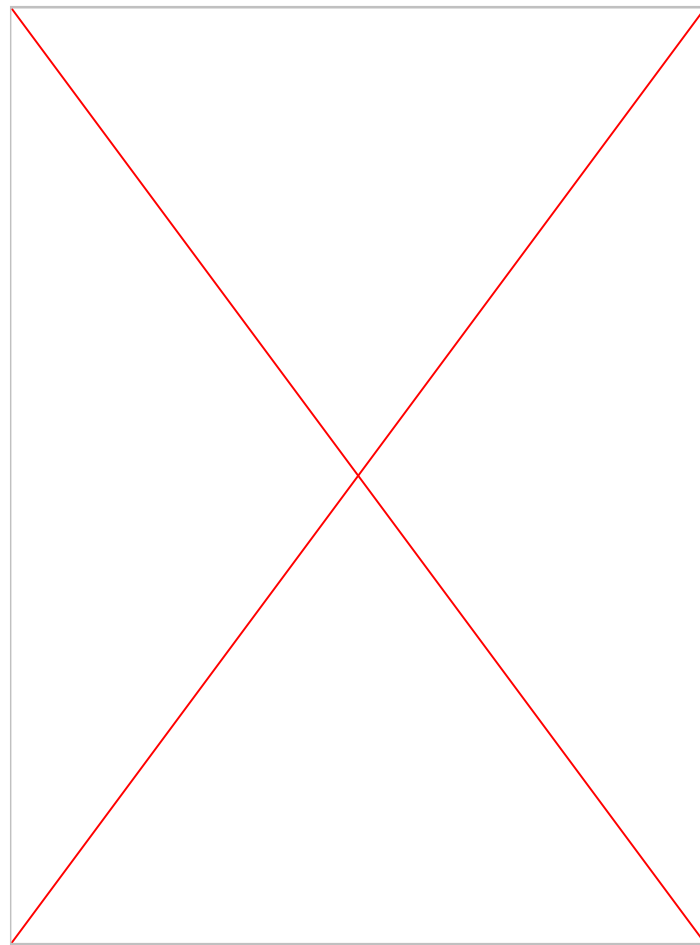
data to be signed (**hashes** of claims)

Example: Verifiable credential in the SD-JWT VC format (serialized form)

[illegible]

