



Adobe Acrobat Sign



WHITE PAPER

Adobe Acrobat Sign Solutions

**An Analysis of Shared Compliance Responsibilities under
the Indian Information Technology Act, 2000**

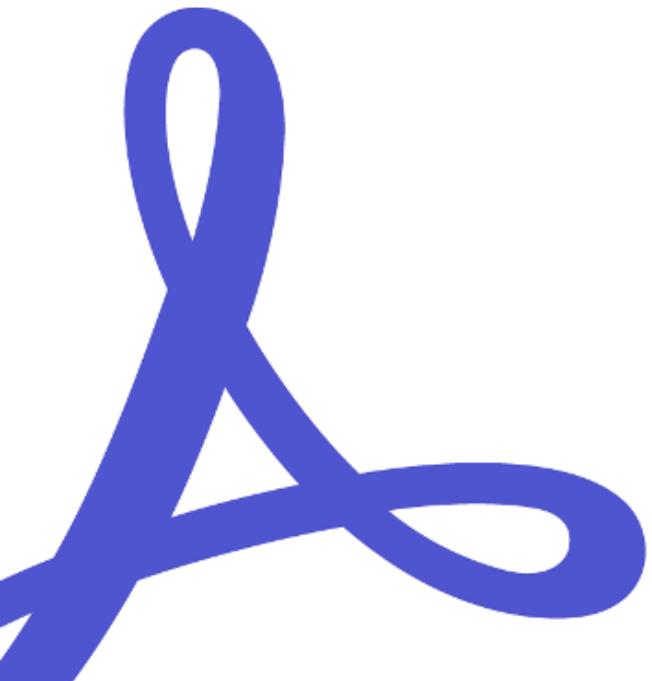


Table of Contents

1. Introduction	3
2. Scope	3
3. Conformance with Regulations	3
Information Technology Act, 2000	4
Associated Rules prescribed under the IT Act	9
Annexure	17
4. Additional Resources	17
5. Contact Info	17
6. Disclaimer	18
7. Glossary	18

1. Introduction

Indian law has recognized electronic signatures, or e-signatures, under the Information Technology Act, 2000 ("IT Act") for over 20 years. With its increased emphasis on improving the ease of doing business; digital inclusion, streamlining the storage of records; and improving the safety, security, and cost-effectiveness of electronic records, the Government of India has promoted the use of digital technologies by Indian citizens and corporations. As a result, there has been a recent increase in the use of e-signatures in India.

This paper presents an analysis of the technical features and relevant integrations that, if properly implemented, allow for the application of signatures compliant under the IT Act using Acrobat Sign Solutions. This assessment focuses on how Adobe, licensed Certifying Authorities ("CAs"), eSign Service Providers ("ESPs") and the organization using Acrobat Sign Solutions share responsibilities for achieving compliance with the IT Act.

2. Scope

This paper focuses on the compliance profile of the Acrobat Sign Solutions (e.g., Aadhaar eSign service and Digital ID (sign using tokens)), alongside the tools and features of Acrobat Sign Solutions, that can be used to help customers comply with the requirements with the IT Act requirements.

The intended reader of this paper is an organization using Acrobat Sign Solutions looking to achieve compliance requirements under the IT Act ("Customer").

3. Conformance with Regulations

The following chart discusses how Acrobat Sign Solutions supports Customer compliance with the IT Act and its related rules/regulations. This chart highlights shared responsibilities among Adobe, CAs, ESPs and Customers related to the IT Act and its related Rules.

An important preliminary responsibility to highlight, is that this chart is predicated on the Customer (i) performing its responsibility to purchase the Aadhaar eSign service from Adobe, obtain the license to use the Aadhaar eSign service provided by Protean via integration with the Acrobat Sign Solutions product, and configure its account to use the Aadhaar eSign service or (ii) using Digital ID (using tokens), where Customers sign using a security token or hardware token connected to their computer.

Note that several sections of the IT Act and its rules/regulations are not discussed in the following chart because the excluded sections are not relevant to the requirements for the formation of a valid electronic signature. Moreover, Adobe is not directly responsible for meeting the legal requirements of the IT Act and its rules/regulations. Adobe only helps its Customers meet the standards required under the IT Act. Please also note that defined terms are bolded and appear alphabetically in a glossary at the end of this article.

