**Bureau of Indian Standards**

*Draft Indian standard*

**इलेक्ट्रॉनिक हस्ताक्षर और इन्फ्रास्ट्रक्चर (ईएसआई) — हस्ताक्षर नीतियाँ;**

**भाग 3: हस्ताक्षर नीतियों के लिए एएसएन.1 प्रारूप**

**Electronic Signatures and Infrastructures (ESI); Signature Policies;**

**Part 3: ASN.1 format for signature policies**

ICS 35.020

|  |
| --- |
| Information Technology and Information Technology Enabled Services Sectional Committee, SSD 10 |

FOREWORD

(*Formal Clauses will be added later*)

This Indian Standard is adopted by the Bureau of Indian Standards (BIS) after the draft is finalized by the Information Technology and Information Technology enabled Services Sectional Committee SSS 10, and approved by the Service Sector Division Council.

This Indian Standard is developed to define an ASN.1 format of machine readable signature policies based on the building blocks that define technical constraints on digital signatures.

During the preparation of this standard, several consultation meetings and discussions were held with a wide cross section of stakeholders.

The present document is part 3 of a multi-part deliverable. Full details of the entire series can be found in part 1.

The present Indian Standard is the technical adoption of the European Standard “ETSI TS 119 172-3 V.1.1.1 (2019-12) Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 3: ASN.1 format for signature policies” developed by ETSI Technical Committee on Electronic Signatures and Infrastructures (ESI). Necessary modifications have been made to adapt it to India and are limited to referencing the Indian relevant regulatory context (Information Technology Act*,* 2000). The technical coverage is otherwise identical.

Specification signature policy ASN.1 module using X.680 ASN.1 syntax is given in ANNEX B (Normative).

*Draft Indian Standard*

**ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); SIGNATURE POLICIES; PART 3: ASN.1 FORMAT FOR SIGNATURE POLICIES**

# **SCOPE**

The present document defines an ASN.1 format of machine readable signature policies based on the building blocks that define technical constraints on digital signatures and are specified in ETSI TS 119 172-1.

Pure signature applicability rules, directly related to procedural constraints imposed by business processes, are out of the scope of the present document which does not define ASN.1 elements for the building blocks specified in ETSI TS 119 172-1 defining only applicability rules.

For each element of the machine readable signature policy, the present document references to the semantics described in ETSI TS 119 172-2 and defines the corresponding ASN.1 syntax.

The present document defines elements which can be used to describe technical constraints on signature creation, signature validation, and signature augmentation. These elements are designed in a way that it is possible to generate ASN.1 documents that include components of a signature generation policy, or/and signature validation policy, and/or signature augmentation policy.

An ASN.1 document conformant to the present specification, defines constraints (on generation, augmentation, validation, any combination of two of them, or the three of them) that one signature has to meet.

NOTE — Complex business processes, where several digital signatures need to be managed, having to meet different set of technical constraints, will require several ASN.1 documents conformant to the present document, each one defining one of these sets of technical constraints.

It is out of the scope to specify mechanisms for protecting the integrity of the machine-readable signature policy documents specified in the present document.

# **REFERENCES**

The standards listed in **Annex A** contain provisions, which through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent edition of these standards.

# **DEFINITION OF TERMS, SYMBOLS AND ABBREVIATIONS**

## **Terms**

For the purposes of the present document, the terms given in ETSI TS 119 172-1 and the following apply:

1. *Signature Applicability Rules — Set of rules, applicable to one or more digital signatures, that defines the requirements for determination of whether a signature is fit for a particular business or legal purpose*
2. *Signature Augmentation Constraint**—* Criteria used when augmenting a digital signature
3. *Signature Augmentation Policy**—* Set of signature augmentation constraints
4. *Signature Creation Application — A*pplication within the signature creation system that creates the AdES digital signature and relies on the signature creation device to create a digital signature value
5. *Signature Creation Constraint**—* Criteria used when creating a digital signature
6. *Signature Creation Policy**—* Set of signature creation constraints processed or to be processed by the signature creation application
7. *Signature Validation Application**—* Application that validates a signature against a signature validation policy, and that outputs a status indication (i.e. the signature validation status) and a signature validation report
8. *Signature Validation Constraint**—* Technical criteria against which a digital signature can be validated

*EXAMPLE:* As specified in ETSI TS 119 102-1.

1. *Signature Validation Policy —* Set of signature validation constraints processed or to be processed by the signature validation application

## **Symbols**

Void.

## **Abbreviations**

For the purposes of the present document, the following abbreviations apply:

|  |  |
| --- | --- |
| **Abbreviation** | **Description** |
| ASN.1 | Abstract Syntax Notation One |
| BER | Basic Encoding Rules |
| DER | Distinguished Encoding Rules |
| OID | Object IDentifier |
| URI | Uniform Resource Identifier |
| XML | eXtensible Markup Language |

# **ASN.1 SYNTAX FOR MACHINE PROCESSABLE SIGNATURE POLICY DOCUMENT**

## **Introduction**

### **4.1.1** *Technical Approach*

The present document takes as starting point the contents of ETSI TS 119 172-1, which defines the building blocks of a human readable signature policy document. These building blocks are of two types:

1. Building blocks defining applicability rules, which are the procedural constraints enforced by the business processes where the digital signatures are used. These procedural constraints, if not satisfied, could prevent further processing (in other words, accepting for the purpose of the business) a certain signed document even if the digital signature is technically valid.
2. Building blocks defining technical constraints, related with technical aspects of the digital signature and its technical validation (signature format, signature attributes, constraints on certificates, time-stamp tokens, revocation material data, etc.).