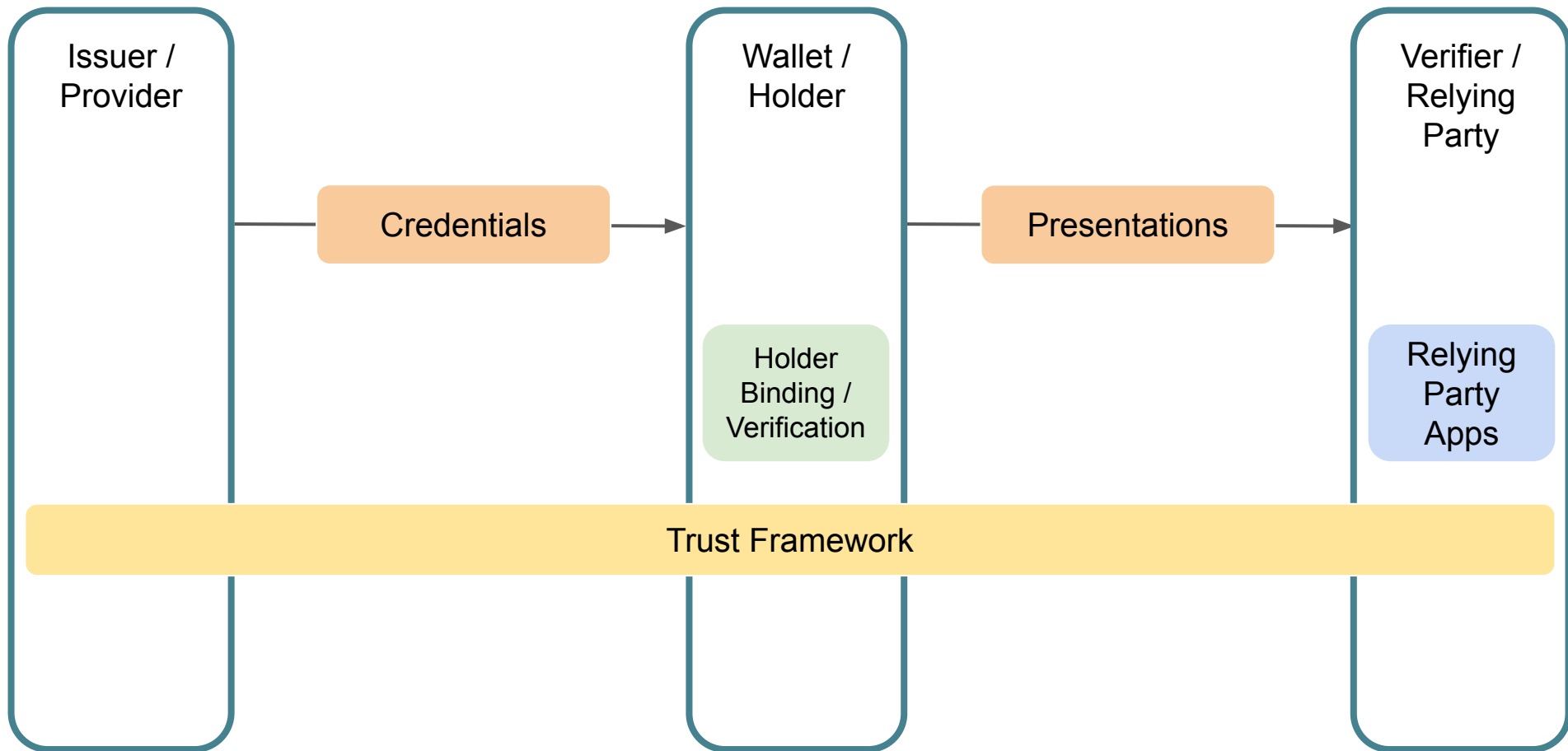


Wallet to Verifier UX
Presentation via Deep Link

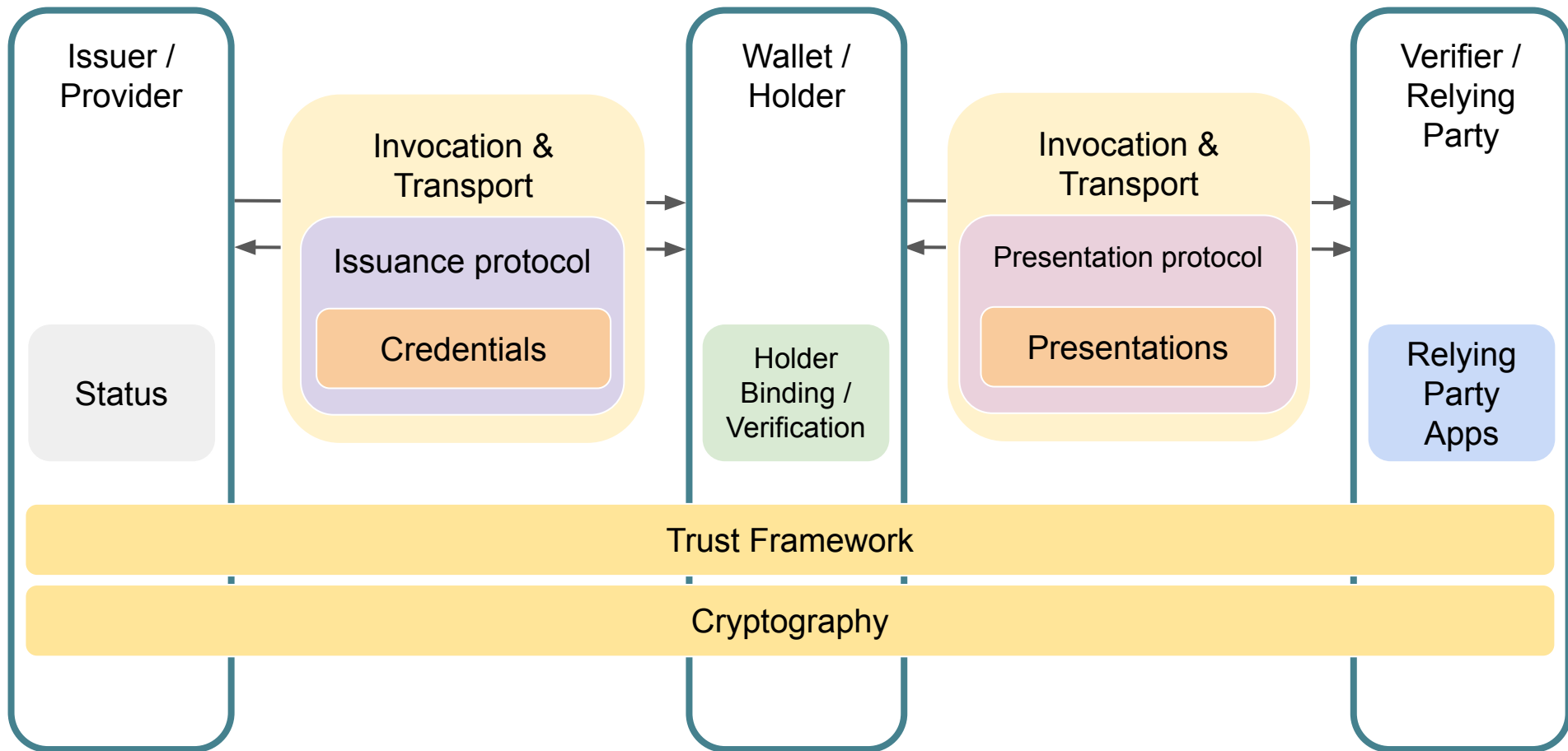


Wallet to Verifier UX
Presentation via Digital Credentials API

Digital Verifiable Credentials Flow



The Building Blocks for the Digital Credentials Stack



What to choose? How do I build my MVP?

Layer / Function	Standards / Choices Available					
Issuance Protocol	OpenID4VCI	ISO 23220-3	DIDComm	...	...	...
Credential Formats	W3C VCDM	SD-JWT-VC	ISO mDoc	AnonCreds	...	...
Presentation Flow	OpenID4VP	DIDComm	mDoc	QR		
Invocation	W3C DC API	QR Code	Deep Link	CHAPI	NFC (mDoc)	...
Transport	BLE (mDoc)	NFC (CTAP)	Camera(QR)	HTTP	BLE (OpenID4VP)	
Trust Framework	X.509 / Trust Lists	OIDF Federation	vLEI	DID	...	...
Status	IETF Status List		W3C Bitstring Status List		...	...

What to choose?

Layer / Function	Standards / Choices Available					
Issuance Protocol	OpenID4VCI	ISO 23220-3	DIDComm	...	...	...
Credential Formats	W3C VCDM	SD-JWT-VC	ISO mDoc	AnonCreds	...	...
