KeyShare

Controller Derivation Architecture

for Identity-Based Access Control

Technical overview: architecture, data flow, security model, integration compatibility, and performance specifications for KeyShare on Mercury panels with LenelS2, Genetec, Acre, and Access It PACS platforms.

For Security Directors, IT Directors, and Solutions Architects conducting technical evaluation.

Architecture Overview: Controller Derivation

KeyShare uses a Controller Derivation architecture: intelligence lives on the panel, not in the cloud or at the reader. The reader authenticates the digital identity. The panel derives a site-specific identifier and makes the access decision. The cloud handles enrollment orchestration and manifest distribution — it is never in the critical path for any door opening.

Layer	Component	Responsibility	Data Held
Edge	Reader (Reader Library)	Authenticate digital ID via ISO 18013-5. Report via OSDP.	Transient session data only.
Panel	Mercury controller (Panel Application)	Derive site-specific UUID. Validate against manifest. Pass credential to PACS.	Signed manifest (UUIDs + validity). Derivation keys.
Cloud	KeyShare Connect	Enrollment orchestration. Manifest generation. PKI management.	Enrollment records. Audit logs.

Three key properties distinguish this from cloud-dependent mobile credential systems:

- **On-premise access decisions.** Every access decision is made locally on the Mercury controller. No cloud round-trip. Doors open during any cloud outage.
- **Zero PII at the edge.** The reader processes identity data in transient memory only. The manifest contains site-specific UUIDs, not personal data.
- **No proprietary integration.** The Panel Application outputs a standard credential number through the panel's native interface. The PACS sees a standard credential.

Data Flow: Enrollment, Authorization, Revocation

Enrollment Flow

1. Employee presents digital ID to Puck at enrollment station.
2. Reader Library authenticates the credential via ISO 18013-5 NFC.
3. Panel Application derives a site-specific UUID using HKDF with site-specific keys.
4. UUID is added to the authorization manifest and distributed to relevant panels.
5. PACS receives a standard credential number mapped to the UUID.
6. Employee is authorized. No PII leaves the enrollment station.

Authorization Flow (Door Tap)

1. Employee taps phone on NFC reader at door.
2. Reader Library authenticates the digital ID and reports to panel via OSDP v2.2.
3. Panel Application derives the UUID and checks against cached manifest.
4. If authorized: standard credential number passed to PACS. Access granted.
5. If not authorized: access denied. Event logged.
6. No cloud round-trip. Decision time: architecture target < 500ms.

Revocation Flow

1. HR/Security revokes access in PACS console (standard workflow).
2. KeyShare Add-On removes UUID from authorization manifest.
3. Updated manifest distributed to all relevant panels.
4. Propagation time: architecture target < 5 minutes (online).
5. Offline panels receive update at next sync interval.

Security Architecture

Domain	Implementation	Standard/Certification
Credential verification	ISO 18013-5 NFC authentication with cryptographic signature check	ISO 18013-5
Reader-to-panel communication	OSDP v2.2 secure channel with AES-128 encryption	OSDP v2.2 (SIA)
Cryptographic library	wolfSSL for all TLS and cryptographic operations	FIPS 140-2 validated (wolfSSL module)
Secure element	Hardware key storage in Common Criteria EAL5+ element	CC EAL5+
UUID derivation	Site-specific, non-reversible. Derivation keys never leave panel.	HKDF-based (implementation detail)
Embedded firmware	Reader Library firmware developed to automotive standard	MISRA C:2012

Integration Compatibility Matrix

Category	Supported	Notes
PACS Platforms	LenelS2 OnGuard Genetec Security Center Acre Access Access It Universal	Integration via KeyShare Add-On installed in PACS console. No API changes to PACS.
Panel Hardware	Mercury EP1502 Mercury EP2500 Mercury EP4502	Panel Application loads as firmware module. No panel replacement required.
Reader Protocol	OSDP v2.2 over RS-485	Secure channel with AES-128 encryption.
Credential Standards	ISO 18013-5 (mDL) W3C Verifiable Credentials	Additional credential formats on roadmap.
Network	TCP/IP (panel to Connect) RS-485 (reader to panel)	No additional network infrastructure required.

Performance and Reliability Specifications

The following are architecture design targets. Actual performance will be validated during deployment at each site.

Metric	Target	Conditions
Door tap to access decision	< 500ms	Panel-local decision, no cloud round-trip
Enrollment time (end-to-end)	< 2 minutes	ID verification + manifest distribution
Manifest sync interval	60 seconds (configurable)	Panel to Connect
Revocation propagation	< 5 minutes (online)	Offline: next sync
Reader uptime target	99.9%	Hardware reliability
Cloud availability (Connect)	99.9%	Not in access decision path

Compliance Alignment

Framework	KeyShare Alignment
FICAM (Federal)	Identity-based access with government-issued credentials. PIV/PIV-I credential support on roadmap.
NIST 800-53	Access control (AC), identification and authentication (IA), audit and accountability (AU) control families addressed.
SOX (Financial)	Identity-verified access logging for IT infrastructure areas. Non-repudiation through cryptographic identity binding.
HIPAA (Healthcare)	Facility access controls (164.310(a)). Unique user identification (164.312(a)). Audit controls (164.312(b)).
ITAR (Defense)	Foreign national detection. Identity-verified access logging. Zone-based access restrictions.

Deployment Requirements

Requirement	Detail
Mercury panels	EP1502, EP2500, or EP4502 with firmware supporting custom applications.
NFC readers	OSDP v2.2 compatible. NFC readers at enrollment stations and access points. Existing readers may require upgrade.
Network	TCP/IP connectivity from panels to KeyShare Connect (cloud). RS-485 from readers to panels (standard).
PACS console	LenelS2, Genetec, Acre, or Access It. KeyShare Add-On installed in console.
Deployment timeline	2-4 weeks typical. Pilot site first, then phased rollout.

Next Steps

- **Book an Architecture Review:** keyshare.id/contact/?type=pacs
- **Download the Solution Brief:** keyshare.id/resources/pacs-solution-brief/
- **Developer Hub:** keyshare.id/docs/