KeyShare

DPI Alignment Brief

KeyShare Digital ID Platform capabilities mapped to Digital Public Infrastructure principles. Open standards, sovereign deployment, inclusion, and ecosystem extensibility.

For government CIOs, multilateral advisors, and development partners evaluating digital identity platforms through the DPI lens.

1. DPI Principle Mapping

DPI Principle	KeyShare Capability	Architectural Evidence
Open Standards	W3C VC, ISO 18013-5, SD-JWT VC, OIDC4VP	No proprietary credential formats. All credentials use standardized data models and presentation protocols.
Interoperability	Multi-format credential support; protocol bridging	Platform accepts mDL, W3C VC, and SD-JWT credentials through a unified verification engine.
Inclusion	Multi-channel: smartphone wallet, NFC cards, delegated agents, SMS/USSD	Citizens without smartphones access services through non-digital channels with equal identity assurance.
Minimalism / Privacy	Selective disclosure; zero-knowledge proofs; ephemeral verification	Only requested attributes are shared. Verifier learns "over 18" without learning date of birth.
Evolvability	Modular architecture; standard-agnostic credential engine	New credential formats and verification protocols can be added without platform re-architecture.

2. SDG 16.9 Alignment

SDG 16.9 calls for legal identity for all by 2030. Three architectural constraints stand between current systems and universal legal identity:

Constraint	Challenge	KeyShare Architecture
Connectivity	Rural and remote populations lack reliable internet.	Offline-first verification using cached trust data and cryptographic self-verification. No cloud required.
Device Access	Many citizens lack smartphones.	NFC cards, delegated agents, and SMS/USSD channels serve citizens without smartphones.
Institutional Capacity	Governments need operational independence from vendors.	Sovereign deployment with full knowledge transfer. Source code available for audit.

3. GovStack Building-Block Mapping

The GovStack framework defines building blocks for digital government infrastructure. KeyShare platform components map directly to these building blocks:

GovStack Building Block	KeyShare Component
Identity	Digital ID Platform — credential issuance, verification, lifecycle
Consent	Consent engine — granular, auditable, jurisdiction-configurable
Digital Registries	Integration layer — connects to civil registries and foundational ID
Messaging	Multi-channel notification — SMS, push, in-app
Payments	Payment verification via Puck NFC (hotel and service delivery contexts)
Workflow	Organization integration layer — configurable per service type

4. Standards Compliance Matrix

Standard	Status	Usage
W3C Verifiable Credentials Data Model 2.0	Implemented	Credential issuance and verification
ISO 18013-5 (mDoc)	Implemented	Mobile driver license verification via NFC
SD-JWT VC	Implemented	Selective disclosure for privacy-preserving presentation
DIDComm v2	Supported	Peer-to-peer credential exchange
OIDC4VP	Implemented	Online credential presentation protocol

5. Sovereign Deployment Model

Model	Description	Data Residency

Sovereign Cloud	Platform hosted on government-approved cloud infrastructure within national borders.	100% in-country. No data crosses borders.
Government-Hosted	Platform runs on government data center infrastructure. Full operational control.	100% on-premises. Government-controlled.
Hybrid	Core services on-premises; analytics and updates via secure cloud channel.	PII on-premises. Anonymized analytics in cloud.

All deployment models include knowledge transfer to government technical teams. Operational independence from KeyShare is a design goal, not a limitation.

Next Steps

- **Request a Government Briefing:** keyshare.id/contact/?type=government
- **Download the Technical Overview:** keyshare.id/resources/gov-technical-overview/