KeyShare

Authorize People, Not Tokens.

Identity-based building access and visitor management — running on your existing Mercury panels and PACS software. Digital IDs at zero cost. Traditional credentials where needed. Everyone gets in.

$8.5M/yr
Quoted to a 500K-employee enterprise for mobile credentials. They never got past pilot.

$0
Per-user fees with KeyShare. Site-based subscription instead.

<60s
Enrollment to first door tap. Name, DOB, tap, access.

0%
Rip-and-replace. Software layer on existing Mercury controllers.

The Credential Cost Problem

A 500,000-employee enterprise was quoted $8.5 million per year for mobile access credentials. They never got past pilot. That story repeats across the industry — enterprises with 5,000 or more employees routinely project six-figure annual credential costs before they've even begun a full rollout.

The cost isn't the worst part. These are vendor-issued tokens — proprietary credentials tied to a single vendor's ecosystem. Every mobile credential is a token the organization pays to issue, pays to maintain, and pays to replace. The organization is renting access to its own buildings.

What KeyShare Changes

Your employees already carry a government-issued digital identity — a mobile driver's license issued by their state, cryptographically signed and verifiable. KeyShare uses that identity for building access. No vendor-issued token. No per-user fee. No onboarding. No credential distribution.

> *Digital IDs at zero cost. Traditional credentials where needed. Everyone gets in.*

How It Works

Step	What Happens	Detail
1. Authorize	Security officer enters a name and date of birth in the PACS. No credential to send.	Access profile assigned through existing PACS workflow. No app to push, no credential to distribute.
2. Tap	Employee presents digital ID at the reader. Identity verified cryptographically on the panel.	ISO 18013-5 NFC verification. Site-specific UUID derived on panel. No PII stored at reader or panel.
3. Access	Door unlocks. Event logged. Revocation is instant — remove authorization, access stops.	Standard credential number passed to PACS. Existing access rules apply. No cloud round-trip for any door.

That's the entire workflow. Security officer enters a name and date of birth. Employee taps their phone at the reader. Door unlocks. Under 60 seconds from enrollment to access.

Mixed-Mode: Digital IDs + Traditional Credentials

KeyShare doesn't require a migration. The system runs identity-based access and traditional credentials simultaneously, on the same panels, through the same PACS, from day one. This isn't a workaround — it's the deployment model.

Scenario	How It Works	Cost Impact
Employees with digital IDs	Identity-based access via KeyShare. No per-user credential fee.	$0 per user. Immediate savings.
Employees without digital IDs	Continue using existing badges or mobile credentials. Nothing changes.	Existing cost structure. No disruption.
New hires in mDL states	Enrolled via digital ID from day one. No credential to provision or ship.	$0 per user. Zero onboarding friction.
Visitors	Identity-verified at reception via Puck. Time-bounded credential. Auto-expires.	No badge printing. No manual provisioning.

If 30% of your employees carry digital IDs today, that's 30% of your per-user credential costs eliminated immediately — with no incremental cost for the 70% who stay on existing credentials. As digital ID adoption grows in each state, your savings grow automatically. No re-deployment. No cutover.

What This Means for System Integrators

Mixed-mode doubles the addressable market. An SI selling a 100%-digital-ID solution can only sell to enterprises ready for full migration — a tiny market today. An SI selling mixed-mode KeyShare can sell to every enterprise, because the system works at any level of digital ID adoption, including zero. More readers, more controllers, more coverage. Annual subscription revenue on every deployment.

Building Access + Visitor Management

Building Access

- Identity-based access using government-issued digital IDs — zero per-user cost
- Mixed-mode: digital IDs and traditional credentials on the same system from day one
- Controller derivation: access decisions made on-panel, not in the cloud
- Runs on existing Mercury panels — no hardware replacement
- OSDP v2.2 secure channel between reader and panel
- No onboarding, no credential distribution, no app to install

Visitor Management

- Identity-verified visitor check-in with 1:1 face matching
- Ephemeral biometric processing (RAM only, zero retention)
- NDA automation with identity-linked electronic signatures
- Time-bounded visitor credentials with automatic expiration
- Foreign national detection for ITAR-controlled facilities

ROI: Partial Adoption Still Saves

You don't need 100% digital ID adoption to see ROI. Every employee on a digital ID is one fewer per-user credential fee.

Enterprise Size	Current Credential Cost (@ $8/user)	30% on Digital ID (Year 1 Savings)	60% on Digital ID (Year 2-3 Savings)
1,000 employees	$8,000/year	$2,400	$4,800
5,000 employees	$40,000/year	$12,000	$24,000
10,000 employees	$80,000/year	$24,000	$48,000
50,000 employees	$400,000/year	$120,000	$240,000

ROI projections assume $8/user/year (mid-range of $4-$17 industry pricing). Actual savings depend on current vendor contract terms and digital ID adoption rate in your workforce's home states. Contact us for a personalized analysis.

Integration Compatibility

Category	Supported
PACS Platforms	LenelS2, Genetec, Acre, Access It
Panel Hardware	Mercury EP series (EP1502, EP2500, EP4502)
Reader Protocol	OSDP v2.2 over RS-485
Credential Standards	ISO 18013-5 (mDL), W3C Verifiable Credentials
Deployment	Software layer on existing panels. No rip-and-replace.

Trust Signals

- **4 US patents granted** covering identity verification and access control
- **Continental Automotive heritage** — founded by the team behind 120M vehicle access systems
- **wolfSSL FIPS 140-2 validated cryptography**
- **Common Criteria EAL5+ secure element** (Puck hardware)
- **Offline-first architecture** — no cloud dependency for access decisions
- **Standards-based, no vendor lock-in:** ISO 18013-5, OSDP v2.2, FIPS 140-2

Next Steps

- **Book an Architecture Review:** keyshare.id/contact/?type=pacs
- **Calculate your savings:** keyshare.id/resources/pacs-roi-calculator/
- **Download the Technical Brief:** keyshare.id/resources/pacs-technical-brief/
- **System Integrators:** Annual subscription revenue. Same-day deployment. keyshare.id/partners/