ETSI TS 119 322 V1.1.1 (2022-11)

Electronic Signatures and Infrastructure (ESI);
Schema for machine-readable cryptographic algorithms, and cipher suites catalogues

Reference
DTS/ESI-0019322

Keywords
algorithm, interoperability, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The assessment of the suitability of cryptographic algorithms, and cipher suites used in the context of digital signatures, seals, or timestamps, as well as related certificates, is essential during their respective lifecycles. Starting from the creation of a signature at a given time and date when only certain algorithms meet the requirements regarding e.g. the collision resistance, and every time when validating the signature until the data is no longer needed or submitted to a preservation system one needs to assess the suitability of all algorithms involved and their respective validity periods.

Catalogues, such as ETSI TS 119 312 [i.2] or the agreed cryptographic mechanisms from SOG-IS [i.3], when given only in human-readable form, need to be translated into a machine-readable one by each provider of signature-related services individually to implement reliable digital-only processes.

The present document derives a generic schema based on IETF RFC 5698 [1] and initially specifies two different formats thereof. It aims at supporting crypto agility, at increasing the (cross-border) interoperability as well as at supporting backwards compatibility with regards to systems already in place when defining this schema such as long-term preservation systems.

1 Scope

The present document provides a generic schema for machine-readable cryptographic algorithms, and cipher suites catalogues based on IETF RFC 5698 [1] and specifies different formats such as XML [i.4] and JSON [i.5].

The present document is limited to a descriptive schema for algorithms and all parameters involved. No assessment of the suitability of any cryptographic algorithm, or cipher suite is given in the present document.

The present document focuses on signature-related algorithms, and cipher suites, and puts an emphasis on enabling a refined suitability description of the algorithms with respect to its status of recommendation as well as the specific context of usage an algorithm is assessed for.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

[1] IETF RFC 5698 (11-2009): "Data Structure for the Security Suitability of Cryptographic Algorithms (DSSC)".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.2] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.3] SOG-IS Crypto Working Group: "SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms" Version 1.2, January 2020.

[i.4] The World Wide Web Consortium (W3C®): "Extensible Markup Language".

NOTE: Available at https://www.w3.org/XML/.

[i.5] IETF RFC 8259 (12-2017): "The JavaScript Object Notation (JSON) Data Interchange Format".

NOTE: Available at RFC 8259: The JavaScript Object Notation (JSON) Data Interchange Format (rfc-editor.org).

[i.7] JSON Schema Specification.

NOTE: Available at http://json-schema.org/specification.html.

[i.8] The World Wide Web Consortium (W3C®): "XML namespace definition".

NOTE: Available at http://www.w3.org/2001/xml.xsd.

[i.9] ETSI TS 119 182-1: "Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures".

[i.10] ESTI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.1], IETF RFC 5698 [1] and the following apply:

AdES (digital) signature: digital signature that is either a CAdES signature (CMS), or a PAdES signature (PDF), or a XAdES signature (XML), or a JAdES signature (JSON)

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 119 001 [i.1] and the following apply:

CMS	Cryptographic Message Syntax
DSA	Digital Signature Algorithm
DSSC	Data Structure for the Security Suitability of Cryptographic Algorithms
JSON	JavaScript Object Notation
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PKCS	Public-Key Cryptography Standard
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
RSA	RSA cryptosystem, named after Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SOG-IS	Senior Officials Group Information Systems Security
URI	Uniform Resource Identifier
XML	eXtensible Markup Language

4 Overall structure of algorithms, and cipher suites catalogues

4.1 Overview

The present document is based on IETF RFC 5698 [1].

A machine-readable catalogue may contain only a subset of the defined algorithms.

Clause 4.2 describes the semantic of the different elements of the machine-readable algorithm catalogue independent of the specific format used.

Annexes A and B specify the format-specific syntax for XML [i.4], [i.8] and JSON [i.5], [i.7] instances of this schema, respectively.

All the semantic of elements shall remain as defined in IETF RFC 5698 [1] where not stated otherwise.

4.2 Elements of a machine-readable algorithm catalogue

4.2.1 Security-suitability-policy

The *security-suitability-policy* element shall be the root element of the machine-readable catalogue.

The semantic of the *security-suitability-policy* element shall be as defined IETF RFC 5698 [1], clause 3.1.

4.2.2 Policy-name

The semantic of the *policy-name* element shall be as defined in IETF RFC 5698 [1], clause 3.2.

