Proximity–Gated Biometric Access Controller

Shivang Rajwanshi

Independent Researcher, India
shivangrajwanshi@gmail.com | +91 96344 02628

September 14, 2025

Problem

- Critical facilities (BTS shelters, POP/DC rooms, outdoor cabinets, racks) rely on badges/PINs that are easily cloned; phone readers are often susceptible to relay attacks.
- Cloud–dependent controllers block access during outages or weak backhaul, forcing insecure overrides.
- Biometrics frequently centralize templates, raising privacy/compliance exposure.
- Security teams lack tamper–evident, queryable logs for audits and incident response.

Solution (overview)

Proximity–Gated Biometric Access Controller is an **edge** access controller that enforces **two factors by design**:

1. A registered smartphone first passes **BLE cryptographic attestation** (ECDH/AES–GCM; nonces/counters; signed policy).
2. Only then is the **fingerprint** sensor enabled; the match runs **locally/offline**.

Security hardening: anti–relay timing windows, secure boot + secure element, debug lockout, and **tamper–evident (hash–chained) logs**.

Technology & Integrations

- Interfaces: **OSDP Secure Channel / Wiegand**, relays/dry–contact.
- **CAN/LIN** for elevators, lockers and vehicle ECUs.
- Templates encrypted at rest; **privacy by design** (no template export).
- Admin console + mobile wallet: provisioning, guest passes, revocation.
- **SIEM** export for SOC workflows; offline continuity and fail–secure behavior.

Security details

- BLE attestation: ECDH key agreement, AES–GCM session, monotonic counters, signed policy bundles.
- Proximity–gated flow prevents fingerprint use unless phone attests within allowed **latency window**.
- Secure boot, key storage in **secure element**, debug interfaces locked.
- All events (attest, match, tamper) chained into a **tamper–evident** log; exportable for audit.

Market (context)

- Global Physical Access Control: $\sim$ \$10–11B; high single–digit CAGR.
- Fingerprint access control: $\sim$ \$4–5B; low–to–mid–teens CAGR.
- Near–term reachable niche via integrators/OEMs across RU/CIS, CEE, GCC, India: $\sim$ \$300–500M (company estimate).

Competitors & Differentiation

Competitor	Strengths	Our differentiation
HID (Signo + Mobile Access)	Biometric reader + mobile credentials	Enforced 2FA: **proximity–gated** biometric; **anti–relay** timing; **offline** decision; **tamper–evident** logs; OSDP + CAN/LIN
Suprema (BioEntry)	Rugged fingerprint + LFD; BLE/RFID	Crypto proximity → enables sensor; local template protection; signed policies
IDEMIA (MorphoWave)	High–throughput contactless fingerprint	Compact controller for standard doors/lockers/vehicle ECUs; offline security; broader I/O

Results to date

- Architecture & security design v2; authentication sequence and test plan.
- Two Indian **patent applications filed** (published): proximity–gated biometrics; BLE anti–relay timing.
- TRL 3–4; preparing EVT prototype; partners/integrators identified.

Business model

- Hardware controller per point (door/rack/cabinet).
- Annual per–device license for premium security features/updates.
- **SaaS**: admin console, audit retention, SIEM connectors (per device/user).
- Managed service (Access–as–a–Service) option; OEM/white–label royalties.

Pilot proposal (example)

- **Sites:** 1–2 remote facilities + 1 POP/DC room (or doors/racks/lockers/elevator enable).
- **Integrations:** OSDP/Wiegand panel, relays; optional CAN/LIN; SIEM feed.
- **Deliverables:** pilot kits, install & test scripts, KPI report with recommendations.

Pilot KPIs

- Unlock latency P50/P95.
- FAR/FRR with PAD (presentation attack detection).
- Offline endurance ≥ 72 hours.
- Anti–relay rejection rate; tamper–to–alert ≤ 5 s.
- Interoperability success (OSDP/Wiegand/CAN–LIN); SIEM event quality.

Contact

Shivang Rajwanshi

Independent Researcher, India

shivangrajwanshi@gmail.com | +91 96344 02628

Patents (published, India): 202511074713 A; 202511073065 A