Government of India
Ministry of Communications & Information Technology
Department of Electronics & Information Technology
Controller of Certifying Authorities

eSign – Online Digital Signature Service

Introduction

Currently personal digital signature requires person's identity verification and issuance of USB dongle having private key, secured with a password/pin. Current scheme of physical verification, document based identity validation, and issuance of physical dongles does not scale to a billion people. For offering fully paperless citizen services, mass adoption of digital signature is necessary. A simple to use online service is required to allow everyone to have the ability to digitally sign electronic documents.

The eSign Service

eSign is an online service that can be integrated within various service delivery applications via an open API to facilitate digitally signing a document by an Aadhaar holder. It is designed for applying Digital Signature using authentication of consumer through Aadhaar authentication and e-KYC service.

Salient Features

❖ **Save cost and time**
❖ **improve user convenience**
❖ **Easy to apply Digital Signature**
❖ **Verifiable Signatures and Signatory**
❖ **Legally recognized**
❖ **Managed by Licensed CAs**
❖ **Privacy concerns addressed**
❖ **Simple Signature verification**
❖ **Short validity certificates**

❖ **Aadhaar e-KYC based authentication**
❖ **Mandatory Aadhaar ID**
❖ **Biometric or OTP (optionally with PIN) based authentication**
❖ **Flexible and fast integration with application**
❖ **Suitable for individual, business and Government**
❖ **API subscription Model**
❖ **Integrity with a complete audit trail**
❖ **Immediate destruction of keys after usage**
❖ **No key storage and key protection concerns.**

- **Easy and secure way to digitally sign information anywhere, anytime -** eSign is an online service without using physical dongles that offers application service providers the functionality to authenticate signers and perform the digital signing of documents using Aadhaar e-KYC service.

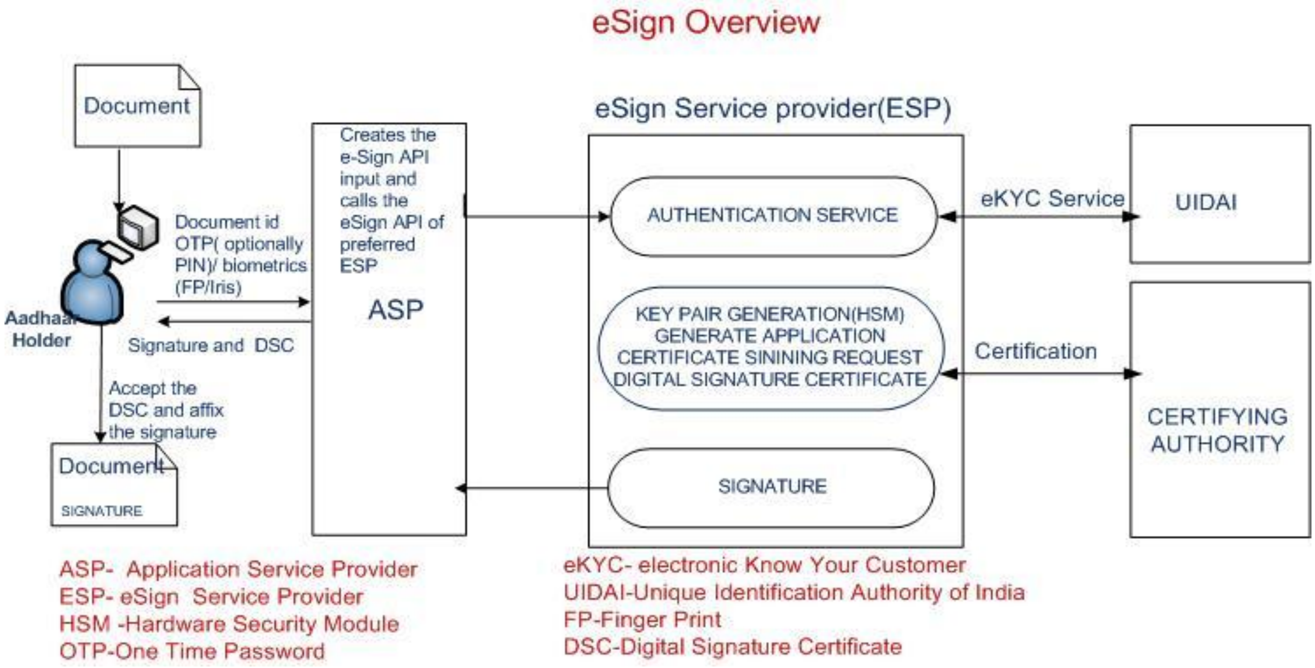
- **Facilitates legally valid signatures -** eSign process involves consumer consent, Digital Signature Certificate generation, Digital Signature creation and affixing and Digital Signature Certificate acceptance in accordance with provisions of Information Technology Act. It enforce compliance, through API specification and licensing model of APIs and comprehensive digital audit trail is established to confirm the validity of transactions, are also preserved.

- **Flexible and easy to implement -** eSign provides configurable authentication options in line with Aadhaar e-KYC service and also record Aadhaar id to verify the identities of signers. The signature option includes biometric or OTP authentication (optionally with PIN) through a registered mobile in the Aadhaar database. eSign enables millions of Aadhaar holders an easy way to access legally valid Digital Signature service.

- **Respecting privacy -** eSign ensure the privacy of the consumer by submitting only the thumbprint (hash) of the document for signature function instead of whole document.

- **Secure online service -** The eSign Service is governed by e-authentication guidelines. While authentication of the signer is carried out using Aadhaar e-KYC, the signature on the document is carried out on a backend server, which is the e-Sign provider. eSign services are offered by trusted third party service provider, currently Certifying Authority. To enhance the security and prevent misuse, certificate holder private keys are created on Hardware Security Module (HSM) and destroyed immediately after one time usage.

How eSign Works



eSign API and Gateway - eSign Application Programming Interfaces (APIs) define the major architectural components and also describe the format and elements of communication among the stake holders like Application Service Provider, Certifying Authorities, Trusted Third parties, Aadhaar e-KYC service and Application Gateway. This Standard eSign enable Application Service Providers to integrate eSign API in their Application with less effort. CDAC is functioning as eSign Gateway provider.

Who and where can use eSign - eSign have flexible subscription Model for individual users, business entities and Governments. eSign based on OTP (optionally with PIN) level authentication is suitable where risks and consequences of data compromise are low but they are not considered to be of major significance. eSign based on Biometric (Fingerprint/Iris) level authentication ideal for and risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.