

DIGITAL SIGNATURE (END ENTITY) RULES, 2015

AMO-33004/99 REGD. NO. D, L..33004/99 Che Gazette of Sftidia 5301 No. 5301 EXTRAORDINARY PART I I—Section J—Sub-section (i) PUBLISHED BY AUTHORITY 26, 2015/q--TT% 4, 1937 NEW DELHI, WEDNESDAY, AUGUST 26, 2015/BHADRA 4, 1937 25 3FT€T, 2015 qr.q;rfi. 2000 (2000 21) 87 t, 3T2Tfr(1. (1) rage, ZUID I F) 2000 (2000 3Tfü-iF 31fiFhT q-q-ft 3643 2 (v) g) (8) (K) THE OAZETTB OF INDIA EXTRAORDINARY ftN't; f@fâ t; t stre (q) (R) (q) (11) (III) t fig æt«3T, 4 THE GAZETrE OF INDIA : EXTRAORDINARY [PART 11—SEC. 3TQiGFIT (ii) fÄfâf& FZT\$T *fiz (zrq) 3. tifä.—ßæfr (q) ft-Rr i--fi ÄRfi ; (für t) 3ifizr *Ter m-zr q-t7Tq-?r FT) 3âr 3i*rzr 3ifizr 1 (6) æn;\$r,— 3(i)J 5 (V) (fiqi) 38 (g.) FTTVT FTTVr e-ræ-r q-Frr (T) ég étT \$Sr zrr (V) éq it tr zrr 5.) 3ifiq 3ifizr OT æi7TOFTr *-crr— ß) Tr srrfiz qT (2) fig (2) 3i*rq (3) trt ft q-r t 38 THE GAZETTE OF INDIA EXTRAORDINARY ART 11=SXC, 3 1 1 eo.4 t (2048, 4096 5280 Vtt*521 1. CADES 5126, 2. PAdES with CADES 3161 t (2) nq•r— 7 q" trtT't ; 'fitrr (11) sfttrr*t t ; g IMI ; (q) (qfû d) 64 Åfr i (g) &fM, 509 609 609 8 (4) (5) (6) (7) THE GAZETTE OF INDIA : EXTRAORDINARY (T) «fr q-ra-r (71) 509 \$Sr, ft-q•r t, [PART 11—SEC. 3(i)] (iii) I qarrtFT 3tR mfr 3(i)] 11 , btfrzr 3275 509 t 3980 3629 4648 180-4 1.5 258 O 14 3741 1, 1.0 <http://www.w3.org/TR/2001/REC.xml.c14n.20010315> 2, 1.1 t) <http://www.w3.org/2000/12/xml-c14n11> 3741 <http://www.w3.org/TR/2001/REC-xml-c14n.20010315> 2, 1.1 9 10 THE GAZETTE OF INDIA : EXTRAORDINARY <http://www.w3.org/2006/12/xml-c14n11> [PART 11—SEC. 3(i)] 1.0. <http://www.w3.org/TR/1999/REC-xslt-19991116> XPath - RFC 3653 zrr TFT.509 3i-âTph-rtr ft-a-tit 1.5 #256, #384, qT #521 1. 6283 XAdES 2. 6283 PAdES XAdES 3161 12. <Signature <Signed Inf0> <canonicalization Method/> <Signature Method/> (<Reference <Digest Value> </Reference>+ </Signed Inf0> <Signature Value> (<KeyInf0> (Key Name) (Key Value) (Retrieval Method) Data> (X509 SKI) 11 (X509 Subject Name) 0<509 Certificate) (X509 CRL) 0<509 Digest) </x509 Data>) (<Object </Signature> qT ; "+" : 3â7 13. 3ifizr z:1FT4i.— (ii) ; (iii) (iv) (trg) (Hrgqfi) MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (Department of Electronics and Information Technology) NOTIFICATION New Delhi, the 25th August, 2015 G.S.R. exercise of the powers conferred by section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:— 1. Short title and commencement.— (1) These rules may be called the Digital Signature (End entity) Rules, 2015. (2) They shall come into force on the date of their publication in the Official Gazette. these rules, unless the context otherwise requires,— (b) "canonicalisation", in relation to a xml digital signature, means the process of converting electronic record that has more than one possible representation into a 'standard', 'normal', or 'canonical form' in which the variations 12 (c) (d) (e) (f) (g) (h) (j) (k) (m) (n) (p) (q) (r) (B) (u) (v) THE GAZETTE OF INDIA : EXTRAORDINARY [PART 11—SEC. 3(i) in representation of electronic record shall be standardised by applying consistent rules, primarily as part Of the xml digital signature creation and verification processes; "counter signature" means a signature on a previous signature in a series Of signatures, affixed after the verification the signature on electronic record und subsequent signatures on previous signatures serially; "detached signature" means the signature that is stored independent of electronic record being signed; "digestmethod element", in relation to a xml digital signature, means the digest algorithm to be used for the original data object or transformed, If any 'xml transforms' exists; "digestvalue element" means the value ofthe digest; "end entity'S means the subscriber or system on behalf of the subscriber in whose name the Electronic Signature Certificate is issued; "end entity signature" means authentication of any electronic record by an end entity by means of a digital signature, electronic method or procedure in accordance With the movisions of gectiane of the "enveloped signature" means enveloping of the signature and the initial electronic record into another electronic record; "enveloping signature" means a signature over a electronic record that is referenced and contained within the signature element; "initial electronic record", in the context of xml digital signature process, means canonicalised and transformed form of signedInfo; "keyinfo element" means an element that enables key information to be packaged ntong with the signature element; "long term signature" means a signature element that is made verifiable tor u long term by implementing measures to enable the detection of unauthorised alterations of signature; "manifest element", in relation to n xml digital signature, means a structurc to carry a list of reference elements processing model defined by the application; "object element" means an

