eSign FAQ

1. What is the online eSign Electronic Signature Service?

eSign Electronic Signature Service is an innovative initiative for allowing easy, efficient, and secure signing of electronic documents by authenticating signer using e-KYC services. With this service, any eSign user can digitally sign an electronic document without having to obtain a physical digital signature dongle. Application Service Providers can integrate this service within their application to offer eSign user a way to sign electronic forms and documents. The need to obtain Digital Signature Certificate through a printed paper application form with ink signature and supporting documents will not be required.

The Digital Signature Certificate issuance and applying of signature to electronic content is carried out in few seconds with eSign. Through the interface provided by the Application Service Provider (ASP), users can apply electronic signature on any electronic content by authenticating themselves through biometric or OTP using e-KYC services. The interfaces are provided to users on a variety of devices such as computer, mobile phone etc. At the backend, eSign service provider facilitates key pair generation and Certifying Authority issues a Digital Signature Certificate. The eSign Service Provider facilitates creation of the Digital Signature of the user for the document which will be applied to the document on acceptance by the user.

2. Where the eSign Online Electronic Signature Service can be used?

An Application Service Provider (ASP) can integrate eSign online electronic signature service so that the users of that ASP will be able to use eSign. A physical paper form/document which is currently used to obtain digital signature certificate can be replaced by its electronic form and thereby facilitate electronic signature of the signer through eSign.

ASPs who can be potential users of eSign include Government agencies, Banks and Financial Institutions, Educational Institutions etc.

3. Can you provide some use-cases of eSign online Electronic Signature Service?

eSign online Electronic Signature Service can be effectively used in scenarios where signed documents are required to be submitted to service providers – Government, Public or Private sector. The agencies which stand to benefit from offering eSign online electronic signature are those that accept large number of signed documents from users.

Some applications which can use eSign for enhancing for enhancing services delivery are the following:-

Digital Locker	✓ Self attestation
Tax	✓ Application for ID, e-filing
Financial Sector	✓ Application for account opening in banks and post office
Transport Department	✓ Application for driving licence renewal, vehicle registration
Various Certificates	✓ Application for birth, caste, marriage, income certificate etc
Passport	✓ Application for issuance, reissue
Telecom	✓ Application for new connection
Educational	✓ Application forms for course enrollment and exams
Member of Parliament	✓ Submission of parliament questions

4. What are the challenges to be addressed using eSign- Online Electronic Signature Service?

Personal digital signature certificate requires person's identity verification and issuance of USB dongle to store private key. The access to private key is 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 hassle-free 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.

5. What are the objectives of eSign online Electronic Signature Service?

eSign Online electronic signature service, offers applications a mechanism to replace manual paper based signatures by integrating this service within their applications. An eSign user can electronically sign a form/document anytime, anywhere, and on any device. eSign service facilitates significant reduction in paper handling costs, improves efficiency, and offers convenience to customers.

6. 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.

7. What are the major difference between traditional digital Signatures eco system and new eSign online Electronic Signature Service?

In the traditional Digital Signature system, an individual is responsible for applying for a Digital Signature Certificate to CA, key pair generation and safe custody of keys. The Certifying Authorities issue Digital Signature Certificate to individuals after verification of credentials submitted in the application form. Such Digital Signature Certificates are valid for 2-3 years. Individual can affix digital signature any time during the validity of Digital Signature Certificate. The certificates are revoked in case of loss or compromise of keys. The verification of the individual's signature requires the verification of whether the DSC is issued under India PKI and also ascertaining the revocation status of the DSC. Key pairs are stored in Crypto Tokens which comply with standards mentioned in the Information Technology Act & Rules to prevent the duplication of keys. It is individual's obligation for safe custody of Crypto Tokens. The signatures are created using the keys certified by CA.

In the new eSign online Electronic Signature Service, based on successful authentication of individual using e-KYC services, the key pairs generation, the certification of the public key based on authenticated response received from e-KYC services, and digital signature of the electronic document are facilitated by the eSign online Electronic Signature Service provider instantaneously within a single online service. The key pairs are used only once and the private key is deleted after one time use. The Digital Signature Certificates are of 30 minutes validity, and this makes verification simple by eliminating the requirements of revocation checking. Document that is signed using eSign will contain a valid digital signature that can be easily verified using standard methods.

8. 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.

9. Whether it is a legally valid signature?

Yes. The Electronic Signatures facilitated through eSign Online Electronic Signature Service are legally valid provided the eSign signature framework is operated under the provisions of Second Schedule of the Information Technology Act and Guidelines issued by the Controller. Please refer *Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 - e-authentication technique using e-KYC services*.

10. Who can provide eSign- Online Electronic Signature Service?

eSign Online Electronic Signature Service is offered by CAs.

11. Who can integrate eSign- Online Electronic Signature Service in their application?

The agency who intent to integrate eSign service should either be:

- A Central/ State Government Ministry / Department or an undertaking owned and managed by Central / State Government, or
- An Authority constituted under the Central / State Act, or
- A Not-for-profit company / Special Purpose organization of national importance, or
- A bank / financial institution / telecom company, or
- A legal entity registered in India

Such entities are referred to as "Application Service Providers" (ASP).

12. What are the requirements for integrating eSign- Online Electronic Signature Service in an application?

- The ASP can apply to eSign Service Provider for integrating eSign- Online Electronic Signature Service in their application as mentioned in the On-Boarding Guidelines. The eSign-Online Electronic Signature Service provider allows access to ASPs after fulfilling the criteria mentioned in the On-Boarding Guidelines.

13. What are the requirements for using eSign- Online Electronic Signature Service for application users?

The user should have e-KYC identification Number. For OTP based authentication, the mobile number should be registered with ESP Database.