4.2.3 Publisher

The semantic of the *publisher* element shall be as defined in IETF RFC 5698 [1], clause 3.3.

4.2.4 Policy-issue-date

The semantic of the *policy-issue-date* element shall be as defined in IETF RFC 5698 [1], clause 3.4.

4.2.5 NextUpdate

The semantic of the *next-update* element shall be as defined in IETF RFC 5698 [1], clause 3.5.

4.2.6 Usage

The semantic of the *usage* element shall be as defined in IETF RFC 5698 [1], clause 3.6.

4.2.7 Algorithm

The semantic of the *algorithm* element shall be as defined in IETF RFC 5698 [1], clause 3.7.

4.2.8 Algorithm-identifier

The semantic of the *algorithm-identifier* element shall be as defined in IETF RFC 5698 [1], clause 3.8.

4.2.9 Evaluation

4.2.9.1 General description

The semantic of the *evaluation* element shall be as defined in IETF RFC 5698 [1], clause 3.9.

The *evaluation* element may contain a *more-details* element.

The *more-details* element may contain zero, one or more *algorithm-usage* elements as defined in clause 4.2.9.2 to allow parameter- and context-specific evaluations of cryptographic mechanisms.

The *more-details* element may contain a *recommendation* element as defined in clause 4.2.9.3 to distinguish between recommended and legacy mechanisms, as defined in ETSI TS 119 312 [i.2], clause 3.1.

The syntax is specified in clauses A.9 (XML) and B.2.9 (JSON), respectively.

4.2.9.2 Algorithm-usage

The *algorithm-usage* element shall contain a URI which allows to further distinguish the validity period of an algorithm based on the usage.

EXAMPLE 1: It allows to differentiate between signature creation and signature validation use cases.

NOTE 1: The amount of data of certificates is comparably small to arbitrary documents, hence when applying a hash algorithm to certificates they are less affected by lowered collision-resistance of the hash algorithm, which in turn could allow for a prolonged suitability period in this specific use case.

Omitting all usage types shall be equivalent to no restriction at all.

When the *validity* element is provided in the corresponding *evaluation* element containing an *algorithm-usage* element, all use cases hierarchical below the one given are included according to the hierarchy diagram (figure 1).

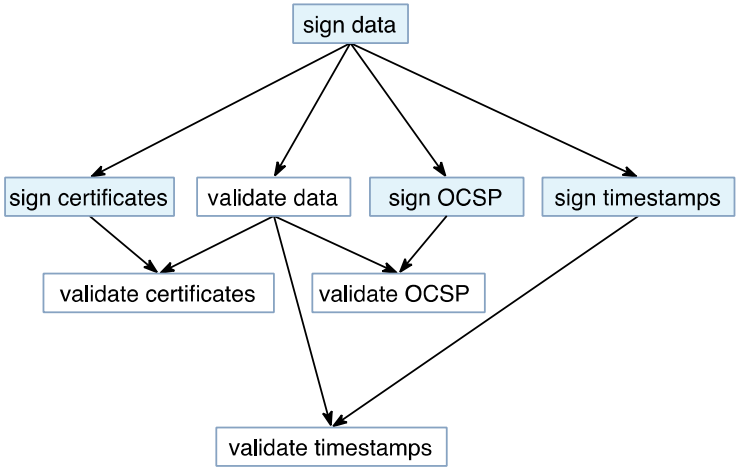

Figure 1: Algorithm usage type hierarchy

EXAMPLE 2: Sign data will include all other types, i.e. it is equivalent to no restriction when no further restriction is provided for the use cases lying below.

NOTE 2: The hierarchy tree inherently includes ambiguity, i.e. there is more than one path from root (sign data) to tree leaves of validation types.

The following algorithm-usage URIs are defined:

- http://uri.etsi.org/19322/sign_data shall be used to indicate that the evaluation is applicable for any signed data.
- http://uri.etsi.org/19322/sign_data/sign_certificates shall be used to indicate that the evaluation is applicable for signing certificates.
- http://uri.etsi.org/19322/sign_data/sign_ocsp shall be used to indicate that the evaluation is applicable for signing OCSP responses.
- http://uri.etsi.org/19322/sign_data/sign_timestamps shall be used to indicate that the evaluation is applicable for signing timestamps.
- http://uri.etsi.org/19322/sign_data/sign_certificates shall be used to indicate that the evaluation is applicable for signing certificates.
- http://uri.etsi.org/19322/sign_data/sign_certificates shall be used to indicate that the evaluation is applicable for signing certificates.
- http://uri.etsi.org/19322/sign_data/validate_data shall be used to indicate that the evaluation is applicable for the validation of any signed data.

