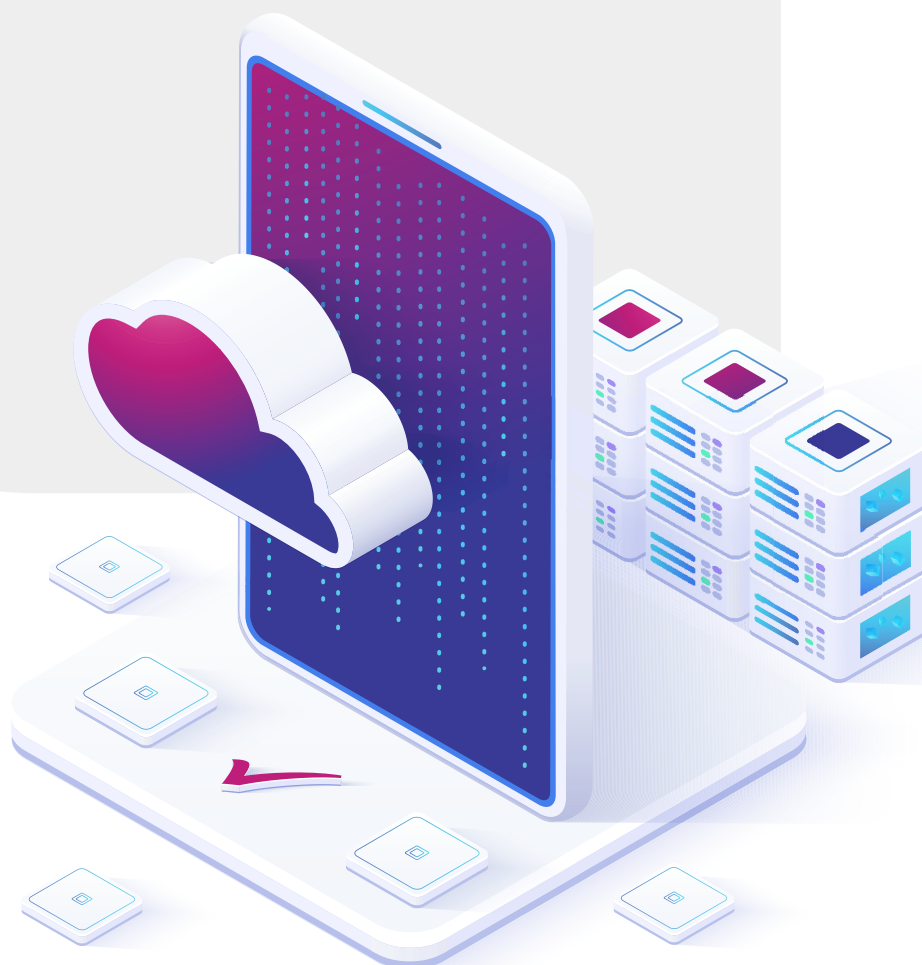


**SUCCESS STORY | RDM PLATFORM**

Device and chip manufacturers  
transform Aadhaar device  
management with

## **Aujas Cybersecurity's Registered Device Management Platform**



# About **the client**

Our customers are leaders in digital security, identification technologies, biometrics, and identity solutions. They offer a range of products and services including chip manufacturing and providing

devices that promise to make digital payments, biometric authentication, and financial access easy and affordable.

## Business **needs**

The customers required a highly scalable, secure, and available system for managing devices within the Aadhaar ecosystem. The system also had to

adhere to all the UIDIA compliances. To address this, they partnered with Aujas Cybersecurity.

Here is an overview of their requirements:

- **Management server:** A secure server with APIs for device management, ensuring device authentication before communicating with the Aadhaar server and rejecting unauthorized devices.
- **Secure signing and firmware management:** Encryption and signing service for biometric devices and chips, ensuring data security.
- **Chip provisioning:** Unique identification for each chip used in Aadhaar-registered biometric devices, a requirement for PCH certification.
- **Secure communication:** Secure API integrations with Aadhaar devices for registration, deregistration, and whitelisting, preventing unauthorized access to the Aadhaar server.
- **UIDAI compliance:** Adherence to UIDAI's L0 and L1 security policies and key management standards with a secure management server.





## Our solution

To help the clients achieve their goals, we implemented our flagship Registered Device Management (RDM) platform - a fully managed

SaaS-based IoT platform supporting both L0 and L1 device specifications for the registration and management of Aadhaar-registered devices..

Here are some of the highlights of the solution:

- **Firmware management:** The platform offers a secure system for firmware management, including signing, encryption, and maintenance. Signing keys are stored in a physical Hardware Security Module (HSM), ensuring robust key management.
- **Seamless firmware upgrade:** Our solution provides a seamless process for upgrading firmware on field devices, enhancing their performance and security.
- **Firmware personalization:** The platform supports firmware customization specific to each device, allowing secure downloads at programming houses.
- **Chip identity service:** Our solution generates unique chip identities by utilizing initial firmware keys and a dedicated chip identity server.

# Benefits delivered

## Key features of the solution

- **Administration portal:** Customizable role-based portal for device management, cost monitoring, and registered device administration
- **Secure API integrations:** Safe API integrations, compliant with UIDAI specifications
- **Device key management:** Management server for device encryption key management via the HSM
- **Telemetry data monitoring:** Device and telemetry data monitoring via the management server
- **Device application management:** Device application change management support following UIDAI guidelines
- **Device SDK support:** Integration across multiple platforms (Linux, Windows, Android) through technical support and testing environments (Stage, Prod) for faster development
- **APIs for registration/de-registration:** API processes for device registration and de-registration

## Benefits

Our collaboration led to substantial improvements, transforming the client's device management ecosystem. Here are four key benefits the client experienced from our collaboration:

- Minimal turnaround time and an option for private cloud setup
- Highly available telemetry API enabling device event posting to the management server
- Deeper insights into biometric device details through fully functional custom dashboards
- Efficient management of devices connected to host machines (Windows, Linux, Android) across India with drill-down capabilities
- Constant improvement in SDKs with bug fixes, enhancements, and new policy changes from UIDAI





## About **Aujas Cybersecurity**

Aujas Cybersecurity empowers clients with enhanced security resilience by minimizing the potential for attacks, threats, and risks. We specialize in architecture risk analysis, comprehensive threat modeling, rigorous penetration testing, and secure coding guidelines. By partnering with us, you can strengthen your security defenses and maintain a robust security posture.

For more information, visit us at [www.aujas.com](http://www.aujas.com) or write to us at [contact@aujas.com](mailto:contact@aujas.com).

