SECUREPASS · GOVERNMENT & PUBLIC SECTOR · EAST AFRICA

A Public Utilities Authority in East Africa Reduces Insider Access Risk Across Field and Office Operations with eMudhra SecurePass

SECTOR	REGION	SOLUTION
Government & public sector	East Africa	SecurePass

CLIENT OVERVIEW

The organisation is a national public utilities authority in East Africa responsible for managing water and electricity distribution across urban and peri-urban areas. The authority employs around 3,500 staff spread across a head office, regional depots, and field operations units. Over the past two years the authority has been digitising its operations, including migrating billing, asset management, and field reporting systems to a centralised platform accessible by office and field staff.

THE CHALLENGE

As the authority's systems moved to a centralised platform, the IT team found itself managing user access across a growing range of applications with no unified tool. Accounts were created manually for each system when staff joined and were supposed to be closed when they left — but in practice, account deactivation depended on line managers remembering to notify the IT team, which did not always happen. A routine IT review found over 150 active accounts for staff who had left the authority over the previous two years. There was also no MFA in place for access to the billing system, which contained sensitive customer payment data. The authority's board had asked IT leadership to address the access management gaps as part of a broader operational risk reduction initiative.

> *"We had people who left two years ago with active accounts on our billing system. It wasn't a case of anyone doing anything wrong — the process simply didn't exist to close accounts consistently."*
>
> **Head of ICT**

THE SOLUTION

eMudhra deployed SecurePass across the authority's office and field workforce. An integration was built between SecurePass and the authority's HR system, automating account provisioning when new staff join and triggering deactivation when the HR record is closed on departure. The initial reconciliation deactivated all 150+ stale accounts identified in the review. MFA was deployed for the billing system and asset management platform using SMS OTP — suited to the authority's operating environment where staff use both smartphones and basic feature phones in field locations. SSO was configured for the centralised platform's key modules, giving office and field staff a single login for the applications they used regularly. Role-based access profiles were set up for the main staff categories — office administrators, field technicians, billing officers, and depot managers — with access scoped to the systems each role required.

RESULTS

All stale accounts were deactivated during the initial reconciliation. The billing system and asset management platform were MFA-protected within six weeks of deployment. The authority's IT review in the following quarter reported that account lifecycle management was now consistent and auditable for the first time.

METRIC	BEFORE	AFTER
Stale accounts deactivated	150+ for departed staff	All deactivated; automated lifecycle in place
Account lifecycle process	Manual; dependent on manager notifications	Automated HR-integrated provisioning and deactivation
MFA coverage — billing system	No MFA; customer payment data at risk	SMS OTP MFA enforced for billing access
SSO coverage	Separate logins per module	Single login for all platform modules
IT audit finding	Access management gaps flagged by board	Account lifecycle rated consistent and auditable

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.