14. Where does someone get assistance for integration of their application with eSign- Online Electronic Signature Service?

The communication between Application Service Provider and eSign- Online Electronic Signature Service is operated in accordance with eSign API Specifications.

15. How does an application provider avail services of more than one eSign Online Service provider?

eSign APIs are designed to interact with one or more eSign Online Electronic Signature Service providers. If application provider desires to interact with only one ESP, it should use the name of the eSign Online Service provider and communication link as mentioned in the eSign API specifications. In the case of multiple eSign Online Service providers, the ASP can manage the service by local integration.

16. Is there any additional authentication required in the case of e-KYC OTP option?

Yes, the following are the options

- **ASP level logon/Password authentication**: Though e-KYC OTP option is relevant to environments where the risks and consequences of data compromise are low and they are not considered to be of major significance. An application level authentication is recommended for eSign Online Electronic Signature Service.

17. How can one ensure that the authentication to application and to eSign Service is by the same person?

In the application implementation, an individual is identified using a code or number instead of name. For example in the case of income TAX e-filing, the person is identified by a PAN number. It is a challenge for application to ensure that the individual who have logon using PAN id is the person who has signed the documents. Mapping (seeding) the individual's application specific ID with their e-KYC identification number in the ASP database is recommended to enable the authenticity of the signature.

18. Can you provide a sample usage scenario for eSign online Electronic Signature Service?

Individuals can use Digital Locker (http://digilocker.gov.in/) to store the electronic copy of their identities/Certificates/etc at a central location. The electronic documents placed in the repository of Digital Locker can be accessed or the link can be shared for verification requirements. These electronic documents can be electronically signed (self-attestation) using eSign Online Electronic Signature Service for integrity and authenticity.

19. What are the different classes of certificates in the eSign Electronic Signature Service?

Based on the verification of identity of individuals and storage of key pairs, three classes of certificates are issued in the traditional way of obtaining Digital Signatures Certificates from a Certifying Authorities. In the case of eSign Online Electronic Signature Service, the Digital Signature Certificates are issued in the following classes.

- **e-KYC – OTP**: class of certificates is issued to individuals use based on OTP authentication of subscriber through - e-KYC Service.

- **e-KYC -Biometric** - Biometric class of certificate is issued based on biometric authentication of subscriber through e-KYC service.

20. Whether Electronic Signatures can be applied to any electronic content of individual's choice?

An individual can obtain Digital Signature Certificate from the existing DSC issuance framework and can be used to digitally sign the electronic content of choice subject to the acceptability of such class of certificate by the relying parties and the validity of the DSCs.

eSign Online Electronic Signature Service are offered to individuals by Application Service providers. In the eSign Online Electronic Signature Service, the choice of type of electronic content on which electronic signatures can be applied are limited to option provided by ASPs.

21. How the trustworthiness of the eSign Online Electronic Signature Service is ensured?

Upon the biometric or OTP authentication of the individual with the already verified information kept in the database of e-KYC provider, key pairs are generated and public key along with information received from e-KYC provider are submitted to CA for certification. Immediately after signature is generated with the private key of individual, the key pairs are deleted. The key pairs are generated on Secure Hardware Security Module to ensure security and privacy.

Audit log files are generated for all events relating to the security of the eSign-Online Electronic Signature Service. The security audit logs are automatically collected and digitally signed by ASPs. All security audit logs, both electronic and non-electronic, shall be retained and are audited periodically.

22. Who owns the eSign Electronic Signature Service and who are the beneficiaries?

eSign Service Providers offer the eSign Online Electronic Signature Service. Application Service Providers and individuals availing service of ASP are the beneficiaries. eSign Online Electronic Signature Service enables ASP to create paperless environment and individual beneficiaries of ASP save cost and time by using this remote signature capability

23. Who are the providers of eSign Electronic Signature Service at present?

At present following providers offer this service. In future, more providers may be added. Please check CCA website (http://esign.gov.in) for updated information.

1. e-Mudhra CA
2. (n)Code Solutions CA
3. CDAC CA
4. NSDL eGov CA

24. How much does it cost to use eSign?

Application service providers can do a price discovery and get the best offer from any of the providers. Depending on the volume and usage, pricing may vary. With large scale adoption and multi-provider ecosystem, market forces will automatically provide the best price for the

application providers. Considering high cost of physical paper handling , archival audit etc. application providers can work out the return of investment easily.

25. What are the requirements for enabling application with eSign Electronic Signature Service?

- ASP should be Service Integrator of eSign online Electronic Signature Service for one or more CAs.
- Integrate eSign API in the application of ASP
- Audit, as per the guidelines of CCA.
- eSign user should have e-KYC identification Number (and registered mobile for OTP based authentication). For biometric based authentication , the individual should have access to biometric capturing device
- ASP database should be seeded with e-KYC identification number to ensure that authenticity of the signer is verifiable by ASP.

26. What is the validity of Digital Signature Certificate?

The Digital Signature Certificate used to verify the signature will be valid for 30 minutes and the private key will be immediately deleted after signing. This eliminates any misuse of the certificate and simplifies the need for checking revocation list during signature verification.

27. Whether the Digital Signature Certificate is revocable?

Revocation of certificate is not necessary as the certificate validity is 30 minutes and private key is deleted immediately after signature creation.

28. Whether a complete paperless office can be setup using eSign Electronic Signature Service?

Yes, Usage will be dependent on the domain requirements. The ASP can use biometric or OTP based authentication for different class of DSCs.

29. Who is responsible for archival of signature?

Both eSign online Electronic Signature Service provider and Application Service providers are responsible for archival of their data and application logs. The eSign online Electronic Signature service provider's logs should include the information received from ASP and also the signature created.

****