Information Technology Act, 2000			
Citation	What the Law Requires	Stakeholder responsible for compliance CA/Adobe/ESP/ Customer	How Acrobat Sign Solutions Supports Customer Compliance
IT Act Chapter 2; Section 3	<p>This provision explains how a subscriber can authenticate an electronic record using their digital signature.</p> <p>The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record, where any person by the use of the public key of the subscriber can verify the electronic record. The private key and the public key must be unique to the subscriber and constitute a functioning key pair.</p>	Customer (Signer)	<p>Adobe collaborates with CAs to provide Customers who are signers with a compliant solution.</p> <p>Adobe is an Application Service Provider ("ASP") that offers Aadhaar eSign service as a part of Acrobat Sign Solutions. Adobe has partnered with Protean eGov Technologies Ltd (formerly NSDL e-Governance Infrastructure Ltd) ("Protean"), a CA that is empanelled as an ESP to provide its users with this Aadhaar eSign service. Taken together, Customers can authenticate electronic records with digital signature technology using the Aadhaar eSign service in Acrobat Sign Solutions.</p> <p>In addition, Adobe partners with a CA, eMudhra Limited ("eMudhra"), to obtain a Document Signer Certificate ("DS Certificate") that meets the Controller of Certifying Authorities ("CCA") requirements.</p> <p>Adobe applies a DS Certificate using asymmetric crypto systems to all documents signed using security tokens to confirm proof of origin and integrity and to also act as a tamper evident seal.</p>
IT Act Chapter 2; Section 3A	<p>A subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which is considered reliable and may be specified in the Second Schedule of the IT Act.</p> <p>An electronic signature or electronic authentication technique shall be considered reliable if-</p> <ul style="list-style-type: none"> • the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person; • the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person; • any alteration to the electronic signature made after affixing such signature is detectable; • any alteration to the information made after its authentication 	Customer (Signer)	<p>Acrobat Sign supports electronic signatures using the Aadhaar eSign service or the Digital ID (using security tokens). As signature affixed using Adobe Sign Solution meets the specific requirements for a reliable electronic authentication technique as described in Section 3A of the IT Act.</p> <p>See our comment to Rule 3 above as well our comments to the Second Schedule separately discussed below.</p>

	<ul style="list-style-type: none"> by electronic signature is detectable; and it fulfils such other conditions which may be prescribed under the IT Act. 		
IT Act; Chapter 5; Section 15	<p>An electronic signature shall be deemed to be a secure electronic signature if:</p> <ul style="list-style-type: none"> the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and the signature creation data was stored and affixed in such exclusive manner as may be prescribed. 	<p>CA / Customer (Signer)</p> <p>No direct compliance obligation on Adobe because it does not manage the signature creation data on behalf of the signer.</p>	<p>CAs and CAs empanelled as ESPs are required to ensure that compliances related to the signature creation data are fulfilled.</p> <p>Indian law only presumes a digital signature from a licensed CA to be legally valid. The CAs (including ESPs) are responsible for identifying / authenticating the signatory and for managing the signature creation data.</p> <p>Adobe has partnered with a CA empanelled ESP, Protean, which generates a digital signature after undertaking identity verification of the signatory. Similarly, it partners with a CA, eMudhra, for the Digital ID (using security tokens) solution.</p>
IT Act; Chapter 5; Section 16	<p>This section allows the Central Government to prescribe the security procedures and practices.</p> <p>The Information Technology (Security Procedure) Rules, 2004 are the rules prescribed under this section of the IT Act, which are discussed separately below.</p>	N/A	N/A
IT Act; Chapter 5; Section 30	<p>This section provides specific obligations on every CA, including requirements to:</p> <ul style="list-style-type: none"> make use of hardware, software, and procedures that are secure from intrusion and misuse; provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions; adhere to security procedures to ensure that the secrecy and privacy of the electronic signature are assured; be the repository of all Electronic Signature Certificates issued under this Act; publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and observe such other standards as may be specified by regulations. 	<p>CA</p> <p>No direct compliance obligation on Adobe.</p>	<p>Please see our comment against Rule 15 above.</p> <p>Adobe has partnered with a CA empanelled as an ESP, Protean, and another CA, eMudhra, which are required to ensure compliance with these requirements.</p>
IT Act; Chapter 5; Section 40	<p>Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, the subscriber shall generate that key pair by applying the security procedure.</p>	<p>CA / Customer (Signer)</p> <p>No direct compliance obligation on Adobe.</p>	<p>Adobe permits customers to affix their digital signatures issued by CAs, including ESPs.</p>

IT Act; Chapter 5; Section 40-A	In respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed.	Customer	Please note that the Digital Signature (End entity) Rules, 2015 issued under the IT Act prescribes duties on customers. These have been captured separately below.
IT Act; Chapter 5; Section 42	This section requires each subscriber to exercise reasonable care to retain control of the private key corresponding to the public key listed in their Digital Signature Certificate and mandates that if such private key is compromised the subscriber must communicate this to the Certifying Authority.	Customer (Signer)	N/A

THE SECOND SCHEDULE: Electronic signature or electronic authentication technique and procedure

