Electromagnetic Temporary Access Lock System

(TAA-1)

Modular Access Control for Shared Community Resources

July 2026

Abstract

This whitepaper defines TAA-1, a modular electromagnetic temporary access system designed for shared community appliances and resources. The system enables time-based, condition-based, and permission-based access without reliance on invasive identity tracking or centralized surveillance. TAA-1 replaces traditional ownership enforcement models with controlled, temporary access windows. It is suitable for laundry machines, shared refrigerators, tool libraries, maker spaces, and EV/battery charging stations. The architecture prioritizes local-first functionality, minimal logging, transparent access logic, and ethical constraints on data collection.

1. Core Concept

Temporary access replaces ownership enforcement. Instead of permanent ownership or always-available access, the system grants defined access windows to shared infrastructure. This reduces conflict, improves fairness, and enables efficient resource utilization without requiring centralized authority or pervasive monitoring.

2. System Architecture

2.1 Layered Design

The system is organized into five distinct layers: **Layer A – Physical**: Electromagnetic lock or solenoid, enclosure, manual override mechanism. **Layer B – Control**: Microcontroller (ESP32 class), timer logic, relay switching for lock and optional appliance power. **Layer C – Credential**: Keypad, RFID reader, or rotating access tokens for low-friction authentication. **Layer D – Policy**: Time windows, duration limits, grace periods, and usage quotas. **Layer E – Audit**: Minimal, non-identifying event logging for system health and dispute resolution.

2.2 Hardware Components

Core components include a 12V DC power supply, solenoid or electromagnetic lock, ESP32 microcontroller, relay module, door/contact sensor, keypad or RFID reader, and optional backup battery for fail-safe operation.

3. Operational Flow

1. User receives a temporary access credential (rotating token, RFID, or time-limited code). 2. System validates the credential against current policy. 3. Lock disengages, allowing entry. 4. Session timer begins; optional appliance power is enabled. 5. Session expires or user ends session. 6. Lock re-engages and power is cut (if applicable). 7. System returns to ready state.

4. Safety and Ethical Requirements

Safety: - Fail-safe or fail-secure configuration must be explicitly defined per use case. - Manual override must be available for staff or emergency personnel. - Fire and emergency conditions must release locks where applicable. **Ethical Design Standard (TAA-1)**: - No biometric dependency. - No unnecessary identity storage. - Local-first functionality (minimal cloud dependency). - Transparent access logic. - Minimal, non-identifying logging only.

5. Threat Model and Mitigations

- Code/token sharing → Mitigated by rotating, time-limited tokens. - Physical tampering → Reinforced enclosure and tamper-evident design. - Power loss → Battery backup or safe-mode behavior. - Misuse/overuse → Session-based enforcement and policy limits.

6. Use Cases and Scalability

Primary use cases include laundry room scheduling, shared refrigerator compartments, tool libraries and maker spaces, and EV/battery charging stations. The system scales from single-device deployments to full-building

community infrastructure nodes through modular design and minimal central coordination.

7. Conclusion

TAA-1 establishes a fair-access infrastructure layer for shared community resources. By combining modular hardware, transparent policy enforcement, and strong ethical constraints on surveillance and identity, the system reduces conflict while enabling efficient shared resource usage without centralized enforcement or pervasive monitoring.

Signed
Aziel
July 2026