The present document specifies an ASN.1 format for the building blocks specified in ETSI TS 119 172-1, which define technical constraints, and allows building documents which define technical constraints in a machine-readable format.

The ASN.1 elements defined within the present contain information that clearly signal whether the constraints that they define apply to the generation of a signature, the validation of a signature, the augmentation of a signature, any combination of two of the former, or to the three of them. Therefore, the ASN.1 documents built using the present document may contain components of signature generation policy, or/and signature validation policy, and/or signature augmentation policy.

### **4.1.2** *ASN.1 Module*

Annex B defines the ASN.1 module which describes the elements defined in the present document.

### **4.1.3** *ASN.1 Encoding*

#### **4.1.3.1** DER

Distinguished Encoding Rules (DER) for ASN.1 types shall be as specified in Recommendation ITU-T X.690.

#### **4.1.3.2** BER

If Basic Encoding Rules (BER) are used for some ASN.1 types, it shall be as specified in Recommendation ITU‑T X.690.

### **4.1.4** *ASN.1 Type To Allow Extensions: The Other Type*

**Semantics**

The Other type shall contain an element of a type as defined by the OTHER.&id.

The Other type shall be parametized by a set of allowed OTHER.&id types, the MyOtherSet.

The MyOtherSet may be extensible, i.e. contains the "…".

NOTE *—* The Other type allows to extends specific types later with specific elements.

**Syntax**

The OTHER class and the Other type shall be as defined in **annex B** and is copied below for information.

OTHER ::= CLASS {

&id OBJECT IDENTIFIER UNIQUE,

&Value OPTIONAL }

WITH SYNTAX {

OTHER-ID &id

[OTHER-TYPE &Value] }

Other{OTHER:MyOtherSet} ::= SEQUENCE {

otherId OTHER.&id({MyOtherSet}),

otherValue OTHER.&Value({MyOtherSet}{@otherId}) OPTIONAL }

## **The SignaturePolicy Type**

### **4.2.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.2.1** of ETSI TS 119 172-2.

### **4.2.2** *Syntax*

The SignaturePolicy type shall be as defined in **annex B** and is copied below for information.

SignaturePolicy ::= SEQUENCE {

digest Digest,

policyComponents PolicyComponents}

The element of type Digest shall be as specified in ~~clause~~ **4.3.2**.

The element of type PolicyComponents shall be as specified in ~~clause~~ **4.4.2.**

## **The Digest Type**

### **4.3.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.3.1** of ETSI TS 119 172-2.

### **4.3.2** *Syntax*

The Digest type shall be as defined in annex B and is copied below for information.

Digest ::= OtherHashAlgAndValue

The type OtherHashAlgAndValue shall be as specified in ETSI EN 319 122-1.

An element of type OtherHashAlgAndValue contains a hashValue element and a hashAlgorithm element. The hashValue element shall contain the result of applying the algorithm identified in the corresponding hashAlgorithm element on the binary encoding of the PolicyComponents element specified in ~~clause~~ **4.4.2**.

## **The PolicyComponents Type**

### **4.4.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.4.1** of ETSI TS 119 172-2.

### **4.4.2** *Syntax*

The PolicyComponents type shall be as defined in **annex B** and is copied below for information.

PolicyComponents ::= SEQUENCE {

geneneralDetails GeneralDetails,

policyRules PolicyRules }

The element of type GeneralDetails shall be as specified in ~~clause~~ **4.5.2**.

The element of type PolicyRules shall be as specified in ~~clause~~ **4.14.2**.

## **The GeneralDetails Type**

### **4.5.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.5.1** of ETSI TS 119 172-2.

### **4.5.2** *Syntax*

The GeneralDetails type shall be as defined in annex B and is copied below for information.

GeneralDetails ::= SEQUENCE {

sigPolicyDetails SigPolicyDetails,

authorityDetails [0] AuthorityDetails OPTIONAL,

otherDetails [1] OtherDetails OPTIONAL }

The element of type SigPolicyDetails shall be as specified in ~~clause~~ **4.6.2**.

The element of type AuthorityDetails shall be as specified in ~~clause~~ **4.7.2**.

The element of type OtherDetails shall be as specified in ~~clause~~ **4.13.2**.

## **The SigPolicyDetails Type**

### **4.6.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.6.1** of ETSI TS 119 172-2.

### **4.6.2** *Syntax*

The SigPolicyDetails type shall be as defined in annex B and is copied below for information.

