KeyShare

Government Technical Overview

Platform architecture, standards compliance, security model, performance targets, and deployment options for the KeyShare Digital ID Platform.

For CTOs, CISOs, and technical evaluators conducting due diligence.

1. Platform Architecture Overview

The KeyShare Digital ID Platform is organized into five layers. Each layer has defined responsibilities and interfaces.

Layer	Responsibility	Key Components
Credential Issuance	Issue verifiable credentials from authoritative sources	Issuer service, identity proofing integration, credential lifecycle
Citizen Wallet	Store and present credentials under citizen control	Mobile wallet app, NFC card interface, delegated agent protocol
Verification Engine	Verify presented credentials in real-time	Multi-format parser, cryptographic verification, revocation checking
Trust Governance	Manage trust anchors, revocation, and policies	PKI management, trust registry, revocation distribution
Organization Integration	Connect to existing government systems	API gateway, civil registry adapters, workflow engine

2. Security Model

Cryptographic Primitives

Algorithm	Usage	Standard
Ed25519	Credential signing	RFC 8032
ES256	W3C VC / JWT signatures	RFC 7518
AES-256	Data at rest encryption	FIPS 197
wolfSSL	TLS and cryptographic operations	FIPS 140-2 validated

Security Architecture Principles

- **Zero-trust network architecture:** No implicit trust between components. Every service authenticates to every other service.
- **Secure element integration:** Private keys stored in hardware security modules (Common Criteria EAL5+). Keys never leave the secure element.
- **Event logging and anomaly detection:** All security-relevant events logged. Anomaly detection flags unusual verification patterns.
- **Vulnerability disclosure:** Coordinated disclosure process. Findings remediated within defined SLA based on severity.

3. Code Auditability

Source code for application and service layers is available to deployment partners for independent security audit. This includes:

- Mobile wallet application (citizen-facing)
- Verification engine and credential processing
- Organization integration APIs
- Trust governance and PKI management

Audit scope covers application and service layers. Infrastructure and operational tooling are not included in the standard audit package.

4. Performance Targets

The following are design targets. Actual performance will be validated in production at each deployment scale.

Metric	Design Target	Conditions
Credential issuance throughput	1,000 credentials/hour	Single issuer instance
Verification latency (online)	< 500ms	Standard network conditions
Verification latency (offline)	< 200ms	Cached trust data, local verification
Offline sync interval	15 minutes	Configurable per deployment
Revocation propagation	< 5 minutes	Online; offline = next sync

5. Offline-First Verification Architecture

The platform is designed for environments with intermittent or no connectivity. Offline verification uses three mechanisms:

- **Cached trust data:** Trust anchors, public keys, and issuer certificates are cached locally. Verification does not require a network round-trip.
- **Local revocation lists:** Revocation data is synced at configurable intervals. Between syncs, the most recent revocation list is used.
- **Cryptographic self-verification:** Credentials are cryptographically signed. Signature verification is a local operation — no network required.

Next Steps

- **Request a Government Briefing:** keyshare.id/contact/?type=government
- **Review the DPI Alignment Brief:** keyshare.id/resources/dpi-alignment-brief/
- **Security and Trust Center:** keyshare.id/security/