CASE STUDY

SECUREPASS · GOVERNMENT & PUBLIC SECTOR · INDIA

Data Hub of One of the State Governments in India Delivers a Unified Citizen Digital Identity Across State e-Governance Applications with eMudhra SecurePass IAM

SECTOR	REGION	SOLUTION
Government & public sector	India	SecurePass

CLIENT OVERVIEW

Data Hub of One of the State Governments in India (Data Hub of One of the State Governments in India) is the nodal state digital infrastructure agency of the State Government, responsible for providing the technology backbone that powers the state's e-Governance services and citizen-facing digital platforms. the state — India's most populous and economically significant state, home to over 120 million citizens — operates one of the country's most extensive state e-Governance ecosystems: spanning revenue and land records, citizen identity services, social welfare scheme delivery, agriculture support, health services, education portals, licensing and permits, transport, and inter-departmental data exchange. Data Hub of One of the State Governments in India provides the shared digital infrastructure that connects these services, and its mandate includes ensuring that the state's citizens can access government services digitally — with convenience, security, and equity — as the state advances its Digital Governance vision.

THE CHALLENGE

Across the state's e-Governance landscape, citizen-facing government services had been developed and deployed department by department — each portal built with its own registration system, its own login mechanism, and its own credential store. A citizen of the state seeking to access multiple government services — checking land records on one portal, applying for a social welfare scheme on another, renewing a licence on a third, and accessing health scheme benefits on a fourth — was required to create and maintain a separate digital identity for each department's system. The cumulative burden this placed on citizens was substantial: multiple usernames and passwords to remember, multiple registration processes to complete, and repeated authentication steps every time a different service was required. For the state's large rural population — many of whom access government services infrequently and through shared devices or assisted digital access points — this fragmentation was a direct barrier to service uptake.

> *"Our citizens were managing a different digital identity for every government service they needed. That is not what Digital the state means — it means one identity, one login, and seamless access to every service the state provides. SecurePass SSO gave us the platform to make that a reality."*
>
> **Director General, Data Hub of One of the State Governments in India**

The security implications of the fragmented identity landscape were equally significant. Multiple credential sets per citizen created multiple attack surfaces: weak or reused passwords across portals, proliferating accounts that citizens struggled to manage securely, and inconsistent authentication standards across departments — some portals enforcing basic password policies while others had no additional security controls at all. There was no unified fraud detection or anomaly monitoring capability spanning across the state's citizen application portfolio; suspicious activity on one portal was invisible to the security teams managing others. For government services handling sensitive personal data — land ownership records, Aadhaar-linked benefit eligibility, health records, and financial transactions — this inconsistency in authentication security created unacceptable risk for both citizens and the state.

From an operational and governance perspective, the siloed portal architecture made it impossible for Data Hub of One of the State Governments in India to maintain a unified view of citizen access patterns across the state's services — or to enforce consistent identity governance, access control policies, and compliance standards across all departments from a central platform. Each department's IT team managed its own user base independently, with no shared provisioning workflows, no cross-portal deprovisioning capability, and no consolidated audit trail. As the state's e-Governance portfolio expanded — with new citizen services being added regularly under the state's digital transformation programme — the fragmentation problem compounded, and the gap between citizen expectation and actual service experience widened.

THE SOLUTION

Data Hub of One of the State Governments in India deployed eMudhra's SecurePass IAM platform — with Single Sign-On (SSO) as the centrepiece — to establish a unified citizen digital identity framework across the state's e-Governance application portfolio, enabling every the state citizen to access all government services through a single, secure, centrally governed digital identity.

SecurePass IAM was deployed as the state-level identity broker for the state's citizen-facing government applications. A unified citizen identity repository was established, providing every registered citizen with a single, authoritative digital identity — one set of credentials, one profile, and one authenticated session that spans all integrated government portals and services. SecurePass SSO was configured across the state's e-Governance application portfolio using federated identity protocols, enabling the platform to act as the central authentication gateway for heterogeneous department portals — regardless of the underlying technology stack of each application. Citizens authenticate once at the SSO gateway and are seamlessly granted access to all services they are entitled to use within their session, eliminating the need to log in separately to each department's portal.

Authentication security was strengthened materially through the SSO deployment. Multi-Factor Authentication (MFA) was enforced at the unified SecurePass gateway — replacing the inconsistent, department-level password controls that had previously varied across portals with a consistent, state-wide authentication standard. Citizens accessing services involving sensitive personal data or high-value transactions are presented with step-up authentication requirements, ensuring that the security level applied to each service interaction is proportionate to the sensitivity of the data and transaction involved. By concentrating authentication into a single governed gateway, Data Hub of One of the State Governments in India gained the ability to apply and update security policies across all connected applications simultaneously — a capability that the previous departmental silo model made operationally impossible.

Role-Based Access Control (RBAC) and centralised identity governance were implemented across the full application portfolio: citizen entitlements to specific services are determined by verified identity attributes, eligibility criteria, and scheme enrolment status — all managed through SecurePass IAM's policy engine and propagated consistently across all connected portals. Automated citizen lifecycle management was deployed to govern the access implications of eligibility changes, scheme enrolments, and identity updates: when a citizen's eligibility status changes — through a scheme renewal, age-based transition, or administrative update — access entitlements across all relevant services are updated automatically, without manual intervention by individual department teams. A unified access audit trail spanning authentication events, service access, and identity changes across all connected applications provides Data Hub of One of the State Governments in India with the cross-portfolio governance visibility and accountability reporting needed to satisfy state IT audit requirements and demonstrate compliance with the national technology ministry's e-Governance security standards.

RESULTS

The deployment of eMudhra SecurePass IAM delivered a transformation in the state's citizen service experience and state e-Governance security posture — replacing a fragmented, department-by-department identity landscape with a unified, citizen-centric digital identity framework that serves the state's 120 million citizens across the state's entire e-Governance application portfolio.

METRIC	BEFORE	AFTER
Citizen Authentication Experience	Separate login per government portal	Single Sign-On across all the state e-Governance applications

METRIC	BEFORE	AFTER
Citizen Digital Identity	Fragmented; separate credentials per department	Unified digital identity for every the state citizen
Cross-Departmental Service Integration	Absent; siloed portals with no data linkage	Integrated service delivery across departments via shared identity
Identity Governance & Access Control	Inconsistent; no centralised policy enforcement	Centralised RBAC and policy governance via SecurePass IAM
User Provisioning & Lifecycle	Manual; administered per application	Automated provisioning and deprovisioning across all services
Security & Fraud Risk	High; multiple credential sets, inconsistent MFA	Reduced attack surface; MFA enforced at unified SSO gateway
Citizen Service Delivery Efficiency	Fragmented; high friction for multi-service access	Seamless multi-service access; significantly reduced citizen effort

Single Sign-On eliminated the credential fragmentation that had placed the burden of multiple digital identities on the state's citizens — including the state's large rural population, for whom that burden had been a genuine barrier to service access. With one identity and one login spanning all state government services, citizen adoption of digital government services increased, and the friction associated with multi-service access journeys was substantially reduced. The concentration of authentication into a single MFA-secured gateway raised the state's citizen portal security standard uniformly across all departments, closing the inconsistency gaps that had left some portals inadequately protected. Centralised identity governance gave Data Hub of One of the State Governments in India, for the first time, a unified operational view of citizen access across the state's e-Governance portfolio — enabling consistent policy enforcement, cross-departmental service integration, and the consolidated audit visibility needed to govern citizen data with the accountability that Digital the state demands.

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.