

The background of the entire page is a photograph of a modern building entrance with a glass door. A smart lock is mounted on the door frame. A hand is holding a tablet in the foreground, displaying a management interface. Overlaid on the image are several digital icons: a smartphone in a circle, a cloud with a padlock, and a dashed line connecting them. The Qburst logo is in the top right corner.

Qburst

A High AI-Q[™]
Company

Secure, Remotely Managed Access Control with an IoT Smart Lock Management System

Enabling centralized, multi-site electronic lock administration while enforcing an edge-first credential trust model to minimize breach exposure.

Overview

QBurst built a multi-platform IoT Smart Lock Management System that orchestrates remote access control across distributed physical locations using AWS IoT Core and AWS IoT Device Shadow.

- **Edge-First Security Architecture:** Designed around the core principle that credentials stay on the device—retaining sensitive access PINs directly on lock hardware to eliminate persistent cloud database credential exposure while coordinating state updates via AWS IoT Device Shadow.
- **Measurable Platform Outcomes:** Delivered centralized remote management across web/mobile applications, complete resilience to connectivity gaps, and an elastic IoT foundation built to scale across new sites without architectural redesign.



100%
Edge Credential
Isolation



Zero
Persistent Cloud
Credentials



AWS IoT
Core & Device
Shadow



Client Profile

Operating in the commercial facility access and safety sector, the Sweden-based client manages smart lock deployments spanning offices, rooms, multi-tenant facilities, and real estate properties. The enterprise requires high-scale, zero-trust remote manageability to streamline credential provisioning across diverse locations.

Multi-Site Access Management and Centralized Credential Risk

Managing distributed physical security hardware presents competing demands between central remote administration and local device security.

- **Centralized Database Vulnerability:** Traditional access control systems store sensitive PINs and codes in central cloud databases, creating high-risk targets for enterprise breaches.
- **Intermittent Hardware Connectivity:** Distributed locks frequently experience temporary network drops, risking lost status updates or failed credential syncs.
- **Fragmented Multi-Channel Administration:** Operations teams required unified administrative control across web and mobile interfaces without maintaining separate backend communication logic.
- **Multi-Location Scaling Constraints:** Onboarding new facilities or groups of locks demanded an elastic communication foundation capable of handling asynchronous device traffic.

Solution: Connected IoT Access Control Platform

We designed and built an end-to-end IoT Smart Lock Management System that manages credentials, configurations, and operational metadata across dispersed physical locations.

- **Device-Centric Credential Isolation:** Enforced an edge-first trust boundary where the central application coordinates access requests while locks hold the secret credentials, limiting the blast radius of a central platform compromise.
- **AWS IoT Core Communication Layer:** Built a secure bi-directional messaging pipeline connecting backend Node.js microservices to electronic locks across remote sites.
- **Asynchronous State Synchronization:** Deployed AWS IoT Device Shadow to maintain synchronized virtual shadows of each lock, allowing administrators to push credential updates and fetch device telemetry even when locks drop offline.

- **Unified Cross-Channel Applications:** Developed responsive Angular/React web portals alongside native iOS and Android mobile apps driven by a shared backend services layer.

Technical Highlights

- **Edge-First Trust Security Model:** Eliminated persistent credential storage in central databases, ensuring sensitive PINs reside exclusively on local device hardware.
- **AWS IoT Core & Device Shadow Integration:** Leveraged shadow states to reconcile requested configuration changes with reported lock states upon reconnect.
- **Node.js Backend Services:** Built microservices to handle device authorization, configuration routing, and IoT topic orchestration.
- **Cross-Platform Mobile & Web Stack:** Implemented Angular and React frontends alongside Android/iOS mobile applications for seamless administrative access across devices.
- **Group & Multi-Site Hierarchy:** Configured hierarchical device metadata structures to allow batch credential updates across individual locks, room clusters, or full facility sites.

Impact

- **Reduced Breach Blast Radius:** Protected user security by ensuring a central database compromise yields no usable access codes or credentials.
- **Offline Hardware Resilience:** Guaranteed zero data loss during network disruptions through automatic Device Shadow state synchronization.
- **Seamless Multi-Location Scale:** Supported infinite device and site expansion via an elastic AWS IoT Core communication pipeline.
- **Unified Administrative Control:** Enabled operations teams to manage single locks or bulk facility groups through unified web and mobile channels.