CASE STUDY

SECUREPASS · GOVERNMENT & PUBLIC SECTOR · INDIA

A Central Government Department in India Secures Employee Access Across a Large Distributed Workforce with eMudhra SecurePass

SECTOR	REGION	SOLUTION
Government & public sector	India	SecurePass

CLIENT OVERVIEW

The organisation is a central government department in India with a workforce of approximately 12,000 employees distributed across a headquarters office and regional offices in every state. The department operates several internal applications — including an HR management system, a case management platform, a document management portal, and various reporting tools — as well as interfaces with central government systems such as PFMS and NIC-hosted services.

THE CHALLENGE

Employees accessed the department's applications using separate credentials for each system, with no single sign-on in place. Provisioning access for new employees required IT requests to be raised manually with each application team, which often resulted in new joiners waiting a week or more for full access. The department also had no formal process for revoking access when employees transferred between offices or retired, and an internal audit flagged over 200 accounts belonging to retired or transferred staff that remained active across various systems. A government cybersecurity directive from CERT-In recommended that all central government departments implement MFA for access to sensitive internal systems — a requirement the department had not yet met.

> *"We had accounts for staff who had retired years ago still sitting active in our systems. And new joiners were waiting over a week for basic access. Both problems needed fixing at the same time."*
>
> **Director of IT and Digital Services**

THE SOLUTION

eMudhra deployed SecurePass across the department's full employee base. A centralised identity directory was established, integrating with the department's HR system to automate provisioning when employees join, transfer, or leave. Stale accounts identified in the audit were deactivated during the initial reconciliation exercise. SSO was configured for all internal applications, allowing employees to access all authorised systems through a single login. MFA was enabled using OTP via government-issued email and an authenticator app option, fulfilling the CERT-In directive requirement. Role-based access profiles were defined for each grade and function within the department, ensuring employees received access appropriate to their responsibilities without needing individual provisioning requests. Regional office IT administrators were given scoped access to manage their own user populations within the centralised platform.

RESULTS

The initial reconciliation deactivated all stale accounts within the first two weeks. New joiner access provisioning dropped from over a week to same-day. The department submitted its CERT-In compliance response referencing the SecurePass MFA deployment. Help desk requests related to password issues reduced noticeably in the first quarter after go-live.

METRIC	BEFORE	AFTER
Stale accounts deactivated	200+ accounts for retired/transferred staff	All deactivated in initial reconciliation
New joiner access provisioning	1 week+ via manual application requests	Same-day via automated HR integration
MFA coverage — internal systems	Not in place; CERT-In directive unmet	OTP-based MFA across all internal systems
SSO coverage	Separate credentials per application	All internal applications under SSO
CERT-In compliance	Directive unmet	Compliance response submitted with MFA evidence

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 1,000+ enterprises across 40+ countries, helping organisations build secure, compliant and paperless digital ecosystems.

Customer name withheld for confidentiality.