SECUREPASS · BANKING & FINANCIAL SERVICES · INDIA

A Private Sector Bank in India Strengthens Workforce Access Security and Cuts Onboarding Time with eMudhra SecurePass

SECTOR	REGION	SOLUTION
Banking & financial services	India	SecurePass

CLIENT OVERVIEW

The organisation is a private sector bank headquartered in south India, operating 320 branches and employing around 8,500 staff across retail banking, operations, and technology functions. The bank has been progressively moving more applications to cloud-hosted infrastructure over the past three years and has seen a corresponding increase in the complexity of managing employee access across a growing application landscape.

THE CHALLENGE

The bank's employees were managing separate login credentials for each of the 18 internal applications they regularly used — including the core banking system, loan origination platform, HR system, and productivity tools. There was no single sign-on capability and no centralised view of user access across the estate. New joiners typically waited three to four days to receive access to all the systems they needed, as each application required a separate provisioning request routed to different teams. More concerning, an internal audit found that 6% of active user accounts belonged to employees who had left the bank, with access not revoked after their exit. The bank's compliance team identified this as a control gap ahead of an RBI IT examination. Multi-factor authentication was in place only for internet banking and not for internal system access.

> *"We had staff with six or seven different passwords for different systems, and we had ex-employees with active accounts. Neither of those is acceptable from a security or compliance standpoint."*
>
> **Chief Information Security Officer**

THE SOLUTION

eMudhra deployed SecurePass to unify identity and access management across the bank's application estate. A centralised identity repository was set up, integrating with the bank's Active Directory and the HR system. Single Sign-On was configured for all 18 internal applications, giving employees access through a single authenticated session. MFA was enabled using OTP via SMS and an authenticator app, applied to all internal system logins and not just customer-facing channels. An automated joiner-mover-leaver workflow was built on top of the HR system integration — provisioning access on an employee's first day and revoking it immediately on exit. Role-based access control was configured for each application to ensure employees received only the access their job function required. The bank's IT team could now run access reviews from a single dashboard rather than querying each system individually.

RESULTS

The joiner-mover-leaver automation eliminated the backlog of stale accounts identified in the audit, with all accounts reconciled within two weeks of go-live. New joiners now receive full system access on their first day. The RBI IT examination team reviewed the deployment and closed the access control finding. Help desk calls related to password resets and access requests dropped noticeably in the first quarter post-deployment.

METRIC	BEFORE	AFTER
Stale accounts (ex-employees with access)	~6% of active accounts	Zero — automated revocation on HR exit trigger
Applications under SSO	0 — separate credentials per application	18 applications under unified SSO
New joiner access turnaround	3–4 days across manual requests	Day-one access via automated provisioning
MFA coverage — internal systems	Internet banking only	All internal application logins
RBI IT examination finding	Access control gap identified	Finding closed post-deployment

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.