<p>IT Act; The Second Schedule; Sl No. 1: e-authentication technique using Aadhaar or other e-KYC services</p>	<p><u>Authentication of an electronic record by e-authentication technique which shall be done by:</u></p> <ul style="list-style-type: none"> • the applicable use of e- authentication, hash, and asymmetric crypto system techniques, leading to issuance of Digital Signature Certificate by CA • a trusted third party service by subscriber's key pair-generation, storing of key pairs and creation of digital signature provided that the trusted third party shall be offered by the CA. The trusted third party shall send application form and certificate signing request to the CA for issuing a Digital Signature Certificate to the subscriber. • Issuance of Digital Signature Certificate by CA shall be based on e-authentication, particulars specified in Form C of Schedule IV of the Information Technology (Certifying Authorities) Rules, 2000, digitally signed verified information from Aadhaar or other e-KYC services and electronic consent of Digital Signature Certificate applicant. • The manner and requirements for e- authentication shall be as issued by the Controller (CCA) from time to time. • The security procedure for creating the subscriber's key pair and other e- KYC services shall be in accordance with the e-authentication guidelines issued by the CCA. • The standards referred to in Rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 shall be complied with, in so far as they relate to the certification function of public key of Digital Signature Certificate applicant. • The manner in which the information is authenticated by means of digital signature shall comply with the manner and standards specified in Rules 3 to 12 of the Digital Signature (End entity) Rules, 2015 in so far as they relate to the creation, storage, and verification of Digital Signature 	<p>CA empanelled as an ESP No direct compliance obligation on Adobe.</p>	<p>Acrobat Sign supports electronic signatures using the Aadhaar eSign service provided by Protean. The CCA regulates the issuance and use of electronic signature service (eSign) in India. CCA prescribes the regulations which the CA and the ASP must adhere to. Through this service, CAs empanelled as ESPs enable ASPs to facilitate their users to digitally sign a document using PAN Card / Aadhaar Number. Adobe, as an ASP, has entered into arrangements with a CA empanelled as an ESP i.e., Protean, to provide its users with the Aadhaar eSign service. Adobe has been on-boarded by the ESP after fulfilling certain stipulated criteria. For each electronic signature generated using Aadhaar, Adobe users will be required to agree to the terms and conditions of Protean, and authorize Protean to use their Aadhaar number to authenticate their identity through OTP verification and then authenticate the electronic record.</p>
--	---	--	---

<p>IT Act; The Second Schedule; SI No. 2: e-authentication technique and procedure for creating and accessing subscriber's signature key facilitated by trusted third party</p>	<p><u>Authentication of an electronic record by e-authentication technique which shall be done by:</u></p> <ul style="list-style-type: none"> • the applicable use of e-authentication, hash and asymmetric crypto system techniques leading to issuance of Digital Signature Certificate by CA, provided that CA shall ensure the subscriber identity verification, secure storage of the keys by trusted third party and subscriber's sole authentication control to the signature key. • Identity verification of Digital Signature Certificate applicant shall be in accordance with the Identity Verification Guidelines issued by CCA from time-to-time. • The requirement to operate as trusted third party shall be specified under e-authentication guidelines issued by the CCA. • A trusted third party shall <ul style="list-style-type: none"> ◦ facilitate Identity verification of Digital Signature Certificate applicant; ◦ establish secure storage for subscriber to have sole control for creation and subsequent usage of subscriber's signature key by sole authentication of subscriber; ◦ facilitate key pair-generation, secure storage of subscriber's signature key and facilitate signature creation functions; ◦ facilitate the submission of Digital Signature Certificate application form and certificate signing request to the CA for issuing a Digital Signature Certificate to the Digital Signature Certificate applicant, and ◦ facilitate revocation of Digital Signature Certificate and destruction of subscriber's signature key. • The manner and requirements for authentication and storage of keys shall be as issued by the CCA from time to time under e-authentication guidelines • The security procedure for creating the subscriber's key pair shall be in accordance with the e-authentication guidelines issued by the CCA. • The standards referred to in Rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 shall be complied with, in so far as they relate to the certification function of public key of Digital Signature Certificate applicant. • The manner in which information is authenticated by means of digital signature shall comply with the manner and standards specified in Rule 3 to 12 of Digital Signature (End entity) Rules, 2015 in so far as they relate to the creation, storage and verification of Digital Signature. 	<p>CA No direct compliance obligation on Adobe. Note: Trusted third party service providers here refer to CAs licensed under the IT Act.</p>	<p>Acrobat Sign does not directly control the authentication of signers for the issuance of digital signature certificates. Instead, Adobe has partnered with a CA, eMudhra, which is expected to be compliant with these rules, to generate signature certificates for documents. The document signer certificates provided by eMudhra ensure proof of origin and document integrity to all documents signed in the Adobe Acrobat Sign platform.</p>
---	--	--	---