optional element of xml digital signature, Which is used for envelope digital signature what the data object being signed included in "ocsp responder" means an online service that provides revocation status of a digital signature certificate; "online certificate status protocol" means an online certificate-revocation checking protocol that enables relying parties to determine the revocation status of an identified digital signature certificate; "parallel signatures" means one or more independent signature over the same electronic record in which the ordering of the signatures is not important; "reference element", in relation to a xml digital signature, means an element that carries a reference to data objects, an optional list of transforms to be applied prior to digest (xml transforms), digestmethod and digestvalue value of referenced data objects; "signedInfo", in relation to a xml digital signature, means an element that contains a set of information to be signed for creating an xml signature, where it shall contain references to the data object that includes the canonicalisation and signature algorithms; "signature" means digital signature or xml digital signature; An element that the actual value of the digital signature "signaturemethod" means an element that contains the algorithm used for signature generation and this algorithm identifies all cryptographic functions involved in the signature generation; (x) (y) (z) (zc) (zd) (ze) (zh) 13 "signatureproperties" means an element that provides a way to carry additional information about the signature, such as a time stamp or any other information which are defined by application; "time stamp" means a notation that indicates the correct date and time of an action and identity of the person or device that sent or received the time stamp and is enforced using time stamp token; "time stamp token" means a cryptographically secure confirmation generated by applying digital signature of a time stamping service provider that includes the time when the confirmation was generated; "time stamping service provider" means a trusted entity authorised to generate time stamps; "xml" means Extensible Markup Language that provides a standard methodology with formal syntax to identify elements of information, describe the structure of data and also to store data in an independent manner, shall have the following properties,— (i) with xml, content and presentation are separate; (ii) the structure of xml data in a particular context is described using either xml schema or a document type definition; (iii) xml schema or a document type definition are stored separately from the xml document itself and can be used as a "xml digital signature element" means an element that defined by standard xml schema for capturing the result of a digital signature operation applied to arbitrary data in xml format, shall satisfy the following.— (i) xml digital signature element shall exist as a standalone document or envelop the data object that it signs; (ii) xml digital signature element shall have signedInfo, signaturevalue, keyInfo, object and has id attribute of type child elements in order in which they appear; "xml digital signature" means the digital signature on xml electronic record; "xml document" means a document with xml logical and physical structure that is used to carry data elements, composed of declarations, elements, comments, character references, and processing instructions and a physical structure composed of entities, starting with the root, or document entity; "xml schema" means a set of pre-defined or user defined keywords and their attributes arranged in a structured manner, shall satisfy the following,— (i) should be used for a particular purpose whereas a schema describes the structure of an xml document and provides specification of element names that indicates which elements are allowed in an xml document, and in what combinations; and (ii) should provide extended functionality such as data types, inheritance, and presentation rules and default values for attributes; "xml transform" means an element that specifies an optional ordered list of processing steps applied to the data objects before it was digested where the transforms include canonicalization, encoding or decoding, extensible style sheet language transformations, xpath filtering, and xml schema validation; "xml namespace" means a uniform resource identifier (uri) reference where the mechanisms described in the specification are used in xml documents as element types and attribute names and also to use various xml vocabularies without having name collision. (2) Words and expressions used herein and not defined but defined in the Act shall have the meanings respectively assigned to them in the said Act

3. Manner of authentication of Information by means of digital signature.—A digital signature shall,— (a) be created and verified by cryptography which concerns with transforming electronic record into seemingly unintelligible forms; (b) use Public Key Cryptography, which employs an algorithm using two different but mathematically related keys; one key (called the private key) for creating a digital signature and another key (called the public key) for verifying a digital signature; (c) use a hash function for creating and verifying a digital signature which required to make digital signature generation and verification efficient

4. Creation of digital signature. The signatory shall, while signing an electronic record or any other item of information, first apply an hash function in the manner specified in the GAZETTE OF INDIA : EXTRAORDINARY (2) The hash function shall produce a hash result. (3) The signatory's hardware or software shall then transform the hash result into a digital signature using signatory's private key and signature algorithm. (4) The contextual information like date and time, shall be then made part of the digital signature. (5) The counter signatures or parallel signatures or both may also be applied to electronic record. (6) The following information may also be a part of signature, (a) (b) (c) (d) (e) the signatory's public key signature certificate(s); the public key certificate(s) of the licensed Certifying Authorities which used to verify the authenticity of the digital signature certificate issued to the signatory; the self signed certificate generated by the Controller used to verify the authenticity of the public key certificate of the licensed Certifying Authorities; the certificate revocation list(s) maintained by the licensed Certifying Authorities, and the controller which is used to check whether the digital signature certificate has been revoked under section 38 the Act; online certificate status protocol responder certificates and online certificate status protocol responses that may be used for certificate revocation (7) To create long term valid digital signature,— (a) a timestamp shall be applied initially to the signed data including the certificates and revocation information; (b) ensure that initial time stamp shall cover all the data and signature(s); (c) a nested time stamp option shall be used to ensure signature validity past the time stamping service provider's (tss) key or algorithm expiry where the nesting of time stamps implies that a subsequent time stamp shall be applied to the prior time stamp; (d) signature(s) and time stamps may be embedded in the data itself or stored separately as standalone

5. 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, the verifier shall check—(a) 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; (b) the time when the digital signature was created. (2) To verify counter signature, the signature on electronic record and thereafter signature on previous signature serially shall be verified. (3) To verify parallel signature, signature on electronic record shall be verified independently. (4) To verify long term signature, the initial timestamp and all subsequent time stamp applied on the each prior timestamp shall be verified

6. Verification of Digital Signature Certificate.—(1) The self signed certificate generated by the Controller, 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 Certifying Authorities. (2) The public key certificate of the licensed Certifying Authorities shall be used to verify the authenticity of the digital signature certificate issued to the subscribers. (3) The certificate revocation list maintained by the licensed Certifying Authorities shall be checked to confirm whether the certificate of the licensed Certifying Authorities is valid or whether it has been revoked under section 38 the Act. (4) While verifying the validity of a digital signature the corresponding digital signature certificate shall chain up through the public key certificate of the issuing Certifying Authority to the self signed certificate of the Controller and if any of the certificates in the trust chain is not trusted the signature shall not be verified. (5) The Digital Signature Certificate shall be verified with respect to time of signature created. (6) The chain of certificates shall be verified in accordance with the standards specified in rule 7. (7) If the certificate validity is less than one hour, the checking of revocation list shall not be required. 3(i) 15, 7. Digital signature standards.—The most important standards that shall be applicable for different activities associated with digital signature functions are as under— Products Cryptographic hash function RSA Public Key Technology Encryption and digital signature Validation of Digital Signature Certificate ECC curve Long term signature formats Time stamp token Standards SHA-2 as specified in FIPS 180-4 PKCS#1 RSA Encryption Standard (12048, 4096 bit); Version 1.5 PKCS#7, CMS RFC 5280 NIST P-256, P-384, or P-521 1. CAdES RFC 5126, 2. PAdES with CAdES As per part 1 8. Manner of authentication of information by means of xml digital signature.— A xml digital signature shall,— (a) (b) (c) (d) (e) be created and verified by cryptography which concerns with transforming electronic record into seemingly unintelligible forms; use Public Key Cryptography, which employs an algorithm using two different but mathematical related keys, one key (called the private key) for creating a xml digital signature and another key (called the public key) for verifying a xml digital signature; use an cryptographic hash function for creating and

verifying a xml digital signature; use canonicalization and xml transformation to create standard electronic record prior to creation and verification of xml digital signature; authenticate xml documents which contain data as references and corresponding hashes, which is affected by the use of hash algorithm canonicalization, xml transformation and public key algorithm

9. Creation of xml digital To sign an electronic record or any other item of information, the signatory shall first constructs reference elements, xml digital signature element, signedinfo, keyinfo and signaturevalue.(2) For the purpose of reference element generation, the signing software shall— (b) (c) (d) create referenc(s) OF vml transform element(s) (optional), digest algorithms and digest value; optionally apply xml transform(s) to each referenced object in a sequential order; apply the hash function in the signatory's hardware or software to each reference elements, store the hash result in the reference element; ensure that if the object element is created, it shall not have a manifest element; ensure that exclusive canonicalization "without comments" has been mandatorily specified in addition to any other transforms. (3) For the purpose xml digital signature generation, the signing software shall— (a) (b) (c) create signedinfo element with signaturemethod, canonicalisation method and reference(s); apply canonicalisation to signedinfo and calculate the hash value of canonicalised signedinfo using the hashing algorithms implied by the signaturemethod; ensure that,— (111) the signatory has seen all the contents of the document before signing; the contents display requirements, in the case of automated signing process, is not required; to stgn mull1p1v (a) each resource shall be rendered on the screen; 16 (c) (d) (e) THE GAZEITE OF INDIA : EXTRAORDINARY ART II—SEC. 3 i) each referenced xml resource shall be rendered using xalt and the xstt shall be the last transform done to render the resource on the screen; each non xml resource shall be rendered using mime type attribute mentioned in the object; generate the signature using the s1Unature algorithm and the hash, the signatory's private key, and the public key parameters (if applicable) and perform base64 encoding of the signature result and use It to form signaturevalue*, construct the slgnature element that Includes slgnedlnfo, Items of information, keylnfo with *509 certificate element and signaturevalue and the xS09 certificate element shall carry the signatory's *509 public key certificate. (4) The contextual information like date and time, Shall be then made part of the xml digitat signature. (5) The counter signatures or parallel signatures or both may also bg applied to electronic record. (6) The following Informmtn may also be a pan of signature— (a) the public key certflcate(s) ofthe, llcensed CertlWIng Authorltlea which used to verlB' the authenticity of the dlglal signature cetilflcute Issued to tho signatory; 'lynvu generatea by the Controller used to verify tho authenticity of the public key certflgate ofthe llcensed CertlWIng Authorltles; (c) the certificate revocation list(s) mulntalned by the llcensed CertlWIng Authorltley and controller which Is used check whether the digital signature certificate has been revoked under section 38 the Act; (d) online egrtlfleatg status protocol responder certificates and online ceniflcate status protocol responses may be used In lleu of certflcate revocation list, (7) To create long term valid xml digital signature— (a) a timestamp shall be applied Initially to the signed document, where the Initial tlme stamp shall cover all the electronic record and slgnature(s); (b) a nested time stamp option shall be used to ensure signature valldfty past the tlme•stampng serylce provider (tssp)s key or algorithm expiry where as nesting of time stamps implies that q subsequent time stomp shall be applied to the prior time stamp; (c) signature(s) and time stamps may be embedded in the data Itselfor stored separately ag standalone. IO. Verification of xml digital Tho verflfcatlon of the xml digital signature shall be accomplished by signature validation, reference validation and certificate validation and an xml digital signature shall be treated valid only if signature validation, refrence validation and cottltlcate validatton as specified below are gomppld wlth. (2) To accompli*h signature validation— (o) canonical form ofslgnedinfo produced during retirence validation shall be used; (b) canonical form of signaturomethod using the canonlealintlon method shall be obtained; (e) the public key contained in the signatory's x509 certflcate that Is Included in the xml digital signature, the canonlcalsled form of slgnedlnfo glgnnttureevolue. and canonlcali9led form of signntturemethod shall be used to verity the signature, (3) To accomplish reference valldatlon— (a) ganonlcalsle the slgnedlnfo element bowd on the canonlcalselton method In the 81gnedinfo shall be uged; (b) for each reference in the 81gnedlnfo— (I) If tran8formatlons were applied by the signatory, thon the verifler software may de•rference the uniform resource identflfor (url) and execute transforms provided by the signatory In the Nference element; (11) compute digen ofreferenced item using the digostmethod speciflgl In ita reference element; (III) compare the computed digest value against digestvatue In the 81gnedlnfo reference; It there

18 any mismatch or validation fails; (4) The Digital Signature Certificate Included In the xml digital signature shall be verified in accordance with the (S) To verify counter signature, the signature on electronic record first and signature on prgvlog signature shall be verified serially, [9TFT 3(i)] qr«r : (6) To verify parallel signature, signature on electronic record shall be verified independently. (7) TO verify long term signature, the initial timestamp and all subsequent time stamp applied on the each prior timestamp shall be verified. 11. The xml digital signature standards.—The most important standards that shall be applicable for different activities associated with xml digital signature functions are as under— the Product XML Digital Signature Standard XML Namespace Signature encoding Signature Value Encoding Reference element Digest Signature Algorithm Signature block Canonicalization Transform Algorithms Signature Type Digital Signature Certificate Standard RFC 3275 with the following constraint Manifest is not permitted inside Object, KeyInfo containing X509Certificate element is mandatory. The Reference Processing shall use the Exclusi Canonicalization(without comments) in addition to other transforms. For XML resource. XSLT shall be the last transform done to enable the rendering of the document on screen. For rendering of document on the screen Each referenced XML resource shall be implemented using XSLT. Each non XML resource shall be implemented using Mime attribute mentioned in the object. FC 3986 TF-8 RFC3629 asc64 RFC 4648 Étpsno-4 HA256withRSA PKCS-I Version 1.5 Exclusive (without comments), XML-EXC-C 14N, RFC 3741 Canonical XML 1. Canonical XML 1.0 (omits comments) ol,ln 200102 i g 2. Canonical XML 1.1 (omits comments) <http://www.w3.org/2006/12/xml-c> 14n I I Exclusive (without comments), XML-EXC-C14N, RFC 3741 Canonical XML • I. Canonical XML 1.0 (omits comments) 2. Canonical XML 1. I (omits comments) [http://www.w3.org.Q006/12/xml-c](http://www.w3.org/Q006/12/xml-c) 14n I I XSLBXML Transforms (XSLT) Version 1.0. W3C [http://www.w3.org,TW1999/REC-xslt-19991116](http://www.w3.org/TW1999/REC-xslt-19991116) XPath - RFC 3653 enveloped or enveloping or detached (DER) X.-SC9 VJ issued as per interoperability guidelines 18 Public Key Algorithms ECC curve Long Term Signature formats Time Stamp Token THE GAZEITE OF INDIA : EXTRAORDINARY RSA PKCS-I Version 1.5 NIST P-256, p-384, or P-521 1. XMLERS RFC 6283 and XAdES 2. XMLERS RFC 6283 and PAdES with XAdES As specified RFC 3161 in XML notation [PART 12. The basic Syntax of xml digital signature and terms used in the rule shall be as follows, namely:- <Signature <SignedInfo> <CanonicalizationMethod/> (<Reference <DigestMethod> <DigestValue> </Reference>+ (<KeyInfo> (KeyName) (KeyVaJue) (RetrievalMethod) (X509SK1) (X509SubjectName) (X509Certificate) (X509CRL) (XS09Digest) (<Object Where denotes zero or one occurrence; occurrences. 9+" denotes one or more occurrences; and "*" denotes zero or more 19 13. Digital Signature functions Standard.— 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 Controller, namely:- (ii) (iii) (iv) (v) 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 Certifying Authorities (CA); Time Stamping Services Guidelines for CertiWing Authorities (CA). [F. No. 19/26/20157CCA] TAPAN RAY, Addl. secy. 25 2015 qrxrfi. 661(«).— 2000 (2000 21) grr 16 87 (2) (3) 2004 3âx t, 1.(1) FT fiNT) 2015 I 2. *firtr (qxq-r 2004 qq, 3TfÄfiq-q 3ifrq (3im:r fr\$Tzr) 2015 g, OTT 3TfÄfrzgr "F) 3i*rzr fizrq, 2015 7 12 term. 40/26/204 6 e-cqur : fi-q-q 11, 3, (i) €. qTÄTfi. 735(3T), 29 2014 I NOTIFICATION New Delhi, the 25th August, 2015 G.S.R. exercise of the powers conferred by clause (e) Of sub-section (2) of Section 87 read with Section 16 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules to amend the Information Technology (Security Procedure) Rules, 2004. I. (I) These rules may be called the Information Technology (Security Procedure) Amendment Rules, 2015. (2) They shall come into force on the date Oftheir publication in the Official Gazette

2. In the Intbrmation Technology (Security Procedure) Rules, 2004,—(a) in rule 2, for clause (e), the following clause shall be substituted, namely:— "(e) words and expressions used in these rules and not defined but defined in the Act and the Digital Signature (Ena entity) Rules, 2015 shall have the same meaning respectively assigned for them in the said Act and rules,";