SigPolicyDetails ::= SEQUENCE {

policyIdentifier OBJECT IDENTIFIER,

policyName InternationalNames,

distributionPoints DistributionPoints OPTIONAL }

InternationalNames ::= SEQUENCE OF MultiLangText

MultiLangText ::= SEQUENCE {

lang PrintableString,

text UTF8String }

DistributionPoints ::= SEQUENCE SIZE (1..MAX) OF IA5String

The policyIdentifier element shall contain an object-identifier that uniquely identifies the signature policy.

The policyName element shall contain one or more names of the signature policy. Each name shall be qualified with an indication of a language, as per the definition of MultiLangText.

The lang element shall contain a tag conformant to IETF RFC 5646 and in lower case, that identifies the language in which the content of the text element is expressed.

The distributionPoints child element shall contain one or more URIs where the signature policy can be reached.

## **The AuthorityDetails Type**

### **4.7.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.7.1** of ETSI TS 119 172-2.

### **4.7.2** *Semantics*

The AuthorityDetails type shall be as defined in annex B and is copied below for information.

AuthorityDetails ::= SEQUENCE {

name [0] Name OPTIONAL,

tradeName [1] TradeName OPTIONAL,

postalAddresses PostalAddresses,

electronicAddresses ElectronicAddresses,

contactPersons [2] ContactPersons OPTIONAL}

The element of type Name shall be as specified in ~~clause~~ **4.8.2**.

The element of type TradeName shall be as specified in ~~clause~~ **4.9.2**.

The element of type PostalAddresses shall be as specified in ~~clause~~ **4.10.2**.

The element of type ElectronicAddresses shall be as specified in ~~clause~~ **4.11.2**.

The element of type ContactPersons shall be as specified in ~~clause~~ **4.12.2**.

## **The Name Type**

### **4.8.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.8.**1 of ETSI TS 119 172-2.

### **4.8.2** *Semantics*

The Name type shall be as defined in annex B and is copied below for information.

Name ::= InternationalNames

The element of type InternationalNames shall be as specified in ~~clause~~ **4.6.2**.

## **The TradeName Type**

### **4.9.1** *Semantics*

The semantics shall be as in ~~clause~~ 4.9.1 of ETSI TS 119 172-2 [3].

### **4.9.2** *Syntax*

The TradeName type shall be as defined in annex B and is copied below for information.

TradeName::= InternationalNames

The type InternationalNames shall be as specified in ~~clause~~ **4.6.2**.

## **The PostalAddresses Type**

### **4.10.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.10.1** of ETSI TS 119 172-2.

### **4.10.2** *Syntax*

The PostalAddresses type shall be as defined in annex B and is copied below for information.

PostalAddresses ::= SEQUENCE OF PostalAddress

The type PostalAddress shall be as specified in ETSI EN 319 122-1.

## **The ElectronicAddresses Type**

### **4.11.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.11.1** of ETSI TS 119 172-2.

### **4.11.2** *Syntax*

The ElectronicAddresses type shall be as defined in annex B and is copied below for information.

ElectronicAddresses::= SEQUENCE OF ElectronicAddresse

ElectronicAddresse ::= MultiLangURI

MultiLangURI ::= SEQUENCE {

lang PrintableString,

uri IA5String }

Each element of type ElectronicAddresses shall be qualified with an indication of a language, as per the definition of MultiLangURI.

The lang element shall contain a tag conformant to IETF RFC 5646 and in lower case, that identifies the language in which the content pointed-to by the URI contained in the uri element is expressed.

## **The ContactPersons Type**

### **4.12.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.12.1** of ETSI TS 119 172-2.

### **4.12.2** *Syntax*

The ContactPersons type shall be as defined in annex B and is copied below for information.

ContactPersons ::= SEQUENCE OF ContactPerson

ContactPerson ::= SEQUENCE {

name UTF8String,

electronicAddresses ElectronicAddresses,

phoneNumbers SEQUENCE OF PrintableString}

An element of type ElectronicAddresses shall be as specified in ~~clause~~ **4.11.2**.

Each PrintableString value in the phoneNumbers element shall contain exactly one phone number of the contact person. Each phone number shall start with the '+' character followed by the country prefix.

## **The OtherDetails Type**

### **4.13.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.13.1** of ETSI TS 119 172-2.

### **4.13.2** *Syntax*

The OtherDetails type shall be as defined in annex B and is copied below for information.

OtherDetails ::= SEQUENCE {

dateOfIssue GeneralizedTime,

signingPeriod [0] SigningPeriod OPTIONAL,

others [1] SEQUENCE SIZE (1..MAX) OF Other{{OtherDetailsOtherSet}} OPTIONAL}

SigningPeriod ::= SEQUENCE {

notBefore GeneralizedTime,

notAfter GeneralizedTime OPTIONAL }

OtherDetailsOtherSet OTHER ::= {...}

The elements of type GeneralizedTime shall be as specified in Recommendation ITU-T X.680.

NOTE — For the moment there are no OTHER.&id defined for the OtherDetailsOtherSet.