- http://uri.etsi.org/19322/sign_data/validate_data/validate_certificates shall be used to indicate that the evaluation is applicable for the validation of certificates.
- http://uri.etsi.org/19322/sign_data/validate_data/validate_ocsp shall be used to indicate that the evaluation is applicable for the validation of OCSP responses.
- http://uri.etsi.org/19322/sign_data/validate_data/validate_timestamps shall be used to indicate that the evaluation is applicable for the validation of timestamps.

NOTE 3: The present document defines URIs which are not used as pointers to a specific location but are used as unique identifiers.

4.2.9.3 Recommendation

The *recommendation* element shall be used to indicate that a mechanism and its parameters are either Recommended (R) or Legacy (L), as defined in ETSI TS 119 312 [i.2], clause 3.1.

Omitting this element shall be equivalent to a recommended mechanism when the end date is absent or lies in the future.

4.2.10 Parameter

The semantic of the *parameter* element shall be as defined in IETF RFC 5698 [1], clause 3.10.

4.2.11 Validity

The semantic of the *validity* element shall be as defined in IETF RFC 5698 [1], clause 3.11.

4.2.12 Information

The semantic of the *information* element shall be as defined in IETF RFC 5698 [1], clause 3.12.

4.2.13 Signature

The *signature* element shall be as defined in IETF RFC 5698 [1], clause 3.13.

5 Machine-readable cryptographic algorithms, and cipher suites catalogues

Machine-readable cryptographic algorithms, and cipher suites catalogues may be defined in different formats.

Two formats are specified in the annexes A (XML [i.4]) and B (JSON [i.5]). Additional formats may be defined in a future version of the present document.

Machine-readable cryptographic algorithms, and cipher suites catalogues should be published in all defined formats, i.e. in XML and JSON format until further additions.

6 Definition of Parameters

For interoperability reasons the recommendation of parameters names for RSA and DSA of IETF RFC 5698 [1], clause 5 should be followed.

7 Processing

The processing shall be as defined in IETF RFC 5698 [1], clause 6.

8 Security Considerations

The security considerations shall be as defined in IETF RFC 5698 [1], clause 7.

Annex A (normative): XML Policy Schema

A.1 SecuritySuitabilityPolicy

The `SecuritySuitabilityPolicy` element shall be as defined in IETF RFC 5698 [1], clause 3.1.

The `id` attribute shall be included when the catalogue is signed.

A.2 PolicyName

The `PolicyName` element shall be as defined in IETF RFC 5698 [1], clause 3.2.

A.3 Publisher

The `Publisher` element shall be as defined in IETF RFC 5698 [1], clause 3.3.

A.4 Policy-issue-date

The `Policy-issue-date` element shall be as defined in IETF RFC 5698 [1], clause 3.4.

A.5 NextUpdate

The `NextUpdate` element shall be as defined in IETF RFC 5698 [1], clause 3.5.

A.6 Usage

NOTE: This element is defined as part of the `SecuritySuitabilityPolicy` element (see clause A.1).

A.7 Algorithm

The `Algorithm` element shall be as defined in IETF RFC 5698 [1], clause 3.7.

A.8 AlgorithmIdentifier

The `AlgorithmIdentifier` shall be as defined in IETF RFC 5698 [1], clause 3.8.

A.9 Evaluation

A.9.1 MoreDetails

NOTE: Instead of the `any` element of the `Evaluation` element of IETF RFC 5698 [1], clause 3.9 the `MoreDetails` element of `ExtentionType` is used for XML instances of the present schema.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema elementFormDefault="qualified" targetNamespace="http://uri.etsi.org/19322/v1.1.1#"
xmlns="http://uri.etsi.org/19322/v1.1.1#" xmlns:xs="http://www.w3.org/2001/XMLSchema">