Associated Rules prescribed under the IT Act			
Information Technology (Certifying Authorities) Rules, 2000			
Citation	What the Law Requires	Stakeholder responsible for compliance CA/Adobe/ESP/ Customer	How Acrobat Sign Solutions Supports Customer Compliance
Information Technology (Certifying Authorities) Rules, 2000; Rule 3	<p>The manner in which information be authenticated by means of Digital Signature. A Digital Signature shall:</p> <ul style="list-style-type: none"> • be created and verified by cryptography that concerns itself with transforming electronic record into seemingly unintelligible forms and back again; • use what is known as Public Key Cryptography and hash function shall be used in both creating and verifying a Digital Signature. 	CA	<p>Adobe has partnered with a CA empanelled as an ESP for facilitating signing solutions such as Aadhaar eSign (Aadhaar Digital ID) and another CA to enable users to sign using individually owned security tokens.</p> <p>CAs (including ESPs) issuing the digital certificates have the obligation to comply with these regulations.</p> <p>Adobe manages digital signatures generated by subscribers with public key cryptography conforming to the requirements.</p>
Information Technology (Certifying Authorities) Rules, 2000; Rule 4	<p>To sign an electronic record or any other item of information, the signer shall first apply the hash function in the signer's software; the hash function shall compute a hash result of standard length which is unique (for all practical purposes) to the electronic record; the signer's software transforming the hash result into a Digital Signature using signer's private key; the resulting Digital Signature shall be unique to both electronic record and private key used to create it; the Digital Signature and the digital signature certificate attached to its electronic record shall be stored or transmitted along with its electronic record.</p>	<p>Adobe/CA / Customer (Signer)</p> <p>Adobe manages the signer's software and Customer (i.e., signer) controls it.</p> <p>CAs/CAs empanelled as ESPs manages the signature creation data to generate the signature.</p>	<p>The hash function is implemented in Adobe software by using the SHA256 hashing algorithm according to NIST 800-57 Part 1 standard. The hash is sent to the CA/CAs empanelled as the ESP which generates the digital signature using the private key of the signer under the control of the signer.</p>
Information Technology (Certifying Authorities) Rules, 2000; Rule 5	<p>Verification of a Digital Signature shall be accomplished by computing a new hash result of the original electronic record by means of the hash function used to create a Digital Signature and by using the public key and the new hash result.</p> <p>The verifier shall check if the Digital Signature was created using the corresponding private key and if the newly computed hash result matches the original result which was transformed into Digital Signature during the signing process.</p> <p>The verification software will confirm the Digital Signature as verified if the signer's private key was used to digitally sign the electronic record, which is known to be the case if the signer's public key was used to</p>	Adobe / Customer	<p>Compliance can be achieved with a verification software such as the signature validation mechanism that is available on most popular PDF reader software. Adobe provides free access to the Acrobat Reader application which provides digital signature verification.</p> <p>Specifically, in Adobe Acrobat, users can click on the 'Signature Panel' to validate the signatures of a document.</p>

	verify the signature because the signer's public key will verify only a Digital Signature created with the signer's private key; and the electronic record was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the Digital Signature during the verification process.		
Information Technology (Certifying Authorities) Rules, 2000; Rule 5-A	<p>This rule details the verification of a Digital Signature Certificate.</p> <p>The self-signed certificate generated by the CCA, which begins the trust chain for the public key infrastructure, shall be used to verify the authenticity of the public key certificate of the licensed CAs.</p> <p>The public key certificate of the licensed CAs shall be used to verify the authenticity of the digital signature certificate issued to the subscribers.</p> <p>The certificate revocation list maintained by the licensed CAs shall be checked to confirm whether the certificate is valid or whether it has been revoked.</p> <p>While verifying the validity of a digital signature the corresponding digital signature certificates should chain up through the public key certificate of the issuing CA to the self-signed certificate of the CCA and if any of the certificates in the trust chain is not trusted the signature will not be verified.</p>	Adobe / Customer	<p>The authenticity of a Digital Signature Certificate issued to the signer is verified in the backend by the CAs by chaining up and verifying the public key certificate through the certificate of the issuing CA to the CCA's self-signed Root certificate. The Certificate Revocation list and timestamp of the digital signature are also checked.</p> <p>To enable compliance with this Rule, both Acrobat and Reader (applications integrated with Adobe Sign) have been programmed to reach out to a web page to periodically download a list of trusted "root" digital certificates of trusted CAs. When any user receives a digitally signed document from a signer whose digital certificate can trace its lineage (chain) back to a certificate on the Adobe Approved Trust List (AATL), that signature will automatically be trusted.</p>
Information Technology (Certifying Authorities) Rules, 2000; Rule 6	CAs' information technology (IT) architecture may support open standards and accepted de facto standards. Rule 6 details various important standards that may be considered for different activities associated with a CAs' functions, including public key infrastructure, digital signature certificates, digital signature and digital signature request format. Please refer to Item 1 in the Annexure to access the full text of these rules.	CA / Adobe	Adobe supports state of the implementation of public key cryptography algorithms according to IETF, ISO and ETSI standards. Adobe has also partnered with a CA empanelled as an ESP for facilitating signing solutions such as Aadhaar eSign (Aadhaar Digital ID) and another CA to enable users to sign using security tokens whose solutions are expected to be compliant with these standards.
Information Technology (Certifying Authorities) Rules, 2000; Rule 7	All Digital Signature Certificates and Certificate Revocation List issued by the CAs shall conform to Interoperability Guidelines for Digital Signature Certificates issued by CCA under the IT Act.	CA / Adobe	Please see our comment to Rule 6 immediately above.
Information Technology (Certifying Authorities) Rules, 2000; Rule 9	The infrastructure associated with all functions of generation, issue and management of Digital Signature Certificate as well as maintenance of Directories containing information about the status, and validity of Digital Signature Certificate shall be installed at any location in India.	CA	Please see our comment to Rule 6 above.
Information Technology (Certifying Authorities) Rules, 2000; Rule 19	Rule 19 outlines the security guidelines for CAs aimed at protecting the integrity, confidentiality and availability of service of CA. The CAs shall have the sole responsibility of integrity, confidentiality and protection of information and information assets employed in its operation, considering classification, declassification, labelling, storage, access and destruction of information assets according to their value, sensitivity and importance of operation. Please refer to Item 1 in the Annexure to access the full text of these rules.	CA	Please see our comment to Rule 6 above.