## **The PolicyRules Type**

### **4.14.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.14.1** of ETSI TS 119 172-2.

### **4.14.2** *Syntax*

The PolicyRules type shall be as defined in annex B and is copied below for information.

PolicyRules ::= SEQUENCE OF PolicyRuleWithScope

PolicyRuleWithScope ::= SEQUENCE {

rule SigPolicyRule,

scope SigPolicyScope OPTIONAL}

SigPolicyRule ::= CHOICE {

commitmentRules [0] CommitmentRules,

basicRule [1] BasicRule }

BasicRule ::= CHOICE {

dataToBeSignedRules [0] DataToBeSignedRules,

sigToDTBSRelationRules [1] SigToDTBSRelationRules,

dTBSCardinality [2] DTBSCardinality,

sigDTBSRelativePosition [3] SigDTBSRelativePosition,

sigFormatsAndLevels [4] SigFormatsAndLevels,

augmentationRules [5] AugmentationRules,

signingCertRules [6] SigningCertRules,

timeEvidencesRules [7] TimeEvidencesRules,

signerAttributeConstraints [8] SignerAttributeConstraints,

qualifyingAttributesRules [9] QualifyingAttributesRules,

sCDLoARules [10] SCDLoARules,

cryptoSuitesRules [11] CryptoSuitesRules,

otherRules [12] Other{{BasicRuleOtherSet}}

}

SigPolicyScope ::= ENUMERATED {

generation (0),

validation (1),

augmentation (2) }

BasicRuleOtherSet OTHER ::= {...}

The element of type CommitmentRules shall be as specified in ~~clause~~ **4.15.2**.

The element of type DataToBeSignedRules shall be as specified in ~~clause~~ **4.16.2**.

The element of type SigToDTBSRelationRules shall be as specified in ~~clause~~ **4.17.2**.

The element of type DTBSCardinality shall be as specified in ~~clause~~ **4.18.2**.

The element of type SigDTBSRelativePosition shall be as specified in ~~clause~~ **4.19.2**.

The element of type SigFormatAndLevels shall be as specified in ~~clause~~ **4.20.2**.

The element of type AugmentationRules shall be as specified in ~~clause~~ **4.21.2**.

The element of type SigningCertRules shall be as specified in ~~clause~~ **4.24.4.2**.

The element of type TimeEvidLoARules shall be as specified in ~~clause~~ **4.25.2**.

The element of type SignerAttributeConstraints shall be as specified in ~~clause~~ **4.26.2**.

The element of type QualifyingAttributesRules shall be as specified in ~~clause~~ **4.27.2.**

The element of type SCDLoARules shall be as specified in ~~clause~~ **4.28.2**.

The element of type CryptoSuitesRules shall be as specified in ~~clause~~ **4.29.2**.

NOTE — For the moment there are no OTHER.&id defined for the BasicRuleOtherSet.

## **The CommitmentRules Type**

### **4.15.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.15** of ETSI TS 119 172-2.

### **4.15.2** *Syntax*

The CommitmentRules type shall be as defined in annex B and is copied below for information.

CommitmentRules ::= SEQUENCE OF CommitmentRule

CommitmentRule ::= SEQUENCE {

commitments SEQUENCE OF Commitment,

matchingIndicator MatchingIndicator,

basicRules SEQUENCE OF BasicRule}

Commitment ::= SEQUENCE {

commitmentIdentifier CommitmentTypeIdentifier,

details SEQUENCE SIZE (1..MAX) OF MultiLangString OPTIONAL}

MultiLangString ::= SEQUENCE {

lang PrintableString,

uri UTF8String }

MatchingIndicator ::= ENUMERATED {

all (0),

none (1),

atLeastOne(2) }

Each Commitment element shall contain an identifier of one commitment taken by the signer (CommitmentTypeIdentifier), and may also contain additional textual details in different languages.

Each entry of details shall be qualified with an indication of a language, as per the definition of MultiLangURI, in ~~clause~~ **4.11.2**.

The element of type CommitmentTypeIdentifier shall be as specified in ETSI EN 319 122-1.

The element of type BasicRule shall be as specified in ~~clause~~ **4.14.2**.

## **The DataToBeSignedRules Type**

### **4.16.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.16.1** of ETSI TS 119 172-2.

### **4.16.2** *Syntax*

The DataToBeSignedRules type shall be as defined in annex B and is copied below for information.

DataToBeSignedRules ::= SEQUENCE OF DataToBeSignedRule

DataToBeSignedRule ::= SEQUENCE {

anyOfMimeType [0] SEQUENCE SIZE (1..MAX) OF UTF8String OPTIONAL,

noneOfMimeType [1] SEQUENCE SIZE (1..MAX) OF UTF8String OPTIONAL }

The DataToBeSignedRule shall not be empty.

## **The SigToDTBSRelationRules Type**

### **4.17.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.17.1** of ETSI TS 119 172-2.

### **4.17.2** *Syntax*

The SigToDTBSRelationRules type shall be as defined in annex B and is copied below for information.