Presentation Flow	OpenID4VP	DIDComm	mDoc	QR		
Invocation	W3C DC API	QR Code	Deep Link	CHAPI	NFC (mDoc)	...
Transport	BLE (mDoc)	NFC (CTAP)	Camera(QR)	HTTP	BLE (OpenID4VP)	
Trust Framework	X.509 / Trust Lists	OIDF Federation	vLEI	DID	...	...
Credentials Status	IETF Status List		W3C Bitstring Status List		...	...

OIDF HAIP
Profile

What to choose?

Layer / Function	Standards / Choices Available					
Issuance Protocol	OpenID4VCI	ISO 23220-3	DIDComm	...	...	...
Credential Formats	W3C VCDM	SD-JWT-VC	ISO mDoc	AnonCreds	...	...
Presentation Flow	OpenID4VP	DIDComm	mDoc	QR		
Invocation	W3C DC API	QR Code	Deep Link	CHAPI	NFC (mDoc)	...
Transport	BLE (mDoc)	NFC (CTAP)	Camera(QR)	HTTP	BLE (OpenID4VP)	
Trust Framework	X.509 / Trust Lists	OIDF Federation	vLEI	DID	...	...
Credentials Status	IETF Status List		W3C Bitstring Status List		...	...

OIDF HAIP
Profile

Trusted by the EU and their 27 member states –
European Union Digital Identity (EUDI)