    <xs:element name="MoreDetails" type="ExtensionType"/>

    <xs:complexType mixed="true" name="ExtensionType">
        <xs:sequence>
         <xs:element name="AlgorithmUsage" type="xs:anyURI" minOccurs="0" maxOccurs="unbounded"/>
         <xs:element name="Recommendation" minOccurs="0" maxOccurs="1">
            <xs:simpleType>
               <xs:restriction base="xs:string">
                  <xs:enumeration value="R"/>
                  <xs:enumeration value="L"/>
               </xs:restriction>
            </xs:simpleType>
            </xs:element>
            <xs:sequence maxOccurs="unbounded" minOccurs="0">
                <xs:any namespace="##other" processContents="lax"/>
            </xs:sequence>
        </xs:sequence>
        <xs:anyAttribute namespace="##any"/>
    </xs:complexType>
</xs:schema>
```

A.9.2 AlgorithmUsage

NOTE: This element is defined as part of the `MoreDetails` element (see clause A.9.1).

A.9.3 Recommendation

NOTE: This element is defined as part of the `MoreDetails` element (see clause A.9.1).

A.10 Parameter

The `Parameter` element shall be as defined in IETF RFC 5698 [1], clause 3.10.

A.11 Validity

The `Validity` element shall be as defined in IETF RFC 5698 [1], clause 3.11.

A.12 Information

The `Information` element shall be as defined in IETF RFC 5698 [1], clause 3.12.

A.13 Signature

The `Signature` element shall be as defined in IETF RFC 5698 [1], clause 3.13.

XAdES [i.10] should be used to sign XML catalogue instances.

A.14 XML Schema file location for namespace http://uri.etsi.org/19322/v1.1.1#

The file available at https://forge.etsi.org/rep/esi/x19_322_algocat_schema/raw/v1.1.1/19322algocatxmlschema.xsd ("19322algocatxmlschema.xsd") contains the definitions of elements and types defined within the namespace whose URI value is http://uri.etsi.org/19322/v1.1.1#.

Annex B (normative): JSON format

B.1 General information

NOTE: The JSON schema defined in [i.7] is used.

All suitability policy elements are entries of the array `anyOf` as indicated in clause B.2

The object `definitions` contains all type definitions of the suitability policy elements as indicated in clause B.2.

B.2 JSON schema

B.2.1 SecuritySuitabilityPolicy

```
"anyOf":[
   {
      "type": "object",
      "properties": {
      "SecuritySuitabilityPolicy": {"$ref":
                                          "#/definitions/SecuritySuitabilityPolicyType"}
      }
   },
   "additionalProperties": false
]

"definitions": {
      "SecuritySuitabilityPolicyType": {
          "type": "object",
          "required": [
              "PolicyName",
              "Publisher",
              "PolicyIssueDate",
              "Algorithm"
          ],
          "properties": {
              "PolicyName": {"$ref": "#/definitions/PolicyNameType"},
              "Publisher": {"$ref": "#/definitions/PublisherType"},
              "PolicyIssueDate": {
                       "type": "string",
                       "format": "date-time"
              },
              "NextUpdate": {
                       "type": "string",
                       "format": "date-time"
              },
              "Usage": {"type": "string"},
              "Algorithm": {
                       "type": "array",
                       "items": {"$ref": "#/definitions/AlgorithmType"},
                       "minItems": 1
              },
              "Signature": {"$ref": "#/definitions/SignatureType"},
              "version": {
                       "type": "string",
                       "default": "1"
              },
              "lang": {
                       "type": "string",
                       "default": "en"
              }
          }
     },
      "additionalProperties": false
}
```

B.2.2 PolicyName

```
{
   "type": "object",
   "properties": {
        "PolicyName": {"$ref": "#/definitions/PolicyNameType"}
   },
   "additionalProperties": false
}

"PolicyNameType": {
   "type": "object",
   "required": ["Name"],
   "properties": {
      "Name": {"type": "string"},
      "ObjectIdentifier": {"type": "string"},
      "URI": {
         "type": "string",
         "format": "uri"
      }
   },
   "additionalProperties": false
}
```

B.2.3 Publisher

```
{
   "type": "object",
   "properties": {
      "Publisher": {"$ref": "#/definitions/PublisherType"}
   }
}

"PublisherType": {
   "type": "object",
   "required": ["Name"],
   "properties": {
      "Name": {"type": "string"},
      "Address": {"type": "string"},
      "URI": {
         "type": "string",
         "format": "uri"
      }
   },
   "additionalProperties": false
}
```

B.2.4 PolicyIssueDate

NOTE: This element is defined as part of the `SecuritySuitabilityPolicy` element (see clause B.2.1).

B.2.5 NextUpdate

NOTE: This element is defined as part of the `SecuritySuitabilityPolicy` element (see clause B.2.1).

B.2.6 Usage

NOTE: This element is defined as part of the `SecuritySuitabilityPolicy` element (see clause B.2.1).

B.2.7 Algorithm