Information Technology (Certifying Authorities) Rules, 2000; Rule 23	Rule 23 outlines the compliance obligations in connection with issuing Digital Signature Certificates by CAs. This includes the requirement to submit a Digital Signature Certificate application by subscribers, generation of certificates upon authorized requests, specification of subscriber identity verification methods, conducting investigations in case of certificate suspension or revocation, providing opportunities for verification by subscribers, immediate notification of any factors affecting the validity of Digital Signature Certificate, and the inclusion of designated expiry dates for all Digital Signature Certificates. Please refer to Item 1 in the Annexure to access the full text of these rules.	CA	Please see our comments to Rule 3, 4, 5, 5A and 6 above.
Information Technology (Certifying Authorities) Rules, 2000; Rule 24	The generation of the Digital Signature Certificate shall involve: <ul style="list-style-type: none"> • receipt of an approved and verified Digital Signature Certificate request; • creating a new Digital Signature Certificate; • binding the key pair associated with the Digital Signature Certificate to a Digital Signature Certificate owner; • issuing the Digital Signature Certificate and the associated public key for operational use; • a distinguished name associated with the Digital Signature Certificate owner; and • a recognized and relevant policy as defined in Certification Practice Statement in accordance with the x.509 Certificate Policy for India PKI (CP) issued by the CCA. 	CA	Please see our comments to Rule 3, 4, 5 5A, and 6 above.
Information Technology (Certifying Authorities) Rules, 2000; Rule 25	Rule 25 provides requirements that a CA must adhere to before issuing a Digital Signature Certificate. Please refer to Item 1 in the Annexure to access the full text of these rules.	CA	Please see our comments to Rule 3, 4, 5 and 5A, and 6 above.
Information Technology (Certifying Authorities) Rules, 2000; Rule 26	The Digital Signature Certificate shall be issued with a designated expiration date and the Digital Signature Certificate shall expire automatically upon the expiration date, at which time it shall be archived. The period for which a Digital Signature Certificate has been issued shall not be extended, but a new Digital Signature Certificate may be issued after the expiry of such period. Please refer to Item 1 in the Annexure to access the full text of these rules.	CA	Please see our comments to Rule 3, 4, 5 and 5A, and 6 above.
Information Technology (Certifying Authorities) Rules, 2000; Rule 29	This rule details when a Digital Signature Certificate shall be revoked and become invalid for any trusted use, such as in the case where: <ul style="list-style-type: none"> • there is a compromise of the Digital Signature Certificate owner's private key; • there is a misuse of the Digital Signature Certificate; • there is a misrepresentation or errors in the Digital Signature Certificate; • the Digital Signature Certificate is no longer required. The revoked Digital Signature Certificate shall be added to the Certificate Revocation List (CRL).	CA	The certificate revocation list is maintained by the CAs/ CAs empanelled as ESPs. The entity issuing the digital certificates has the obligation to comply with these regulations.