OIDF OpenID for Verifiable Credentials

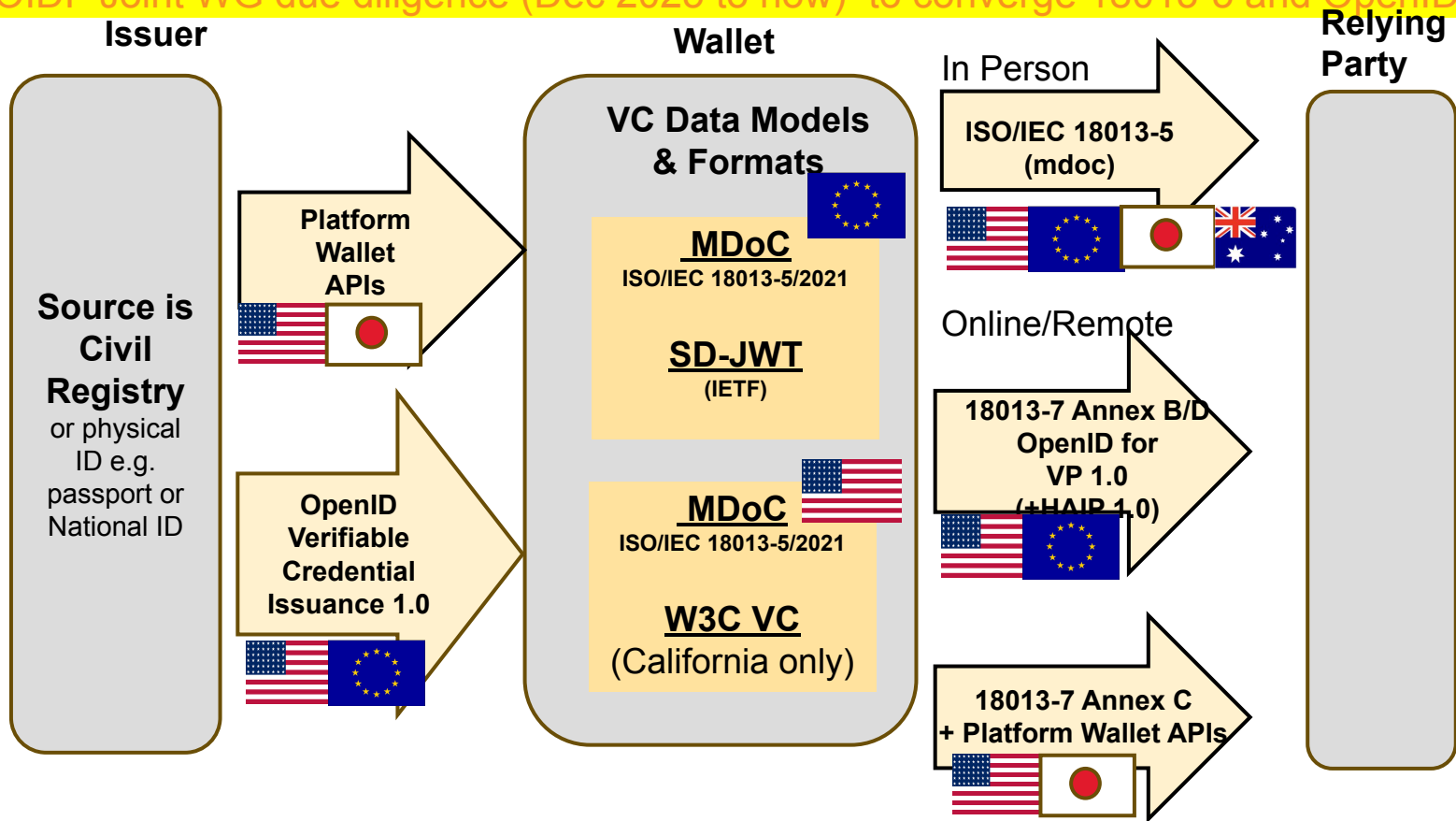
- OpenID for Verifiable Credential Issuance (OID4VCI)
 - Issuance protocol based on OAuth-protected credential issuance endpoints
 - UX via web browsers, asynchronous via pre-authz code flow, and interactive authorization endpoint supporting native app flow
 - Can be initiated by Issuer or the Wallet
- OpenID for Verifiable Presentations (OID4VP)
 - Presentation protocol supporting various credential formats and transports (same device via Deep Links, cross-device via QR Code, or hybrid via the W3C Digital Credential API)
- OpenIDVC High Assurance Profile (HAIP)
 - Defines a high-security, privacy-preserving interoperability profile
 - Selects and constrains features from existing standards (e.g. OID4VP, OID4VCI)
 - Ensures interoperable issuance and presentation flows
 - Targets ecosystems requiring high assurance levels
 - Selected credential formats
 - IETF SD-JWT VC
 - ISO mdoc

Other Insights: Spec Convergence, Spec Selection



Will Wallet Standards Converge?

ISO/OIDF Joint WG due diligence (Dec 2025 to now) to converge 18013-5 and OpenID4VP



OpenID Federation

- Specs
 - OpenID Federation 1.0 Final, “next generation of x509,” inclusive of x509
 - OpenID Federation 1.1 is backward compatible, splits out OpenID Connect
 - Protocol can work with OIDC, FAPI, OpenID4VP/VC/HAIP (eIDAS 2.0)
- Adoption
 - Selected by EDUGain to transition from SAML to a more agile trust registry approach (e.g. GEANT, AFF, 9+ others)
 - Selected by Italian Government for two digital identity ecosystems
 - Selected by Bank of International Settlements for Project Aperta, cross border interoperability of open data in trade finance (UAE, Brazil, UK, HK; OIDF observer)
 - In development for a Australian bank, to deliver Agentic AI use case and integrate Wallet and VC functionality (OpenID4VP/VC)
 - In review by HL7, FHIR for health data access and consent based exchange

Any new digital wallet or open banking, open health, or open data ecosystem will want to consider it