```
{
   "type": "object",
   "properties": {
      "Algorithm": {"$ref": "#/definitions/AlgorithmType"}
   },
    "additionalProperties": false
}
```

```
"AlgorithmType": {
    "type": "object",
    "required": [
        "AlgorithmIdentifier",
        "Evaluation"
    ],
    "properties": {
        "AlgorithmIdentifier": {"$ref": "#/definitions/AlgorithmIdentifierType"},
        "Evaluation": {
            "type": "array",
            "items": {"$ref": "#/definitions/EvaluationType"},
            "minItems": 1
        },
        "Information": {"$ref": "#/definitions/InformationType"}
    },
     "additionalProperties": false
}
```

B.2.8 AlgorithmIdentifier

```
{
    "type": "object",
    "properties": {
        "AlgorithmIdentifier": {"$ref": "#/definitions/AlgorithmIdentifierType"}
    },
     "additionalProperties": false
   }


"AlgorithmIdentifierType": {
    "type": "object",
    "required": [
        "Name",
        "ObjectIdentifier"
    ],
    "properties": {
       "Name": {"type": "string"},
        "ObjectIdentifier": {
           "type": "array",
            "items": {"type": "string"},
            "minItems": 1
        },
        "URI": {
           "type": "array",
            "items": {
                "type": "string",
                "format": "uri"
            },
            "minItems": 0
        },
         "additionalProperties": false
       }
   }
```

B.2.9 Evaluation

B.2.9.1 General description

```
{
    "type": "object",
    "properties": {
        "Evaluation": {"$ref": "#/definitions/EvaluationType"}
    },
     "additionalProperties": false
   }


"EvaluationType": {
    "type": "object",
    "required": ["Validity"],
    "properties": {
        "Parameter": {
            "type": "array",
            "items": {"$ref": "#/definitions/ParameterType"},
            "minItems": 0
```

```
        },
         "Validity": {"$ref": "#/definitions/ValidityType"},
           "AlgorithmUsage": {
                "type": "string",
                "format": "uri"
           },
           "Recommendation": {
                "type": "string",
                "pattern": "L|R"
           },
           "Any": {"type": "object"}
    },
    "additionalProperties": true
}
```

B.2.9.2 AlgorithmUsage

NOTE: This element is defined as part of the `Evaluation` element (see clause B.2.9.1).

B.2.9.3 Recommendation

NOTE: This element is defined as part of the `Evaluation` element (see clause B.2.9.1).

B.2.10 Parameter

```
{
    "type": "object",
    "properties": {
        "Parameter": {"$ref": "#/definitions/ParameterType"}
    },
     "additionalProperties": false
}


"ParameterType": {
    "type": "object",
    "required": ["name"],
    "properties": {
       "Min": {"type": "integer"},
       "Max": {"type": "integer"},
       "Any": {"type": "object"},
       "name": {"type": "string"}
    },
     "additionalProperties": true
}
```

B.2.11 Validity

```
{
    "type": "object",
    "properties": {
        "Validity": {"$ref": "#/definitions/ValidityType"}
    },
     "additionalProperties": false
}


"ValidityType": {
    "type": "object",
    "properties": {
        "Start": {
            "type": "string",
            "format": "date"
        },
        "End": {
            "type": "string",
            "format": "date"
        }
    },
    "additionalProperties": false
}
```

B.2.12 Information

```
{
    "type": "object",
    "properties": {
        "Information": {"$ref": "#/definitions/InformationType"}
    }
}

"InformationType": {
    "type": "object",
    "required": ["Text"],
    "properties": {
        "Text": {
            "type": "array",
            "items": {"type": "string"},
            "minItems": 1
        }
    },
     "additionalProperties": false
}
```

B.2.13 Signature

JAdES [i.9] should be used to sign JSON catalogue instances.

B.3 JSON Schema file location

The file available at https://forge.etsi.org/rep/esi/x19_322_algocat_schema/raw/v1.1.1/19322algocatjsonschema.json ("19322cryptoalgojsonschema.json") contains the definitions of elements and types defined within the JSON schema associated to the present document.

History

Document history		
V1.1.1	November 2022	Publication