Information Technology (Certifying Authority) Regulations, 2001			
Citation	What the Law Requires	Stakeholder responsible for compliance CA/Adobe/ESP/Customer	How Acrobat Sign Solutions Supports Customer Compliance
Information Technology (Certifying Authority) Regulations, 2001; Rule 3	Rule 3 lists the terms and conditions of the licence that permits CAs to issue Digital Signature Certificates. This includes maintaining (i) overall management obligations (e.g., ensuring security policies and safeguards are in place), (ii) certificate and key management practices (e.g., approved security controls in the certificate management processes), (iii) systems and operation controls (e.g., access and integrity controls), and (iv) other physical security, financial and compliance audit measures. Please refer to Item 2 in the Annexure to access the full text of these regulations.	CA No direct compliance obligation on Adobe.	Adobe has partnered with a CA empanelled as an ESP for facilitating signing solutions such as Aadhaar eSign (Aadhaar Digital ID) and another CA to enable users to sign using security tokens whose solutions are expected to be compliant with these standards. The CAs (including ESPs) are expected to be compliant with these regulations.
Information Technology (Certifying Authority) Regulations, 2001; Rule 4	Rule 4 lists down the standards that must be followed by the CAs for carrying out its functions in relation to Public Key Infrastructure, Public Key Cryptography, Federal Information Processing Standards, Discrete Logarithm Systems, Elliptic Curve Systems, Integer Factorization (IF) systems, Key agreement schemes, Form and size of the key pairs, Directory Services, Publication of Public Key Certificate and Public Key Certificate Standard, TBS certificate related requirements etc. Please refer to Item 2 in the Annexure to access the full text of these regulations.	CA	See our comment to Rule 3 immediately above.
Information Technology (Certifying Authority) Regulations, 2001; Rule 6	Rule 6 provides that where the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, the subscriber shall communicate the same without any delay to the CA in the format prescribed by the regulation.	Customer No direct compliance obligation on Adobe.	N/A

Information Technology (Security Procedure) Rules, 2004			
Citation	What the Law Requires	Stakeholder responsible for compliance CA/Adobe/ESP/ Customer	How Acrobat Sign Solutions Supports Customer Compliance
Information Technology (Security Procedure) Rules, 2004; Rule 4	<p>A digital signature shall be deemed to be a secure digital signature for the purposes of the Act if the following procedure has been applied to it:</p> <ul style="list-style-type: none"> • that the smart card or hardware token, as the case may be, with cryptographic module, in it, is used to create the key pair; • that the private key used to create the digital signature always remains in the smart card or hardware token as the case may be; • that the hash of the content to be signed is taken from the host system to the smart card or hardware token and the private key is used to create the digital signature and the signed hash is returned to the host system; • that the information contained in the smart card or hardware token, as the case may be, is solely under the control of the person who is purported to have created the digital signature; • that the digital signature can be verified by using the public key listed in the Digital Signature Certificate issued to that person; • that the standards referred to in Rule 7 or Rule 12 of the Digital Signature (End entity) Rules, 2015 have been complied with, in so far as they relate to the creation, storage and transmission of the digital signature; and • that the digital signature is linked to the electronic record in such a manner that if the electronic record was altered the digital signature would be invalidated. 	<p>CA</p> <p>No direct compliance obligation on Adobe.</p>	<p>Adobe has partnered with a CA empanelled as an ESP for providing signing solutions such as Aadhaar eSign (Aadhaar Digital ID) or another CA to enable users to sign using security tokens. The CAs (including ESPs) are required to be compliant with these regulations.</p> <p>Although the responsibility of creating the digital signature is managed by the CA / CA empanelled as an ESP, Acrobat Sign Solutions software provides a state of the art implementation of Public Key Cryptography which supports all the standards required by this provision.</p> <p>In addition, Customers are responsible for properly managing and deploying its smart card/token.</p>

Digital Signature (End Entity) Rules, 2015			
Citation	What the Law Requires	Stakeholder responsible for compliance CA/Adobe/ESP/ Customer	How Acrobat Sign Solutions Supports Customer Compliance
Digital Signature (End Entity) Rules, 2015; Rule 3	<p>Rule 3 provides that a digital signature shall be created and verified by cryptography which concerns with transforming electronic record into seemingly unintelligible forms; use Public Key Cryptography; and use a hash function for creating and verifying a digital signature which required to make digital signature generation and verification efficient. Please refer to Item 3 in the Annexure to access the full text of these rules.</p>	CA / Customer	<p>Adobe has partnered with a CA empanelled as an ESP for facilitating signing solutions such as Aadhaar eSign (Aadhaar Digital ID) and another CA to enable users to sign using security tokens, whose solutions are expected to be compliant with these standards. The CAs (including ESPs) are expected to be compliant with these regulations.</p>
Digital Signature (End Entity) Rules, 2015; Rule 4	<p>Rule 4 details the process that the signatory shall complete while signing an electronic record. The signatory shall first apply an hash function in the signatory's hardware or software. The hash function shall produce a hash result. The signatory's hardware or software shall then transform the hash result into a digital signature using signatory's private key and signature algorithm. The contextual information like date and time, shall be then made part of the digital signature. The counter signatures or parallel signatures or both may also be applied to electronic record.</p> <p>The signature may also include the signatory's public key signature certificate(s); the public key certificate(s) of the licensed CAs; the self signed certificate generated by the CCA used to verify the authenticity of the public key certificate of the licensed CAs; the certificate revocation list(s) maintained by the licensed CAs, and the CCA; and online certificate status protocol responder certificates and online certificate status protocol responses that may be used in lieu of certificate revocation list.</p> <p>Please refer to Item 3 in the Annexure to access the full text of these rules.</p>	CA / Adobe / Customer	<p>While the provision notes that the signatory, while signing, is required to apply hash function; this action is completed by the digital signature created using the hardware or software provided by the CAs. Further, the CAs typically ensures that the information requirements are part of the digital signature.</p> <p>The hash function is implemented in Adobe software by using the SHA256 hashing algorithm according to NIST 800-57 Part 1 standard. The hash is sent to the CAs /CAs empanelled as ESPs which generates the digital signature using the private key of the signer under the control of the signer.</p>
Digital Signature (End Entity) Rules, 2015; Rule 5	<p>Rule 5 outlines the requirements for the verification of digital signature. The verification of a digital signature shall be accomplished by computing a new hash result of the original electronic record by means of the hash function used to create a digital signature and by using the public key and the new hash result.</p> <p>The verifier shall check if the digital signature was created using the corresponding private key and shall be applicable for parallel and counter signatures applied on the electronic record, if present and the time when the digital signature was created.</p> <p>Please refer to Item 3 in the Annexure to access the full text of these rules.</p>	CA / Adobe / Customer	<p>Please note that this process need not be carried out by the customer directly but by a verification software such as the signature validation mechanism that is available on most popular PDF reader software. Adobe provides free access to the Acrobat Reader application which provides digital signature verification.</p> <p>Specifically, in Adobe Acrobat software, users can click on the 'Signature Panel' to validate the signatures of a document.</p>

