A Defence Establishment in India Establishes Sovereign Internal CA and Validation Authority with eMudhra emCA

Client Overview

The One of the Defence Establishments in India's One of the Defence Establishments in India (One of the Defence Establishments in India) is a mission-critical digital infrastructure initiative establishing a secure, integrated communications and network management framework across the One of the Defence Establishments in India's operational and administrative domains. As part of India's broader defence modernisation programme, One of the Defence Establishments in India is designed to provide a unified, secure networking backbone for the Army's dispersed commands, formations, and installations — supporting authenticated communications, secure data exchange, and identity-assured access across classified and sensitive military networks. Underpinning the integrity of this infrastructure is a requirement for a sovereign, internally governed digital certificate ecosystem: one that operates entirely within the Army's own security perimeter, without dependency on any external commercial or civilian Certificate Authority service.

The Challenge

Prior to this initiative, the One of the Defence Establishments in India's reliance on external certificate services for authenticating digital identities and securing communications presented a structural vulnerability incompatible with the security requirements of a national defence organisation. External Certificate Authority providers — operating under civilian governance frameworks, connected to public networks, and subject to third-party operational dependencies — cannot meet the fundamental requirement of defence-grade PKI: that the issuance, validation, and revocation of certificates securing military communications must occur entirely within infrastructure under the Army's direct operational control, physically and logically isolated from external networks.

The absence of an internal CA infrastructure meant that certificate issuance for One of the Defence Establishments in India's user and device identities was dependent on civilian service providers whose systems could not be integrated with air-gapped or classified military network segments. Certificate requests, approvals, and issuance events passed through channels outside the Army's security perimeter — creating exposure points that are wholly unacceptable in a defence context

> "A defence PKI cannot depend on civilian infrastructure. Certificate issuance, registration, and validation for military communications must happen inside our own perimeter, under our governance, with no external dependencies. That was the non-negotiable requirement that drove the One of the Defence Establishments in India CA deployment."
>
> **Senior Director, IT & Cybersecurity, One of the Defence Establishments in India One of the Defence Establishments in India**

where adversarial interception of PKI operations could compromise the integrity of authenticated military communications at scale. Certificate revocation was similarly constrained: without an in-house OCSP (Online Certificate Status Protocol) Validation Authority, there was no mechanism to perform real-time certificate status checks within closed military network environments, leaving relying party systems unable to verify certificate validity without querying external services that classified networks cannot reach.

The challenge extended to subscriber management. Without an internal Registration Authority (RA), the vetting, approval, and enrolment of certificate subscribers — Army personnel, devices, and systems requiring digital identities — could not be conducted within the Army's own governance and verification framework. Defence environments require that subscriber identity proofing and certificate approval workflows are executed by authorised military personnel under defined chain-of-command procedures, not delegated to commercial RA operators outside the defence establishment. The absence of an integrated internal RA capability was a direct gap in the Army's ability to implement the end-to-end sovereign PKI lifecycle that One of the Defence Establishments in India demanded.

The Solution

The One of the Defence Establishments in India's One of the Defence Establishments in India programme selected eMudhra's emCA — deploying the CA module, Registration Authority (RA), and OCSP-based Validation Authority — to implement a fully self-contained, air-gap-capable internal PKI infrastructure that operates entirely within the Army's security perimeter and governance framework.

The emCA deployment established a dedicated internal CA hierarchy for One of the Defence Establishments in India: a Root CA and subordinate Issuing CAs configured to issue digital certificates for Army personnel, devices, applications, and communication systems across the One

of the Defence Establishments in India network. The CA infrastructure was architected for air-gapped operation — all CA functions, including key generation, certificate issuance, and CRL publication, operate entirely within the Army's closed network environment with no dependency on external internet connectivity or civilian PKI services. Certificate profiles were configured to meet defence-specific requirements: cryptographic standards, key usage constraints, subject naming conventions, and validity parameters aligned to the operational and security policies governing One of the Defence Establishments in India digital identities.

eMudhra's emRA (Registration Authority) module was deployed as the integrated subscriber management layer, enabling authorised Army personnel to conduct the full certificate applicant lifecycle — identity vetting, credential verification, request approval, and subscriber enrolment — within the Army's own command and access control framework. RA operator roles were configured in strict alignment with the Army's internal authorisation hierarchy, ensuring that certificate approval authority is exercised by designated military personnel at appropriate command levels, with dual-control procedures enforced for sensitive registration actions. The emRA-emCA integration ensured that the end-to-end certificate provisioning workflow — from subscriber vetting through issuance — operates as a single, internally governed, auditable process with no hand-off to any external party.

The OCSP Validation Authority was deployed as the real-time certificate status service for One of the Defence Establishments in India's relying party systems. Operating as an internal OCSP responder within the Army's network, the Validation Authority enables applications, communication platforms, and access control systems across One of the Defence Establishments in India to query certificate validity in real time — without any external network dependency. This capability is essential for the authenticated, certificate-backed workflows that One of the Defence Establishments in India supports: secure login, encrypted communications, digital signing of military documents, and access control to sensitive systems all depend on the ability to verify that the certificates presented are current, valid, and not revoked. The internal OCSP responder delivers this assurance entirely within the Army's closed network perimeter. CRL distribution was configured in parallel to ensure that revocation information is consistently available to all One of the Defence Establishments in India relying party systems even in disconnected or degraded network conditions.

Results

The deployment of eMudhra emCA — encompassing the CA, RA, and OCSP Validation Authority modules — delivered a sovereign, end-to-end internal PKI capability for the One of the Defence Establishments in India's One of the Defence Establishments in India programme, eliminating all dependency on external certificate services and establishing a defence-grade digital trust infrastructure operating entirely within the Army's own governance and security perimeter.

Metric	Before	After
Internal CA Infrastructure	Absent; reliant on external certificate services	Fully operational in-house CA via emCA deployed
Certificate Issuance Control	External dependency; no direct governance	Independent, internally governed issuance under One of the Defence Establishments in India

Metric	Before	After
OCSP Validation Authority	Not in place; no real-time validation	Live OCSP responder for real-time certificate validation
Registration Authority (RA)	Not in place; managed externally	Integrated emRA for subscriber vetting and approval
Classified Network Compatibility	External CA services incompatible with air-gapped ops	Fully air-gap capable; operates within closed military networks
Certificate Policy Governance	Governed by external provider policies	Internally defined and enforced military-grade policy framework
Audit Trail & Operational Accountability	Fragmented; records held externally	Complete internal audit trail across CA, RA, and OCSP events

With emCA operational, the One of the Defence Establishments in India's One of the Defence Establishments in India now issues, validates, and governs digital certificates for its personnel, devices, and systems entirely within its own infrastructure — with no external CA dependency, no civilian network exposure, and no third-party involvement in any stage of the certificate lifecycle. The integrated OCSP Validation Authority provides real-time certificate status assurance to One of the Defence Establishments in India's relying party systems within the closed military network, enabling the authenticated communications, secure access controls, and digitally verified workflows that the Army's operational requirements demand. The comprehensive internal audit trail — spanning CA issuance events, RA registration actions, and OCSP validation transactions — provides the Army's security and compliance leadership with full accountability over every PKI operation within the One of the Defence Establishments in India environment.

About eMudhra

eMudhra is a globally trusted provider of digital trust services, offering eSignatures, PKI, Certificate Lifecycle Management, Multi-Factor Authentication, and Identity & Access Management solutions. Licensed by the Controller of Certifying Authorities (CCA), India, eMudhra serves 1000+ enterprises across 40+ countries, helping organisations build secure, compliant, and paperless digital ecosystems.