MOSIP connect

Mastering Cryptographic Key Lifecycle Management in MOSIP

Format: Presentation and Brainstorming

Date: 11th/12th February, 2026

Duration: 45 mins (Including Q&A)

Target Audience: Countries, SIs

Targeted Expertise/Roles: Developers, Technical Architects, Technical BA

Max. no. of Participants: 40

Pre-requisites: Pre-registration for the session, Review pre-read material

Presenters: MOSIP Team

Objective:

Cryptographic key lifecycle management is central to **trust, privacy, and system integrity** in national digital identity platforms. In MOSIP-based ecosystems, cryptographic keys span enrollment devices, packet security, internal services (Preregistration, Resident Portal, ID-Repository, IDA), ecosystem partners, and trust frameworks, making disciplined, well-governed key management essential for **long-term platform resilience**.

This session presents a practical, deployment-driven view of how cryptographic keys are managed across their **full lifecycle in MOSIP implementations**. Drawing on real operational experience from large-scale national identity programs, it explains how MOSIP's architecture and operational practices are designed to **anticipate, mitigate, and manage** key-related risks under real-world regulatory, ecosystem, and scale constraints.

Participants will explore how keys are securely **created, stored, used, rotated, and retired** across enrollment, processing, internal services, and partner integrations. The session highlights common industry failure patterns, such as device key exposure, compromised partner keys, **misconfigured rotation policies**, and delayed revocation.

This session will enable participants to understand how to design and use resilient, auditable, and scalable key management lifecycles, and confidently support safe rotation and rapid revocation without service disruption.

Session Outcome:

By the end of this session, participants will be able to:

- Identify key lifecycle risks and failure points.
- Respond effectively to key compromise scenarios.

- Design and enforce key rotation and expiry policies.
- Make informed decisions on key retention and deletion.
- Apply practical approaches to key storage and migration.
- Align implementation with governance and configuration.
- Establish a safe and efficient key management cycle.

Pre-reads:

We recommend going through the links below ahead of the session.

- **Key Manager**: Centralised service managing the cryptographic lifecycle, providing REST APIs for secure encryption, decryption, and digital signing across MOSIP. Find out more here
- **Zero-Knowledge Encryption**: Privacy-first security ensuring data remains inaccessible to administrators; only the resident's unique ID can unlock and decrypt their identity. Find out more here
- **HSM Integration**: Utilises physical hardware modules via PKCS#11 to store root keys securely, preventing any plain-text exposure of sensitive cryptographic material. Find out more here

Thank you. We look forward to your participation in the session!