SigToDTBSRelationRules::= SEQUENCE {

dTBSCardinality DTBSCardinality,

sigDTBSRelativePosition [0] SigDTBSRelativePosition OPTIONAL,

sigFormatsAndLevels [1] SigFormatsAndLevels OPTIONAL }

The element of type DTBSCardinality shall be as specified in ~~clause~~ **4.18.2**.

The element of type SigDTBSRelativePosition shall be as specified in ~~clause~~ **4.19.2**.

The element of type SigFormatsAndLevels shall be as specified in ~~clause~~ **4.20.2**.

## **The DTBSCardinality Type**

### **4.18.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.18.1** of ETSI TS 119 172-2.

### **4.18.2** *Syntax*

The DTBSCardinality type shall be as defined in annex B and is copied below for information.

DTBSCardinality::= SEQUENCE {

maxDTBSNumber [0] MaxDTBSNumber OPTIONAL,

minDTBSNumber [1] MinDTBSNumber OPTIONAL }

MaxDTBSNumber ::= SEQUENCE {

dTBSNumber INTEGER,

maxValueQualifier MaxValueQualifier }

MaxValueQualifier ::= ENUMERATED {

lessThan (0),

lessOrEqualTo (1),

equal (2) }

MinDTBSNumber ::= SEQUENCE {

dTBSNumber INTEGER,

minValueQualifier MinValueQualifier }

MinValueQualifier ::= ENUMERATED {

higherThan (0),

higherOrEqualTo (1),

equal (2) }

## **The SigDTBSRelativePosition Type**

### **4.19.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.20.1** of ETSI TS 119 172-2.

### **4.19.2** *Syntax*

The SigDTBSRelativePosition type shall be as defined in annex B and is copied below for information.

SigDTBSRelativePosition ::= SEQUENCE OF SigDTBSRelativePositionValue

SigDTBSRelativePositionValue::= ENUMERATED {

envelopingSig (0),

envelopedSig (1),

detachedSig (2),

aSiC (3) }

The value of SigDTBSRelativePosition element shall be a list of one or more SigDTBSRelativePositionValue entries. Each entry in the list shall indicate either that the signature is enclosed in an ASiC container (value "ASiC"), or the relative position of the signature and one of the data object it signs ("EnvelopingSig" for enveloping signatures, "EnvelopedSig" for enveloped signatures, and "DetachedSig" for detached signatures).

NOTE — As a result of their characteristics, a policy for XML and XAdES digital signatures could include up to three values, other than ASiC. An XML or a XAdES digital signature can be enveloped in one of the data objects it signs, enveloping a second signed data object, and detached from a third signed data object.

If the value "ASiC" is present in the list, no other value shall be present. The presence of this value means that the signature shall appear in an ASiC container.

For each value within the list other than "ASiC", the signature shall be placed with respect to one or more signed digital objects as indicated by that value.

*EXAMPLE:*

If the value of SigDTBSRelativePosition contains "EnvelopingSig” and “DetachedSig", the signature policy establishes that the signature will be enveloping one or more signed data objects and will be detached from one or more signed data objects.

## **The SigFormatsAndLevels Type**

### **4.20.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.20.1** of ETSI TS 119 172-2.

### **4.20.2** *Syntax*

The SigFormatsAndLevels type shall be as defined in annex B and is copied below for information.

SigFormatsAndLevels ::= SEQUENCE {

sigFormats [0] SEQUENCE SIZE (1..MAX) OF IA5String OPTIONAL,

sigLevels [1] SEQUENCE SIZE (1..MAX) OF IA5String OPTIONAL}

Instances of SigFormatAndLevels shall not be empty.

Absence of the sigFormats element shall indicate that any format is allowed.

The sigFormats shall contain URIs identifying the admitted signature formats.

Absence of the sigLevels element shall indicate that any level is allowed.

The sigLevels shall contain URIs identifying the admitted signature levels.

*EXAMPLE:*

ETSI TS 119 192 defines URIs for different signature formats and levels.

## **The AugmentationRules Type**

### **4.21.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.21.1** of ETSI TS 119 172-2.

### **4.21.2** *Syntax*

The DTBSCardinality type shall be as defined in annex B and is copied below for information.

AugmentationRules ::= SEQUENCE {

previousValidationRequired BOOLEAN,

levelID IA5String,

augQualifier AugmentationQualifier }

AugmentationQualifier ::= ENUMERATED {

thisLevel (0),

minLevel (1),

maxLevel (2) }

The element levelID shall contain an URI describing the augmentation level.

*EXAMPLE:*

ETSI TS 119 192 defines URIs for different signature formats and levels.

## **Types For Defining Constraints On Certificates' Trust And Certificates Revocation Status**

### **4.22.1** *Introduction*

The present clause defines four types:

1. TrustAnchorsList which defines the trust anchors.
2. NameConstraints which defines constraints on the names of entities.
3. PolicyConstraints for defining constraints on certificate policies.
4. CertificateTrustTrees which defines constraints on the trust conditions required to certificates.

### **4.22.2** *The TrustAnchors Type*

#### **4.22.2.1** Semantics

The semantics shall be as in ~~clause~~ **4.22.2.1** of ETSI TS 119 172-2.

