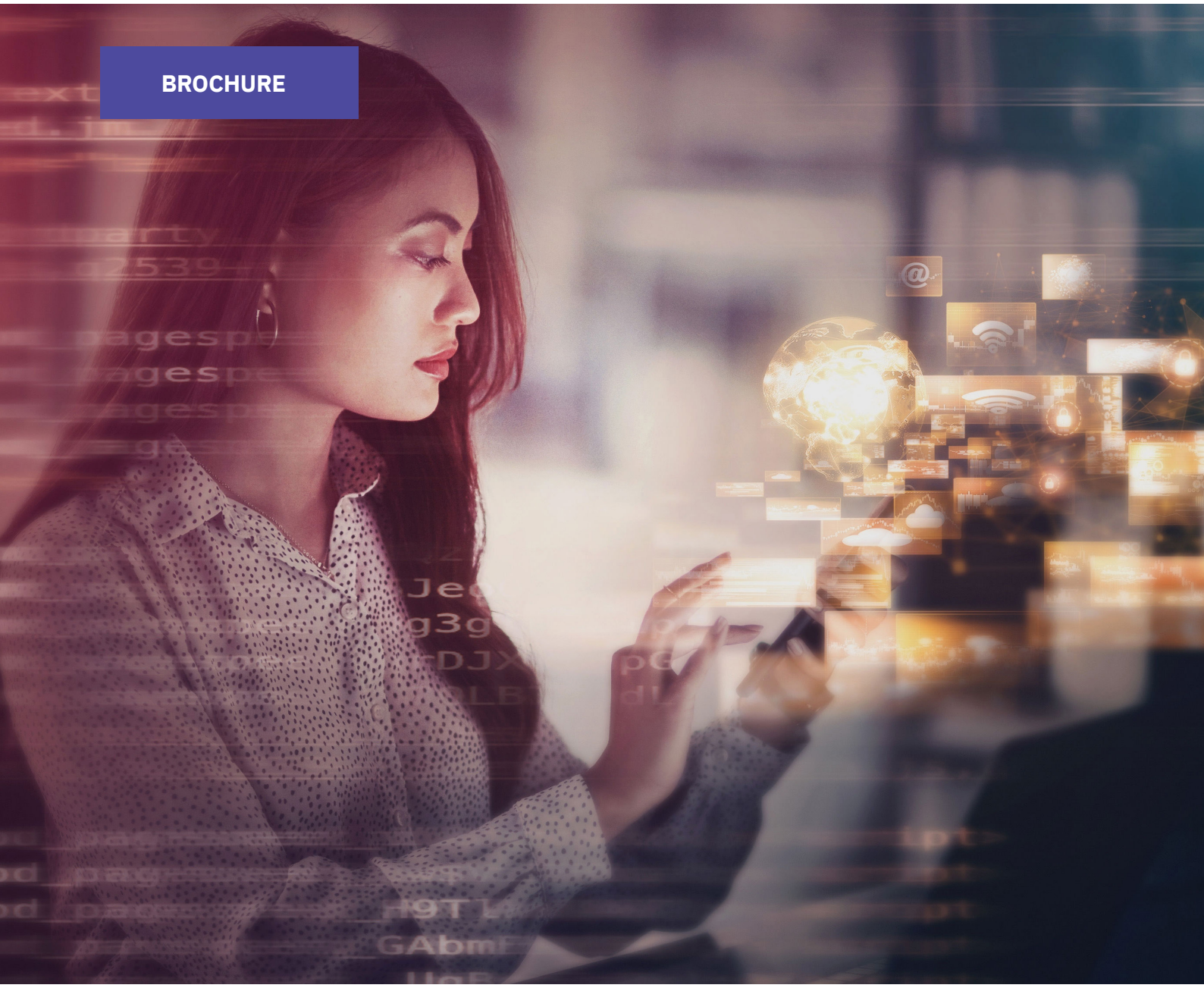
AUJAS
CYBERSECURITY
An NSEIT Company

aujas.com



Registered device management and chip mastering for AADHAAR and MOSIP registered devices

Cybersecurity challenges in large-scale management of registered devices

In this digital era where privacy is a top priority, organizations face complex device management challenges including compliance with diverse regulatory standards and ensuring privacy and uninterrupted service for critical platforms like Aadhaar and MOSIP.

- **Compliance:** Managing devices that need to comply with diverse L0 and L1 standards can be complex and challenging.
- **Privacy:** Ensuring the security and privacy of critical identity data on registered devices is a constant concern.
- **Device integrity:** Preventing tampering and maintaining the integrity of registered devices is essential for secure operations.
- **Maximizing device availability:** Uninterrupted service is crucial for critical identity management platforms like Aadhaar and MOSIP.
- **Scalability:** As organizations grow, managing an increasing number of devices becomes challenging.

The **solution**

Aujas Cybersecurity's Registered Device Management (RDM) platform is your one-stop solution for registering and managing L0 and L1 compliant devices for national identity management platforms like Aadhaar and MOSIP. Our fully managed, SaaS based IoT platform ensures device compliance, maximizes availability, and simplifies management. We offer critical services like secure signing, encryption, firmware maintenance, and chip mastering specifically designed for L0 and L1 devices.

Device onboarding
Multiple options are available for onboarding devices, such as one-time tokens, device whitelisting, key-based whitelisting, and manufacturer-based whitelisting. The device can be onboarded at any stage from manufacturing to customer deployment. Onboarded devices can be mapped to specific customers too for telemetry.

Device management
Simplified device management enables customers to register and deregister the device, upgrade to new software, rotate keys, etc. The same features are extended to your customers for easy management and support by both the manufacturer and the customer.

SDK
Compatible with various platforms—Linux, Windows, Android, and iOS. We facilitate integration with fully developed RD service source code, ensuring customers can start seamlessly from day one. Developers benefit from three environments (Stage, Pre-Prod, Prod) to test all possibilities before making it live for the customers.

Why Aujas Cybersecurity's **RDM platform?**

Simplified management

Effortless device management streamlines processes like registration, deregistration, software upgrades, and key rotation for swift operations.

High availability

Our platform boasts a robust service architecture with full Disaster Recovery (DR) capabilities. Automated DevOps practices ensure real-time monitoring for high availability, usage, and scalability.

Multiple onboarding options

We offer multiple device onboarding methods, including one-time tokens, device whitelisting, and manufacturer whitelisting. Devices can be onboarded at any point from manufacturing to customer deployment, with the added capability to map them to specific customers for telemetry purposes.

In-built compliance

Our Hardware Security Module is compliant with the FIPS 140-2 Level 3 standard. The device management server undergoes regular security audits, maintaining the highest security standards

Device manufacturing support

The RDM platform is tailored to provision L1 device identity seamlessly during the manufacturing process.

Reliable technical support

Customized technical support is available during integration, with portal and email-based support post-integration through an automated ticketing system driven by SLA's.

2 million+ devices

10 Leading registered L0 and L1device manufacturers as clients

About **Aujas Cybersecurity**

Aujas Cybersecurity -An NSEIT Company 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 or write to us at contact@aujas.com.

Cupertino | Dallas | Jersey City | Ottawa | Riyadh | Dubai | Mumbai | New Delhi | Bangalore

Follow us at: