(X509 Subject Name)

(X509 Certificate)

(X509 CRL)

(X509 Digest)

</x509 Data>)

</Keyinfo>)

(<Object ID?>)*

</Signature>

जहां "?" शून्य या एक बार उपदर्शित होने को दर्शाता है ; "+" एक या अधिक बार उपदर्शित होने को दर्शाता है ; और "*" शून्य या अधिक बार उपदर्शित होने को दर्शाता है ।

**13. अंकीय हस्ताक्षर कृत्य मानक**.— हस्ताक्षर प्रोफाइल और हस्ताक्षर प्ररूप की बाबत अंकीय हस्ताक्षर सृजन और सत्यापन की रीति नियंत्रक द्वारा जारी निम्नलिखित मार्गदर्शक सिद्धांतों के भी अनुरूप होगी, अर्थात् :-

(i) अंकीय हस्ताक्षर प्रमाणपत्र के लिए सूचना प्रौद्योगिकी अधिनियम के अधीन जारी अंर्तकार्यकारी मार्गदर्शक सिद्धांत ;

(ii) भारत पीकेआई के लिए एक्स.509 प्रमाणपत्र नीति ;

(iii) हस्ताक्षर प्रोफाइल ;

(iv) प्रमाणीकरण प्राधिकारियों (सीए) के लिए ऑनलाइन प्रमाणपत्र प्रास्थिति प्रोटोकाल (ओसीएसपी) सेवा मार्गदर्शक सिद्धांत ;

(v) प्रमाणपत्र प्राधिकारियों (सीए) के लिए समय स्टॉप सेवा मार्गदर्शक सिद्धांत ।

[फा. सं. 19/26/2015-सीसीए]

तपन राय, अपर सचिव

**MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY**

**(Department of Electronics and Information Technology)**

**NOTIFICATION**

New Delhi, the 25th August, 2015

**G.S.R. 660(E).—**In 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.

**Definitions-—**(1)In these rules, unless the context otherwise requires,—

(a) "Act" means the Information Technology Act, 2000(21 of 2000);

(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

in representation of electronic record shall be standardised by applying consistent rules, primarily as part of the xml digital signature creation and verification processes;

(c) "counter signature" means a signature on a previous signature in a series of signatures, affixed after the verification the signature on electronic record and subsequent signatures on previous signatures serially;

(d) "detached signature" means the signature that is stored independent of electronic record being signed;

(e) "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;

(f) "digestvalue element" means the value of the digest;

(g) "end entity" means the subscriber or system on behalf of the subscriber in whose name the Electronic Signature Certificate is issued;

(h) "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 provisions of sections 3 or 3A of the Act;

(i) "enveloped signature" means enveloping of the signature and the initial electronic record into another electronic record;

(j) "enveloping signature" means a signature over a electronic record that is referenced and contained within the signature element;

(k) "initial electronic record", in the context of xml digital signature process, means canonicalised and transformed form of signedInfo;

(l) "keyinfo element" means an element that enables key information to be packaged along with the signature element;

(m) "long term signature" means a signature element that is made verifiable for a long term by implementing measures to enable the detection of unauthorised alterations of signature;

(n) "manifest element", in relation to a xml digital signature, means a structure to carry a list of reference elements processing model defined by the application;

(o) "object element" means an optional element of xml digital signature, which is used for enveloping signature where the data object being signed is included in the xml;

(p) "ocsp responder" means an online service that provides revocation status of a digital signature certificate;

(q) "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;

(r) "parallel signatures" means one or more independent signature over the same electronic record in which the ordering of the signatures is not important;

(s) "reference element", in relation to a xml digital signature, means an element that carries a references to data objects, an optional list of transforms to be applied prior to digest (xml transforms), digestmethod and digestvalue value of referenced data objects;

(t) "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 contains references to the data object that includes the canonicalisation and signature algorithms;

(u) "signature" means digital signature or xml digital signature;

(v) "signaturevalue" means an element that the actual value of the digital signature;

(w) "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) "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;

(y) "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;

(z) "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;

(za) "time stamping service provider " means a trusted entity authorised to generate time stamps;

(zb) "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 to validate a given xml document for conformance;

(zc) "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;

(zd) **"**xml digital signature" means the digital signature on xml electronic record;

(ze) "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;

(zf) "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 where as 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;

(zg) "xml transform" means an element that specify 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;

(zh) "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 mathematical 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 an hash function for creating and verifying a digital signature which required to make digital signature generation and verification efficient.

4. **Creation of digital signature.—**(1) The signatory shall, while signing an electronic record or any other item of information, first apply an hash function in the signatory's hardware or software.

(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) the signatory's public key signature certificate(s);

(b) 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;

(c) the self signed certificate generated by the Controller used to verify the authenticity of the public key certificate of the licensed Certifying Authorities;

(d) 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;

(e) online certificate status protocol responder certificates and online certificate status protocol responses that may be used in lieu of certificate revocation list.

(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 (tssp) 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.—**(1)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.

**7. Digital signature standards.—**The most important standards that shall be applicable for different activities associated with digital signature functions are as under—

| 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,<br>2. PAdES with CAdES |
| Time stamp token | As specified RFC 3161 |

8. **Manner of authentication of information by means of xml digital signature.—** A xml 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 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;

(c) use an cryptographic hash function for creating and verifying a xml digital signature;

(d) use canonicalization and xml transformation to create standard electronic record prior to creation and verification of xml digital signature;

(e) 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 signature**.—(1) 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—

(a) create reference(s) element(s) with reference to the item of information, xml transform element(s) (optional), digest algorithms and digest value;

(b) optionally apply xml transform(s) to each referenced object in a sequential order;

(c) apply the hash function in the signatory's hardware or software to each reference elements, store the hash result in the reference element;

(d) ensure that if the object element is created, it shall not have a manifest element;

(e) 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) create signedinfo element with signaturemethod, canonicalisation method and reference(s);

(b) apply canonicalisation to signedinfo and calculate the hash value of canonicalised signedinfo using the hashing algorithms implied by the signaturemethod;

(c) ensure that,—

(i) the signatory has seen all the contents of the document before signing;

(ii) the contents display requirements, in the case of automated signing process, is not required;

(iii) to sign multiple resources together,—

(a) each resource shall be rendered on the screen;

(b) each referenced xml resource shall be rendered using xslt and the xslt shall be the last transform done to render the resource on the screen;

(c) each non xml resource shall be rendered using mimetype attribute mentioned in the object;

(d) generate the signature using the signature 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;

(e) construct the signature element that includes signedinfo, items of information, keyinfo with ×509 certificate element and signaturevalue and the x509 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 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) 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;

(b) the self signed certificate generated by the Controller used to verify the authenticity of the public key certificate of the licensed Certifying Authorities;

(c) the certificate revocation list(s) maintained by the licensed Certifying Authorities and controller which is used check whether the digital signature certificate has been revoked under section 38 the Act;

(d) online certificate status protocol responder certificates and online certificate status protocol responses may be used in lieu of certificate 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 time stamp shall cover all the electronic record and signature(s);

(b) a nested time stamp option shall be used to ensure signature validity past the time-stamping service provider (tssp)'s key or algorithm expiry where as nesting of time stamps implies that a subsequent time stamp shall be applied to the prior time stamp;

(c) signature(s) and time stamps may be embedded in the data itself or stored separately as standalone.

**10. Verification of xml digital signature**.—(1) The verification 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, reference validation and certificate validation as specified below are complied with.

(2) To accomplish signature validation—

(a) canonical form of signedinfo as produced during reference validation shall be used;

(b) canonical form of signaturemethod using the canonicalization method shall be obtained;

(c) the public key contained in the signatory's x509 certificate that is included in the xml digital signature, the canonicalisied form of signedinfo signaturevalue, and canonicalisied form of signaturemethod shall be used to verify the signature.

(3) To accomplish reference validation—

(a) canonicalise the signedinfo element based on the canonicalisation method in the signedinfo shall be used;

(b) for each reference in the signedinfo—

(i) if transformations were applied by the signatory, then the verifier software may de-reference the uniform resource identifier (uri) and execute transforms provided by the signatory in the reference element;

(ii) compute digest of referenced item using the digestmethod specified in its reference element;

(iii) compare the computed digest value against digestvalue in the signedinfo reference; if there is any mismatch or validation fails;

(4) The Digital Signature Certificate included in the xml digital signature shall be verified in accordance with the provisions specified in rule 6.

(5) To verify counter signature, the signature on electronic record first and signature on previous signature shall be verified serially.

(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 | Standard |
|---|---|
| XML Digital Signature Standard | RFC 3275 with the following constraint<br>o Manifest is not permitted inside Object,<br>o KeyInfo containing X509Certificate element is mandatory.<br>o The Reference Processing shall use the Exclusive Canonicalization(without comments) in addition to other transforms.<br>o For XML resource, XSLT shall be the last transform done to enable the rendering of the document on screen.<br>o For rendering of document on the screen<br>o Each referenced XML resource shall be implemented using XSLT.<br>o Each non XML resource shall be implemented using Mime Type attribute mentioned in the object. |
| XML Namespace | RFC 3986 |
| Signature encoding | UTF-8 RFC 3629 |
| Signature Value Encoding | Base64 RFC 4648 |
| Reference element Digest | SHA256 FIPS 180-4 |
| Signature Algorithm | SHA256withRSA PKCS-1 Version 1.5 |
| Signature block Canonicalization | o Exclusive (without comments), XML-EXC-C14N, RFC 3741<br>o Canonical XML<br>1. Canonical XML 1.0 (omits comments)<br>http://www.w3.org/TR/2001/REC-xml-c14n-20010315<br>2. Canonical XML 1.1 (omits comments)<br>http://www.w3.org/2006/12/xml-c14n11 |
| Transform Algorithms | Exclusive (without comments), XML-EXC-C14N, RFC 3741<br>Canonical XML<br>1. Canonical XML 1.0 (omits comments)<br>http://www.w3.org/TR/2001/REC-xml-c14n-20010315<br>2. Canonical XML 1.1 (omits comments)<br>http://www.w3.org/2006/12/xml-c14n11<br>XSLT-XSL Transforms (XSLT) Version 1.0. W3C http://www.w3.org/TR/1999/REC-xslt-19991116<br>XPath – RFC 3653 |
| Signature Type | enveloped or enveloping or detached |
| Digital Signature Certificate | (DER) X.509 V3 issued as per interoperability guidelines |

| | |
|---|---|
| Public Key Algorithms | RSA PKCS-1 Version 1.5 |
| ECC curve | NIST P-256, P-384, or P-521 |
| Long Term Signature formats | 1. XMLERS RFC 6283 and XAdES<br>2. XMLERS RFC 6283 and PAdES with XAdES |
| Time Stamp Token | As specified RFC 3161 in XML notation |

**12.** The basic Syntax of xml digital signature and terms used in the rule shall be as follows, namely:-

<Signature ID?>

<SignedInfo>

<CanonicalizationMethod/>

<SignatureMethod/>

(<Reference URI?>

(<Transforms>)?

<DigestMethod>

<DigestValue>

</Reference>+

</SignedInfo>

<SignatureValue>

(<KeyInfo>

(KeyName)

(KeyValue)

(RetrievalMethod)

(<X509Data>

(X509SKI)

(X509SubjectName)

(X509Certificate)

(X509CRL)

(X509Digest)

</x509Data>)

</Keyinfo>)

(<Object ID?>)*

</Signature>

Where "?" denotes zero or one occurrence; "+" denotes one or more occurrences; and "*" denotes zero or more occurrences."