Digital Signature (End Entity) Rules, 2015; Rule 6	<p>Rule 6 outlines the requirements for the verification of Digital Signature Certificate. The self signed certificate generated by the CCA shall be used to verify the authenticity of the public key certificate of the licensed CAs. The public key certificate of the licensed CAs shall be used to verify the authenticity of the digital signature certificate issued to the subscribers.</p> <p>The certificate revocation list maintained by the licensed CAs shall be checked to confirm whether the certificate of the licensed CAs is valid or whether it has been revoked.</p> <p>While verifying the validity of a digital signature the corresponding digital signature certificate shall chain up through the public key certificate of the issuing CA to the self signed certificate of the CCA and if any of the certificates in the trust chain is not trusted the signature shall not be verified.</p> <p>Please refer to Item 3 in the Annexure to access the full text of these rules.</p>	CA/ Adobe / Customer	<p>The authenticity of a Digital Signature Certificate issued to the signor is verified in the backend by the CAs by chaining up and verifying the public key certificate through the certificate of the issuing CA to the CCA's self-signed certificate. The Certificate Revocation list and timestamp of the digital signature is also checked.</p> <p>Further, both Acrobat and Reader (applications integrated with Acrobat Sign) have been programmed to reach out to a web page to periodically download a list of trusted "root" digital certificates of trusted CAs.</p>																
Digital Signature (End Entity) Rules, 2015; Rule 7	<p>The most important standards that shall be applicable for different activities associated with digital signature functions are as under—</p> <table border="1" data-bbox="526 649 1507 1323"> <thead> <tr> <th data-bbox="526 649 935 731">Products</th><th data-bbox="935 649 1507 731">Standards</th></tr> </thead> <tbody> <tr> <td data-bbox="526 731 935 812">Cryptographic hash function</td><td data-bbox="935 731 1507 812">SHA-2 as specified in FIPS 180-4</td></tr> <tr> <td data-bbox="526 812 935 894">RSA Public Key Technology</td><td data-bbox="935 812 1507 894">PKCS#1 RSA Encryption Standard ([2048, 4096 bit]); Version 1.5</td></tr> <tr> <td data-bbox="526 894 935 975">Encryption and digital signature</td><td data-bbox="935 894 1507 975">PKCS#7, CMS</td></tr> <tr> <td data-bbox="526 975 935 1057">Validation of Digital Signature Certificate</td><td data-bbox="935 975 1507 1057">RFC 5280</td></tr> <tr> <td data-bbox="526 1057 935 1139">ECC curve</td><td data-bbox="935 1057 1507 1139">NIST P-256, P-384, or P-521</td></tr> <tr> <td data-bbox="526 1139 935 1220">Long term signature formats</td><td data-bbox="935 1139 1507 1220">1. CAdES RFC 5126, 2. PAdES with CAdES</td></tr> <tr> <td data-bbox="526 1220 935 1323">Time stamp token</td><td data-bbox="935 1220 1507 1323">As specified RFC 3161</td></tr> </tbody> </table>	Products	Standards	Cryptographic hash function	SHA-2 as specified in FIPS 180-4	RSA Public Key Technology	PKCS#1 RSA Encryption Standard ([2048, 4096 bit]); Version 1.5	Encryption and digital signature	PKCS#7, CMS	Validation of Digital Signature Certificate	RFC 5280	ECC curve	NIST P-256, P-384, or P-521	Long term signature formats	1. CAdES RFC 5126, 2. PAdES with CAdES	Time stamp token	As specified RFC 3161	CA / Adobe / Customer	<p>Please see response against Rule 3 and 4 above.</p> <p>Although the responsibility of creating the digital certificate is managed by the CAs (including ESPs), Adobe Acrobat Sign provides an industry implementation of public key cryptography which supports all the standards required by this provision.</p>
Products	Standards																		
Cryptographic hash function	SHA-2 as specified in FIPS 180-4																		
RSA Public Key Technology	PKCS#1 RSA Encryption Standard ([2048, 4096 bit]); Version 1.5																		
Encryption and digital signature	PKCS#7, CMS																		
Validation of Digital Signature Certificate	RFC 5280																		
ECC curve	NIST P-256, P-384, or P-521																		
Long term signature formats	1. CAdES RFC 5126, 2. PAdES with CAdES																		
Time stamp token	As specified RFC 3161																		