#### **4.22.2.2** Syntax

The TrustAnchors type shall be as defined in annex A and is copied below for information.

TrustAnchors ::= SEQUENCE OF TrustAnchor

TrustAnchor ::= CHOICE {

certificate CertAndReliableTime,

tAInTrustedList TAsInTrustedList }

CertAndReliableTime ::= SEQUENCE {

cert Certificate,

reliableUntil GeneralizedTime OPTIONAL }

TAsInTrustedList::= SEQUENCE {

uri IA5String,

serviceTypes [0] SEQUENCE SIZE (1..MAX) OF IA5String OPTIONAL,

serviceStatuses [1] SEQUENCE SIZE (1..MAX) OF IA5String OPTIONAL }

The element of type Certificate shall be as specified in IETF RFC 5912.

The element uri shall contain a reference to the Trusted List.as defined in ETSI TS 119 612.

The element serviceType, when present, shall contain a non-empty list of URIs expressing acceptable service types.

The element serviceStatuses, when present, shall contain a non-empty list of URIs expressing acceptable service statuses.

### **4.22.3** *The NameConstraints Type*

#### **4.22.3.1** Semantics

The semantics shall be as in ~~clause~~ **4.22.3.1** of ETSI TS 119 172-2.

#### **4.22.3.2** Syntax

The NameConstraints type shall be as defined in annex B and is copied below for information.

NameConstraints ::= SEQUENCE {

permittedSubtrees [0] GeneralSubtrees OPTIONAL,

excludedSubtrees [1] GeneralSubtrees OPTIONAL }

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {

base GeneralName,

minimum [0] BaseDistance DEFAULT 0,

maximum [1] BaseDistance OPTIONAL }

BaseDistance ::= INTEGER (0..MAX)

The element of type GeneralName shall be as specified in IETF RFC 5912.

### **4.22.4** *The PolicyConstraints Type*

#### **4.22.4.1** Semantics

The semantics shall be as in ~~clause~~ **4.22.4.1** of ETSI TS 119 172-2.

#### **4.22.4.2** Syntax

The PolicyConstraints type shall be as defined in annex B and is copied below for information.

PolicyConstraints ::= SEQUENCE {

requireExplicitPolicy [0] SkipCerts OPTIONAL,

inhibitPolicyMapping [1] SkipCerts OPTIONAL }

SkipCerts ::= INTEGER (0..MAX)

### **4.22.5** *The CertificateTrustTrees Type*

#### **4.22.5.1** Semantics

The semantics shall be as in ~~clause~~ **4.22.5.1** of ETSI TS 119 172-2.

#### **4.22.5.2** Syntax

The CertificateTrustTrees type shall be as defined in annex B and is copied below for information.

CertificateTrustTrees ::= SEQUENCE OF CertificateTrustPoint

CertificateTrustPoint ::= SEQUENCE {

trustAnchors TrustAnchors,

pathLenConstraint [0] PathLenConstraint OPTIONAL,

acceptablePolicySet [1] AcceptablePolicySet OPTIONAL,

nameConstraints [2] NameConstraints OPTIONAL,

policyConstraints [3] PolicyConstraints OPTIONAL,

userCertPath [4] UserCertPath OPTIONAL }

PathLenConstraint ::= INTEGER (0..MAX)

AcceptablePolicySet ::= SEQUENCE OF CertPolicyId

CertPolicyId ::= OBJECT IDENTIFIER

UserCertPath ::= CHOICE {

asInSignature [0] BOOLEAN,

path [1] SEQUENCE OF Certificate }

The element of type TrustAnchors shall be as specified in ~~clause~~ **4.22.2.2**.

The element of type NameConstraints shall be as specified in ~~clause~~ **4.22.3.2**.

The element of type PolicyConstraints shall be as specified in ~~clause~~ **4.22.4.2.**

## **Types For Defining Constraints On Certificates' Revocation Status**

### **4.23.1** *Introduction*

The present clause defines two types:

1. CertificateRevReq which defines constraints on the certificate revocation checks procedures.
2. CertificateRevStatus which defines constraints on the trust conditions required on the certificates' revocation data.

### **4.23.2** *The CertificateRevReq Type*

#### **4.23.2.1** Semantics

The semantics shall be as in ~~clause~~ **4.23.2.1** of ETSI TS 119 172-2.

#### **4.23.2.2** Syntax

The CertificateRevReq type shall be as defined in annex B and is copied below for information.

CertificateRevReq ::= SEQUENCE {

endCertRevReq EnuRevReq,

caCerts EnuRevReq }

EnuRevReq ::= ENUMERATED {

clrCheck (0),

ocspCheck (1),

bothCheck (2),

eitherCheck (3),

noCheck (4),

other (5)}

### **4.23.3** *The CertificateRevTrust Type*

#### **4.23.3.1** Semantics

The semantics shall be as in ~~clause~~ **4.23.3.1** of ETSI TS 119 172-2.

#### **4.23.3.2** Syntax

The CertificateRevTrust type shall be as defined in annex B and is copied below for information.

