KeyShare

We Adapt to Your Architecture.

Three integration topologies. PMS compatibility. Lock vendor support. Wallet platform certification. The IT Director's pre-qualification guide.

Integration Topologies

KeyShare's Guest Experience Platform (GEP) uses a standardized adapter framework to connect with hotel subsystems. Each integration is a self-contained adapter that translates between GEP's internal data model and the external system's API. This makes GEP PMS-agnostic and lock-system-agnostic — you connect GEP to your existing stack, you don't replace it.

Topology	How It Works	Best For
Middleware Path	GEP connects to your middleware via a single API surface. Your middleware handles downstream routing to PMS, locks, payment, loyalty, etc.	When you have a comprehensive middleware that routes to most subsystems. Gives you full architectural control.
Direct Adapter Path	GEP connects directly to each subsystem using built-in adapters. Each adapter handles authentication, data transformation, sync, and error handling.	When no middleware exists, or for subsystems outside your middleware scope.
Hybrid (Most Common)	GEP routes PMS data through your middleware while connecting directly to lock systems and subsystems outside middleware scope. Both paths operate simultaneously.	When your middleware covers PMS but not every subsystem. This is the most common topology.

The right topology depends on how your middleware is structured and which subsystems it covers. Start with the capabilities that matter most. Same hardware. Software-unlocked upgrades. No rip-and-replace.

PMS Compatibility Matrix

PMS Platform	Integration Model	Auth Method	Sync Behavior
Oracle Opera	REST API adapter	OAuth 2.0	Real-time + batch fallback
Mews	REST API adapter	API key + webhook	Real-time event-driven
Apaleo	REST API adapter	OAuth 2.0	Real-time event-driven
BookingCenter	REST API adapter	API key	Polling (configurable)
Shiji	REST API adapter	OAuth 2.0	Real-time + batch fallback
Cloudbeds	REST API adapter	OAuth 2.0	Real-time event-driven

If your PMS is not listed above, contact us. New PMS adapters are added regularly based on customer demand. The adapter framework is designed so new PMS integrations require only a new adapter configuration — no changes to GEP core, Puck firmware, or guest-facing experience.

Lock Vendor Support

Vendor	Status	What This Means
Assa Abloy (Vostio)	Integrated	Adapter deployed, certified, in production. NFC wallet key provisioning operational.
SALTO	Integrated	Adapter deployed, certified, in production. NFC wallet key provisioning operational.
dormakaba	In Progress	Integration under development. Contact us for timeline.
Onity	Planned	On the integration roadmap. Contact us for timeline.

Native Wallet Key Delivery

KeyShare delivers room keys directly to the guest's native mobile wallet — no app download required. This is "wallet-native" key delivery, distinct from app-dependent systems that require a proprietary app to mediate between the lock and the phone.

- NFC protocol compliance: ISO 14443 A/B, ISO 18013-5
- Presentation protocols: ISO 18013-5 (in-person NFC), OIDC4VP (online)
- Secure element: Common Criteria EAL5+ (on the Puck hardware)

One Tap, Six Systems Unified

When a guest taps the Puck, six things happen in a single interaction:

Step	What Happens	Systems Involved
1. Verify	Digital ID cryptographically verified in under 2 seconds.	Puck (local, no network)
2. Match	Reservation matched by name + arrival date.	GEP Local → PMS adapter → PMS
3. Authorize	Payment incidental authorization captured. Tokenized. PCI-neutral.	GEP → Payment adapter
4. Recognize	Loyalty status checked. If not enrolled, enrollment offered.	GEP → Loyalty adapter
5. Deliver	Wallet key provisioned and delivered to native mobile wallet.	GEP → Lock adapter → lock vendor
6. Complete	Check-in confirmed in PMS. Guest walks to room.	GEP → PMS adapter → PMS

Total guest-facing time: under 3 seconds from tap to wallet key. The guest is recognized, not processed.

The architecture is offline-first: GEP Local operates independently when cloud connectivity is unavailable. Identity verification and room assignment continue. Wallet key provisioning queues until connectivity resumes.

Zero credential storage. All identity data processed in volatile memory only. Your PII exposure does not increase by deploying KeyShare. Discretion by architecture.

Next Steps

- **Book a Demo:** keyshare.id/contact/?type=hotel
- **PMS or lock vendor not listed?** keyshare.id/contact/?type=hotel — we're adding integrations regularly.