India Updates

Asia PKI Consortium: Special Steering Committee Meeting
Indian Digital Certificate Userbase

1. 10 Million+ DSC (Long Lived Certificate) Users
2. 110 Million+ eSign (Short Lived Certificate) Users and growing.
3. National Regulator: Controller of Certifying Authorities
4. 15 Certifying Authorities licensed by Government
5. Signatures Trusted in Adobe & Microsoft Applications
Key Features of eSign

- Regulated common set of APIs by Government Regulator
- Wide implementation with numerous signing applications and use cases.
- Short Lived Key Pair, and Short Lived Certificates (30 minutes validity), LTV with CRL

Enrolment / Authentication / eSign Cost

**UIDAI / Aadhaar based: v2**
- 1.28 Billion Enrolments (95%+ Population)
- Easy Authentication with Aadhaar (National ID) + OTP
- Cost: USD 0.40 per transaction
- Limited by law for private use cases.

**CA/TSP acting as KYC Provider (Since 2019): v3**
- 3 Mn+ Enrolments. Seamless online enrolment with 5-10K+ users everyday.
- Easy Authentication with PIN + OTP, FIDO, Mobile App, Registered Device, etc
- Cost: USD 0.10 per transaction
- Used by all kind of use cases.
The Enrolment Process

1. User Request
   - Submits online request

2. Documents
   - Electronic Documents

3. Video Verification
   - Automated & Human Checks

4. Email & Mobile Verifications
   - Electronic Verifications

5. Organization Verification
   - Online Check with Business Tax Registry

6. Personal Tax ID Verification
   - Online Check with Personal Tax Registry

Quick processing | Completely Online | Less rejection ratio | Transparent to user | Mobile & PC Support
How eSign (Short Lived Certificates) Work in India

- **Document**
- **eSign User**
- **ASP**
  - Create eSign API input
  - Obtain signature from ESP
- **eSign Service Provider (ESP)**
  - Initialize
  - Key Generation
  - Certification
  - Signature Creation
  - Key Destruction
- **One Time User Enrolment (UIDAI / CA)**
- **Enroll**
  - e-KYC Provider (UIDAI / CA)
- **Auth**
- **Certifying Authority**
- **HSM**

- **Document ID & e-KYC ID**
- **Authentication**
- **Signature & DSC**

**Abbreviations**
- **HSM** – Hardware Security Module
- **ASP** – Application Service Provider
- **DSC** – Digital Signature Certificate
- **e-KYC** – electronic Know Your Customer
- **ESP** – eSign Service Provider

**Note:**
- The diagram illustrates the process of eSign in India, involving various steps such as user enrolment, authentication, and obtaining signatures from an eSign service provider. The process is facilitated by different providers and security mechanisms.
## Quick comparison: Traditional DSC v/s Online eSign

<table>
<thead>
<tr>
<th></th>
<th>DSC (Long Lived Certificate)</th>
<th>eSign (Short Lived Certificate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Type</td>
<td>Individuals &amp; Org Individuals</td>
<td>Individuals &amp; Org Individuals</td>
</tr>
<tr>
<td>Integration</td>
<td>Client system driver based integration</td>
<td>Fully online</td>
</tr>
<tr>
<td>Dependency</td>
<td>Desktop OS and crypto token is required</td>
<td>No dependency on Hardware</td>
</tr>
<tr>
<td>Password handling</td>
<td>After 10 failed attempt, certificate reissuance is required</td>
<td>Web portal based password reset options</td>
</tr>
<tr>
<td>Reissuance of certificate</td>
<td>Reissuance of certificate is required if token gets lost</td>
<td>No reissuance required</td>
</tr>
<tr>
<td>Hardware cost for User</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>OS Support</td>
<td>Limited OS support by token vendors</td>
<td>Cross browser cross OS support</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Driver and other troubleshooting required</td>
<td>High availability of service</td>
</tr>
<tr>
<td>Timestamping and LTV</td>
<td>Local Time / Application Dependent</td>
<td>Integrated Timestamping &amp; LTV</td>
</tr>
<tr>
<td>Bulk signing</td>
<td>Based on client system configuration</td>
<td>5 documents/transaction</td>
</tr>
<tr>
<td>Sign using mobile</td>
<td>Not possible</td>
<td>Yes. Compatible on any device</td>
</tr>
</tbody>
</table>
eMudhra enables enterprises and consumers to engage, exchange information and transact securely, efficiently and with enhanced customer experience.