CertificateRevTrust ::= SEQUENCE {

certificateRevReq CertificateRevReq,

freshness [0] Freshness OPTIONAL,

sigCertIssuedByCAKeepsExpiredRevokedCertsInfo [1] Duration OPTIONAL }

Freshness ::= CHOICE {

maxDifferenceRevocationAndValidation [0] Duration,

timeAfterSignature [1] Duration }

Duration ::= PrintableString

The element of type CertificateRevReq shall be as specified in ~~clause~~ **4.23.2.2**.

The value of the timeAfterSignature element shall be the time after the best-signature time as computed in ETSI TS 119 102-1.

The value of the sigCertIssuedByCAKeepsExpiredRevokedCertsInfo element shall be a time indication.

If the sigCertIssuedByCAKeepsExpiredRevokedCertsInfo element is present then it is mandated that the signing certificate has been issued by a certification authority that keeps revocation notices for revoked certificates even after they have expired, for a period of time exceeding the value of this child element. If the SigCertIssuedByCAKeepsExpiredRevokedCertsInfo child is absent, this constraint is not mandated.

The content of an element of Duration type shall contain a printable string expressing the duration as defined for the duration type as defined in ~~clause~~ **3.2.6** of the description of the XML Schema.

NOTE — The duration type in [the XMLSchema](http://www.w3.org/2001/XMLSchema) is specified in the following way "PnYnMnDTnHnMnS" where:

* P indicates the period (required)
* nY indicates the number of years
* nM indicates the number of months
* nD indicates the number of days
* T indicates the start of a time section (required when specifying hours, minutes, or seconds)
* nH indicates the number of hours
* nM indicates the number of minutes
* nS indicates the number of seconds

## **The SigningCertRules Type**

### **4.24.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.24.1** of ETSI TS 119 172-2.

### **4.24.2** *Syntax*

The SigningCertRules type shall be as defined in annex B and is copied below for information.

SigningCertRules ::= SEQUENCE {

signingCertTrustConditions SigningCertTrustConditions,

mandatedSigningCertInfo MandatedSigningCertInfo OPTIONAL }

The element of type CertificateRevReq shall be as specified in ~~clause~~ **4.24.4.2**.

The element of type MandatedSigningCertInfo shall be as defined in ~~clause~~ **4.24.3.2**.

### **4.24.3** *The MandatedSigningCertInfor Typo*

#### **4.24.3.1** Semantics

The semantics shall be as in ~~clause~~ **4.24.3.1** of ETSI TS 119 172-2.

#### **4.24.3.2** Syntax

The MandatedSigningCertInfo element shall be as defined in annex B and is copied below for information.

MandatedSigningCertInfo ::= ENUMERATED {

signingCertOnly (0),

fullPath (1) }

### **4.24.4** *The SigningCertTrustConditions Typo*

#### **4.24.4.1** Semantics

The semantics shall be as in ~~clause~~ **4.24.4.1** of ETSI TS 119 172-2.

#### **4.24.4.2** Syntax

The SigningCertTrustConditions type shall be as defined in annex B and is copied below for information.

SigningCertTrustConditions ::= SEQUENCE {

signerTrustTrees CertificateTrustTrees,

signerRevTrust CertificateRevTrust }

The element of type CertificateTrustTrees shall be as specified in ~~clause~~ **4.22.5.2**.

The element of type CertificateRevTrust shall be as specified in ~~clause~~ **4.23.3.2**.

## **The TimeEvidencesRules Type**

### **4.25.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.25.1** of ETSI TS 119 172-2.

### **4.25.2** *Syntax*

The TimeEvidLoARules type shall be as defined in annex B and is copied below for information.

TimeEvidencesRules::= SEQUENCE OF RulesForSetOfEvidences

RulesForSetOfEvidences ::= SEQUENCE {

evidenceIdentifiers SEQUENCE OF IA5String,

levelOfAssurance IA5String,

timeStampTrustCondition TimestampTrustCondition OPTIONAL }

TimestampTrustCondition ::= SEQUENCE {

ttsCertificateTrustTrees [0] CertificateTrustTrees OPTIONAL,

ttsRevReq [1] CertificateRevReq OPTIONAL,

ttsNameConstraints [2] NameConstraints OPTIONAL,

signatureTimestampDelay [3] DeltaTime OPTIONAL }

DeltaTime ::= SEQUENCE {

deltaSeconds INTEGER,

deltaMinutes INTEGER,

deltaHours INTEGER,

deltaDays INTEGER }

The element of type CertificateTrustTrees shall be as specified in ~~clause~~ **4.22.5.2**.

The element of type CertificateRevReq shall be as specified in ~~clause~~ **4.23.2.2**.

The element of type NameConstraints shall be as specified in ~~clause~~ **4.22.3.2**.

## **The SignerAttributeConstraints Type**

### **4.26.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.26.1** of **ETSI TS 119 172-2**.

### **4.26.2** *Syntax*

The SignerAttributeConstraints type shall be as defined in annex B and is copied below for information.