Digital Signature (End Entity) Rules, 2015; Rule 8- Rule 12	<p>Rules 8-12 discuss requirements for xml digital signatures.</p> <p>Please refer to Item 3 in the Annexure to access the full text of these rules.</p>	N/A	XML signature is not supported in Adobe Acrobat Sign software.
Digital Signature (End Entity) Rules, 2015; Rule 13	<p>The manner of digital signature creation and verification, in respect of signature profile and signature format, shall also conform to the following guidelines issued by CCA, including:</p> <ul style="list-style-type: none"> • Interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act; • X.509 Certificate Policy for India PKI; • Signature profiles; • Online Certificate Status Protocol (OCSP) Service Guidelines for CAs; • Time Stamping Services Guidelines for CAs. 	CA / Adobe / Customer	Although the responsibility of creating the digital certificate is managed by CAs (including ESPs), Adobe Acrobat Sign provides an industry standard implementation of public key cryptography which supports all the standards required by this provision.

Annexure

Reference No.	Name of the Statute	Embedded PDF of the Statute
1.	Information Technology (Certifying Authorities) Rules, 2000	 The Information Technology (Certifyi
2.	Information Technology (Certifying Authority) Regulations, 2001	 The Information Technology (Certifyi
3.	Digital Signature (End Entity) Rules, 2015	 The Information Technology (Securi

4. Additional Resources

For more information, please also see these helpful resources:

- Information on Electronic Signature Laws & Regulations in India provided by Adobe is available here: <https://helpx.adobe.com/legal/esignatures/regulations/india.html>.
- Electronic Signatures in India Whitepaper by Adobe & Trilegal available here: <https://www.adobe.com/content/dam/dx-dc/pdf/uk/electronic-signatures-in-india-uk.pdf>.

5. Contact Info

To learn more about how Acrobat Sign Solutions can benefit your organization, contact your Adobe sales representative today at 1-800-87ADOBESTRONG>

6. Disclaimer

This document is intended to help businesses analyze their responsibilities and compliance related to the India IT Act and its related rules/regulations. Adobe does not provide legal advice on any specific use cases, and this analysis is not meant to provide any specific legal guidance. To apply this analysis to any specific use case needs, please consult an attorney. To the maximum extent permitted by law, Adobe provides this material on an "as is" basis. Adobe disclaims and makes no representation or warranty of any kind with respect to this material, express, implied or statutory, including representations, guarantees or warranties of merchantability, fitness for a particular purpose, or accuracy.

7. Glossary

Aadhaar number is a 12-digit random number issued by the Unique Identification Authority of India (UIDAI) to residents of India based on their biometrics and demographic data.

Asymmetric crypto system means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

Certifying Authority or CA means a person who has been granted a licence to issue an electronic signature Certificate under section 24 of the IT Act.

Controller or CCA means the Controller of Certifying Authorities.

Data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the IT Act.

Digital signature certificate means a digital signature certificate issued under section 35(4) of the IT Act.

Electronic signature means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature.

Electronic signature certificate means an Electronic Signature Certificate issued under Section 35 of the IT Act and includes Digital Signature Certificate.

Electronic record means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

End entity means the subscriber or system on behalf of the subscriber in whose name the Electronic Signature Certificate is issued.

eSign Service Providers or ESPs are trusted third parties that provide eSign service and are licensed CAs.

Hash function means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible: (a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm; and (b) that two electronic records can produce the same hash result using the algorithm.

Key pair, in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

Private key means the key of a key pair used to create a digital signature.

Public key means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.

Public key cryptography employs an algorithm using two different but mathematical related "keys": a private key – one for creating a Digital Signature or transforming data into a seemingly unintelligible form, and another key, a public key, for verifying a Digital Signature or returning the electronic record to original form.

Signature creation data, in the case of a digital signature, means the private key of subscriber.

Subscriber means a person in whose name the electronic signature certificate is issued.