SECUREPASS · TELECOMMUNICATIONS · SOUTHERN AFRICA

A Mobile Network Operator in Southern Africa Standardises Staff Identity and Reduces Account-Related Security Incidents with eMudhra SecurePass

SECTOR	REGION	SOLUTION
Telecommunications	Southern Africa	SecurePass

CLIENT OVERVIEW

The organisation is a mobile network operator in Southern Africa providing voice, data, and mobile financial services to approximately 5 million subscribers. The company employs around 1,100 staff across network operations, retail, customer care, finance, and IT functions. The operator has been working through a technology refresh programme over the past two years, and identity and access management was identified as a capability that needed to be modernised as part of that programme.

THE CHALLENGE

The operator's employees managed separate credentials for the network management system, billing platform, customer care tools, and HR system — four distinct logins for many staff, with no SSO in place. Password fatigue had contributed to a pattern of weak and reused passwords across systems, and the IT security team had logged three incidents in the prior 18 months involving compromised employee credentials — two related to phishing, one involving an account found to be sharing a password with a personal email account. There was also no formalised access review process, and the IT team was managing provisioning requests through a combination of email and verbal requests from line managers, which had resulted in over-privileged accounts accumulating over time.

> *"Three credential compromise incidents in eighteen months, all linked to weak or reused passwords, made it clear we needed MFA. The fragmented login experience was part of the problem — people reuse passwords when they have too many to remember."*
>
> **IT Security Manager**

THE SOLUTION

eMudhra deployed SecurePass to unify identity management and enforce stronger authentication across the operator's workforce. A centralised identity directory was established, consolidating user accounts from the four separate application stores. MFA was deployed using push notifications and SMS OTP, applied to all system logins. SSO was configured for the network management system, billing platform, customer care tools, and HR system — reducing the number of separate credentials each employee managed. Role-based access profiles were defined for the main workforce functions, and an access reconciliation exercise aligned existing accounts to appropriate role profiles, removing over-privilege that had accumulated from the informal provisioning process. An automated joiner-mover-leaver workflow was integrated with HR, and a formal semi-annual access review process was configured within SecurePass.

RESULTS

No credential compromise incidents have been recorded in the 14 months since MFA was deployed. The SSO rollout reduced the number of separate logins each employee managed from four to one. The IT security team closed the credential security risk item at the review following deployment.

METRIC	BEFORE	AFTER
Credential compromise incidents	3 incidents in 18 months	Zero in 14 months post-MFA deployment
Employee login experience	4 separate credentials for main systems	Single SSO login for all systems
MFA coverage	Not enforced	Push and SMS OTP for all workforce logins
Over-privileged accounts	Accumulated from informal provisioning	Aligned to role profiles in access reconciliation
IT security risk item	Credential security flagged as open risk	Closed at review following 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.