SignerAttributeConstraints ::= SEQUENCE {

noSignerAttributesAllowed BOOLEAN,

constraintsOnOneSetOfAttributes SEQUENCE OF AttributeSetConstraints }

AttributeSetConstraints ::= SEQUENCE {

howCertAttribute HowCertAttribute,

attrCertificateTrustTrees [0] CertificateTrustTrees OPTIONAL,

attrRevReq [1] CertificateRevTrust OPTIONAL,

attributeConstraints [2] AttributeConstraints OPTIONAL }

HowCertAttribute ::= ENUMERATED {

claimedAttribute (0),

certifiedAttribtes (1),

signedAssertions (2),

any (3)

AttributeConstraints ::= SEQUENCE {

attributeIdMustBePresent [0] OBJECT IDENTIFIER OPTIONAL,

attributeValueConstraints [1] SEQUENCE SIZE (1..MAX) OF

Other{{AttributeValueConstraintsOtherSet}} OPTIONAL }

AttributeValueConstraintsOtherSet OTHER ::= {...}

The element of type CertificateTrustTrees shall be as specified in ~~clause~~ **4.22.5.2**.

The element of type CertificateRevTrust shall be as specified in ~~clause~~ **4.23.3.2**.

NOTE — For the moment there are no OTHER.&id defined for the AttributeValueConstraintsOtherSet.

## **The QualifyingAttributesRules Type**

### **4.27.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.27.1** of ETSI TS 119 172-2.

### **4.27.2** *Syntax*

The QualifyingAttributesRules type shall be as defined in annex B and is copied below for information.

QualifyingAttributesRules ::= SEQUENCE OF LevelAttributesRules

LevelAttributesRules ::= SEQUENCE {

levelIdentifier [0] IA5String,

signedAttributes [1] SignatureAttributes OPTIONAL,

unsignedAttributes [2] SignatureAttributes OPTIONAL }

SignatureAttributes ::= SEQUENCE OF CHOICE {

choice [0] SEQUENCE OF SignatureAttribute,

sigAttr [1] SignatureAttribute }

SignatureAttribute ::= SEQUENCE {

identifier OBJECT IDENTIFIER,

mandatory BOOLEAN }

## **The SCDLoARules Type**

### **4.28.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.28.1** of ETSI TS 119 172-2.

### **4.28.2** *Syntax*

The SCDLoARules type shall be as defined in annex B and is copied below for information.

SCDLoARules ::= IA5String

The SCDDLoARules shall be a URI value indicating the Level of Assurance of the signature creation device.

## **The CryptoSuitesRules** **Type**

### **4.29.1** *Semantics*

The semantics shall be as in ~~clause~~ **4.29.1** of ETSI TS 119 172-2.

### **4.29.2** *Syntax*

The CryptoSuitesRules type shall be as defined in annex B and is copied below for information.

CryptoSuitesRules ::= SEQUENCE OF AlgConstraints

AlgConstraints ::= SEQUENCE {

algID OBJECT IDENTIFIER,

usages SEQUENCE SIZE (1..MAX) OF IA5String,

minKeyLength [0] INTEGER OPTIONAL,

minHashLength [1] INTEGER OPTIONAL,

other Other{{AlgConstraintsOtherSet}} OPTIONAL

}

AlgConstraintsOtherSet OTHER ::= {...}

The usages element shall contain URIs as in the UsageType in ~~clause~~ **4.29.2** of ETSI TS 119 172-2.

NOTE — For the moment there are no OTHER.&id defined for the AlgConstraintsOtherSet.

**ANNEX A**

(*Clause 2*)

**LIST OF REFERRED STANDARDS**

|  |  |
| --- | --- |
| *IS No.* | *Title* |
| ETSI EN 319 122-1 | Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures |
| ETSI TS 119 612 | Electronic Signatures and Infrastructures (ESI); Trusted Lists |
| ETSI TS 119 172-2 | Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 2: XML format for signature policies |
| Recommendation ITU-T X.680 (2015) | Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation |
| Recommendation ITU-T X.690 (2015) | Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) |
| IETF RFC 5646 | Tags for Identifying Languages |
| IETF RFC 5912 (2010) | New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX) |
| W3C Recommendation | XML Schema Part 2: Datatypes Second Edition  NOTE — See <https://www.w3.org/TR/xmlschema-2/> |
| ETSI TS 119 102-1 | Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation |
| ETSI TS 119 172-1 | Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents |
| ETSI TS 119 192 | Electronic Signatures and Infrastructures (ESI); AdES related Uniform Resource Identifier |

**ANNEX** **B**

(Normative)

**SPECIFICATION** **SIGNATURE POLICY ASN.1 MODULE USING X.680 ASN.1 SYNTAX**

The file at <https://forge.etsi.org/rep/esi/x19_17203_ASN1_sign-policies/raw/v1.1.1/19172asn1Module.txt> contains ASN.1 module ETSI-SigPolicy-ASN1 { itu-t(0) identified-organization(4) etsi(0) sigpolicy-asn1(19172) id-mod(0) sigpolicy-syntax680(1)}.