eSign - Evolving Opportunities and Applications

CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

NOVEMBER 15, 2017
Presentation Outline

- e-Sign
- Architecture
- Interesting Challenges
- Roles and Responsibilities
- Evolving Applications
- Usage Scenario
Digital Signatures, IT Act and CCA

Most common and popular method for digital signature is through use of cryptographic USB token

◦ Private key of the signer is stored in token
◦ Password while accessing the token provides additional security

Requires application to be submitted to CA

Manual verification of identity – Role of RA
Overall Process

Manual Intervention

1. Subscriber provides Proof of Identity
2. RA verifies credentials basis assurance level
3. RA send passcode to subscriber
4. Subscriber creates Public private key pair
5. Submit Public Key with own details to CA
6. CA certifies public key of subscriber
7. CA publishes certificate in repository
8. CA provides certificate to subscriber
Government of India vide its Gazette Notification (January 2015) announced a method that facilitates CA to offer e-Sign service.

Objective of eSign service is to offer on-line service to citizens for instant signing of their documents securely in a legally acceptable form.

Two major challenges involved are:
- (a) authentication of the user
- (b) Trusted method of signing

Aadhaar eKYC service is used as PoA and PoI.

PKI method is used as a trusted method of signing.

Citizens with Aadhaar ID can use eSign service to obtain them digitally signed.
eSign Service

Offers on-line platform to citizens for instant signing of their documents securely in a legally acceptable form.

Enables citizens with valid Aadhaar ID and registered mobile number to carryout digital signing of their documents on-line.

Certifying Authority (CA) utilizes the service of Unique Identification Authority of India (UIDAI) for on-line e-authentication and Aadhaar eKYC Service.

CA under the Controller of Certifying Authorities (CCA)
e-Sign Overview
Highlights

Legally valid (CA under CCA and UIDAI)
- Aadhaar-eKyc – OTP
- Aadhaar-eKyc - Biometric (FP/Iris)

Privacy
- Hash of the document is obtained by ESP for digital signing
- Consent based

Paper-less
- Aadhaar based fully online electronic service

Ease of use
- No worry of safeguarding keys

Instantaneous and regulatory friendly
Architecture

Document

Aadhaar Holder

Accept the DSC and affix the signature

Document Signature

Application Service Provider (ASP)
Creates the eSign API input and calls the eSign API of preferred ESP

Authentication Service

eKVY service

UIDAI

Key Pair Generation (HSM)
Generate Application Certificate Signing Request
Digital Signature Certificate

Signature

Certification

Certifying Authority

HSM – Hardware Security Module
OTP – One Time Password
ESP – eSign Service Provider
ASP – Application Service Provider
eKVY – electronic Know Your Customer
DSC – Digital Signature Certificate
FP – Finger Print
UIDAI – Unique Identification Authority of India
e-Sign Framework

Communication between ASP and ESP defined as per CCA guidelines
Communication between ESP and UIDAI defined as per UIDAI guideline
Data exchange using secure channel (HTTPS)
Payload in the format of XML (POST)
RESTful web service interface

Offers 2 services
- OTP
- Esign

Response in PKCS7 format
Stakeholders in e-Sign Service

- **Clients**
  - Mobile / Tablet Applications
  - Desktop Applications
  - Internet Applications

- **Application Service Provider (ASP)**
  - Generate eSign API request and send it to Gateway or ESP directly

- **Gateway**
  - Connect to ESP directly for biometric (FP/Iris) or OTP authentication

- **eSign Service Providers (ESPs)**

- **Certifying Authorities (CAs)**

- **Aadhar eKyc Services**
Role of ASP

Citizen interacts with ESP through ASP only

Application to enable input of
- Aadhaar number
- OTP value (v1.0 specs)
- Document to be signed
- User consent for using his/her e-KYC data for generating Digital Signature Certificate (DSC)

Receive PKCS7 response

XMLs to be exchanged between ASP and ESP to be digitally signed

Maintain audit logs as per CCA guidelines
Role of ESP

- Receive Request XMLs from ASP
- Forward requests to CIDR for OTP generation and authentication of user
- Generate key pair for the user on HSM
- Sign the document hash using private key
- Generation of DSC for the user by C-DAC CA
- One time usage of key for signing – key pair deleted
- Supports document(s) signing
- Response to ASP in PKCS7 format (digital signature and certificate chain)
- Maintain audit logs as per CCA guidelines
Role of UIDAI

- Receive OTP request from ESP
- Send OTP to the registered mobile number
- Receive user authentication request from ESP
- User’s e-KYC given as response to ESP on successful authentication
eSign v2.0 Specs

Data exchange using secure channel (HTTPS)

Payload in the format of XML (POST)

RESTful web service interface

Offers eSign under 2 scenarios -
- User performs eKYC via ASP application and sends authenticated response for signing
  - PreVerified eKYC: enables ASP to leverage its KUA service for authentication purpose
  - ESP facilitates authentication of eSign user and uses the response for signing

Bulk signing facility – upto 10 document hashes can be signed in a single request

Response in PKCS7 format
eSign v2.0 Overall Flow

**eSign User**
- eSign user creates hash & request signature

**ASP**
- Redirect to ESP by submitting request XML

**ESP**
- ESP validates the details & initiates the process for eSign user authentication
- ESP obtains e-KYC response from e-KYC Provider

**Back End**
- e-KYC Service Provider
- Certifying Authority

**ESP**
- ESP obtains DSC and creates signature data
- ESP receives response (response URL)

**eSign User**
- eSign user verifies and affixes signature
Evolving Opportunities & Applications
## Evolving Opportunities

<table>
<thead>
<tr>
<th>Various Sectors</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Digital Locker</td>
<td>Self-Attestation</td>
</tr>
<tr>
<td>2. Financial Sector</td>
<td>Application for account opening in banks and post offices</td>
</tr>
<tr>
<td></td>
<td>(Loan processing,</td>
</tr>
<tr>
<td>3. E-Governance</td>
<td>Documents to be furnished by Citizen or being offered to citizen</td>
</tr>
<tr>
<td></td>
<td>(birth certificates, caste, marriage etc.)</td>
</tr>
<tr>
<td>4. Universities</td>
<td>Certificates and application forms for course enrollment and</td>
</tr>
<tr>
<td></td>
<td>exams</td>
</tr>
<tr>
<td>5. Health</td>
<td>Prescription, integration with HMIS, Telemedicine</td>
</tr>
<tr>
<td>6. Transport Department</td>
<td>Application for driving license renewal, vehicle registration</td>
</tr>
<tr>
<td>7. Telecom</td>
<td>Application of new connection</td>
</tr>
<tr>
<td>8. Legal</td>
<td>Documentation</td>
</tr>
</tbody>
</table>
Common Use Cases

Inter departmental Workflow automation (HR, procurement, claims etc in Govt.)

Business to Customer Services
  ◦ eSign enabled Online application

Business to Business
  ◦ eSign enabled online Process Flow
  ◦ eSign enabled online Legal Contracts
ESPs and Usage scenario

ESIGN SERVICE PROVIDERS

1. eMudra Ltd
2. Centre for Development of Advanced Computing (C-DAC)
3. (n)-Code Solutions
4. NSDL eGovernance Infrastructure Ltd
5. Capricorn Identity Services Pvt Ltd.
Costing models

Per signature costs

Costs towards ASP development and integration

Bulk-signing cost

User based pricing (packs)
References

https://authportal.uidai.gov.in/static/aadhaar_authentication_api_1_6.pdf
https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf
Thank You