



A MOSIP Product

For more on eSignet



eSignet is a **digital identity verification tool** that simplifies access to online services – enabling inclusive, consent-based identity verification **using existing IDs**.

Designed for security, scale, and convenience, it allows individuals to log in or share verified information (eKYC) using IDs they already have – such as national or functional IDs from healthcare, education, or population registries. By eliminating the need for new IDs, eSignet streamlines access to digital services while ensuring user consent and data protection.

eSignet:

- Acts as a **login provider** for service providers, enabling individuals to access services without the need to create another set of login details
- Enables assured and **trusted identity verification** against recognised identity providers, ensuring high assurance and security
- Facilitates **profile creation and eKYC** through controlled, secure, and consent-based data sharing with service providers

An illustration of a person with blue hair, wearing a green shirt and dark pants, sitting on a large yellow padlock. They are using a laptop. The padlock has a dark blue keyhole. The background is a solid orange color.The eSignet logo, consisting of an orange '@' symbol followed by the word 'Signet' in white, is positioned above a list of key features. The list is numbered 01 through 09 and is set against a dark blue background with two vertical green lines.

eSignet

Key Features

- 01** Allows login with any trusted ID
- 02** Inclusive authentication via biometrics, OTP, and digital wallets
- 03** Supports integration with multiple ID registries and service providers
- 04** Quick and secure onboarding
- 05** Built-in consent collection
- 06** Protection against unwanted profiling
- 07** Multi-level assurance and secure protocols
- 08** Integration with digital wallets
- 09** KYC verified sign-up



User-Centric Architecture

- **One ID:** Access government and private sector services with a single, integrated identity credential.
- **Mandatory User Consent:** Built-in consent flows ensure users authorise access to personal information.
- **Flexible Authentication Options:** Supports multiple verification methods, including biometric and enhanced liveness detection.
- **Credential Integrity:** All authentication occurs within the eSignet platform, ensuring data is not shared with service providers without consent.

Advanced Authentication Framework

- **National-Scale Ready:** Built for robust, high-volume authentication and KYC.
- **Biometric Integration:** Leverages the Secure Biometric Interface (SBI) for advanced verification.
- **Standards-Based:** Built on OpenID Connect and OAuth 2.0 for seamless integration via trusted libraries for secure user authentication.
- **Enhanced Security:** Implements secure flows like authorisation code flow, with built-in fraud mitigation features.

Quick, Secure Digital Access

- **High-Assurance Methods:** Maintains the same verification standards as registration – OTP, biometrics, cryptographic keys.
- **Digital KYC Service:** Enables governments to offer secure digital verification and e-KYC services.
- **Seamless Integration:** Standards-based protocols reduce onboarding time for service providers.
- **Inclusive Access:** Multiple verification modes ensure accessibility across varying user contexts and devices.



Open Standards and Protocols

- **OAuth 2.0**
- **OIDC**
- **OpenID4VCI**
- **IEEE SA P3167 SBI**

Inclusivity at its Core

eSignet is designed to ensure inclusive access, the solution supports multiple verification models and modalities tailored to suit diverse user needs and device access.

Verification Models

- Assisted user verification and data collection
- Self-identification for online services

Verification Modalities

- **OTP authentication** for feature phone users
- **Face authentication** via wallet for smartphone users
- **Biometric authentication** through assisted modes for users without any devices

Why Choose eSignet?

- 01** Standards-driven
- 02** No vendor lock-in
- 03** Open source
- 04** Easy to integrate
- 05** Secure by design
- 06** Inclusive
- 07** Compatible with any trusted ID provider



Who Can Use eSignet?

Government Agencies

Add a secure, standards-based identity verification layer to existing identities.

Service Providers

Enable secure and efficient service delivery, identity verification, eKYC and consent-based data access across domains like banking, insurance, telecom, and welfare delivery.

Residents & Citizens

Access multiple digital services with one trusted credential – secure, simple, and consent-based.

Developers & System Integrators

Easily integrate digital ID authentication and eKYC into existing applications using open standards and tools, to test and demonstrate use cases.

Potential Use Cases

eSignet has the potential for broad application across public and private sectors, thereby enhancing efficiency and improving service delivery.

Social Welfare Programmes

Distribution of benefits to the eligible individuals.

Taxation

Simplifying tax filing and ensure taxpayer identification.

Voting Systems

Authenticating voters during elections.

Banking

Streamline customer onboarding process enabling secure transactions.

Insurance

Verifying identities during policy issuance and claims processing.

Border Control

Enhancing security at borders by verifying identities of travelers and ensuring secure cross-border movement.

