e-Hastakshar: C-DAC's On-line Digital Signing Service

1. What is a Digital Signature?

Currently, many applications or forms submitted by a citizen require physical signature of the citizen. A digital signature takes the concept of traditional paper-based signing and turns it into an electronic "fingerprint." This "fingerprint," or coded message, is unique to both the document and the signer and binds them together. In short, a digital signature has the same function as that of a handwritten signature. Some of the salient features of digital signature are non-repudiation, integrity and authenticity. The Information Technology Act 2000 provides the required legal sanctity to digital signatures based on asymmetric crypto systems.

2. Who can avail e-Sign service to sign the documents?

Any Indian citizen having Aadhaar with Registered mobile number.

3. Who provides Digital Signature Certificate to ASPs?

Any Certifying Authority (CA), who is licensed by a Controller of Certifying Authorities (CCA).

4. What is Aadhaar Paperless Offline KYC?

It is a secure sharable document which can be used by any Aadhaar number holder for offline verification of Identification. Aadhaar holder will download the document, which contain Name, Address, Photo, Gender, DOB, Mobile Number (In hashed form) and Email Address (In hashed form) in a digitally signed XML. However, this document does not contain Aadhaar number.

5. How to share this Paperless Offline eKYC document with the ESP?

Aadhaar holders can share the XML ZIP file along with the Share Code to ESP as per their mutual convenience.

6. What are the modes on which OTP shall be received by Aadhaar holder for authentication purpose in eSign 2.1?

e-Hastakshar enables Document signer to receive the OTP on registered Mobile number. In case mobile number is not registered with Aadhaar, an error code of 112 will be returned.

7. Is biometric supported in esign 2.1?

Yes

8. Is biometric supported in esign 3.0?

No

9. Is it mandatory to create signer ID in eSign 3.0?

Yes, it is mandatory to create signer ID for offline process.

10. What is the validity of Offline KYC XML?

3 Months

11. What is the validity of signer ID?

2 Years.

12. What are the main features of eSign 2.1 specifications?

eSign 2.1 facilitates capturing of Authentication ID and authentication data of the individual to be carried out by ESP. eHastakshar uses the service of UIDAI for authenticating the document signer through its e-KYC mechanism.

13. What are the main features of eSign 3.0 specifications?

Features of eSign 3.0:

- One time registration process is defined between an eSign User and eSign Service Provider (ESP) based on offline Aadhaar eKYC XML.
- eSign CA also maintains eKYC data of verified users for issuance of DSC
- Once verified, eKYC data can be used for 2 years
- For each DSC issuance, 2 factor authentication is required
- Authentication modes supported: OTP/TOTP/MobileAccessToken with PIN (currently C-DAC supports only OTP with PIN)
- Up to 5 document hashes can be signed in a single transaction
- Signer can view document submitted for signing at ESP Authentication Page and can de-select a document for signing

14. Is bulk signing supported eSign 2.1? If so details.

No

15. Is bulk signing supported in eSign 3.0? If so details.

Yes, Up to 5 document hashes can be signed in a single transaction

16. What are the modes on which OTP shall be received by Aadhaar holder for authentication purpose?

e-Hastakshar enables Document signer to receive the OTP on registered Mobile number based on eKYC service.

17. What is licensing model of APIs?

Not Applicable

18. What is eSign API license key?

It is the ASP-ID given by ESPs after sharing required details with ESPs. Refer http://www.cca.gov.in/cca/?q=eSign.html.

19. How to ensure that the ASP-ID will remain unique?

C-DAC will allocate and will ensure the uniqueness.

20. ASP should make sure that the affixing of digital signature to document or storage of digital signature only after the signatory's approval of contents of certificate and signature.

ESP will return the signed hash of the document along with the document signer's public certificate. ASP has to affix/store the digital signature after presenting the details to the signer and taking their explicit consent for the same.

21. What are the different security and audit requirement to be carried out for the ASP application?

There are two aspects of security and audit assessment to be carried out: a) Security assessment of the application by ICERT empanelled agency where the security threats, vulnerabilities etc. are carried out for the ASP application and its environment (OS, web server etc.) b) Application audit to be carried by IS certified auditor to ensure the application data, logs etc. are maintained as per Annexure-11.

22. Whether eSign online Electronic Signature Service is a replacement for the existing Digital Signature?

No. The existing method of obtaining Digital Signature Certificate by submission of a paper application form to a Certifying Authority, key pair generation by applicant Certification of public key of applicant by a Certifying Authority, signature generation as and when required using signature generation tools/utilities , safe custody of key pairs on Crypto tokens by DSC holder till the expiry of Digital Signature Certificate, etc. will continue to exist along with eSign Online Electronic Signature Service . The Application Service Provider determines the suitability of eSign Online Signature service in their application.

23. Is my privacy protected?

Yes. Document content that is being signed is not sent in the clear to eSign service provider. The privacy of signer's information is protected by sending only the one-way hash of the document to eSign online Electronic Signature Service provider. Each signature requires a new key-pair and certification of the new Public Key by a Certifying Authority. This back-end process is completely transparent to the signer. In addition, e-KYC data based on offline Aadhaar XML is not sent back to the Application Service Provider and is retained only within the eSign provider as the e-KYC audit record.

24. How much does it cost to use eSign?

The payment model can be mailed to you upon request.

25. Can we control the e-signature appearance? Is that configurable? Can we use our own logo/font? Can we control the size and placement of the signature box on the document?

Yes, it is customizable.

26. Can the same document be signed by multiple people?

Yes, it can be signed by multiple people. It will involve multiple transactions, involving the same document.

27. If the internet connection is lost during an eSign request process - Is the entire process re-initiated or does it resume from the point when the internet connection was lost, once the internet connection is available?

The transaction will have to be re-initiated.