IEC 62351-11

Edition 1.0 2016-09

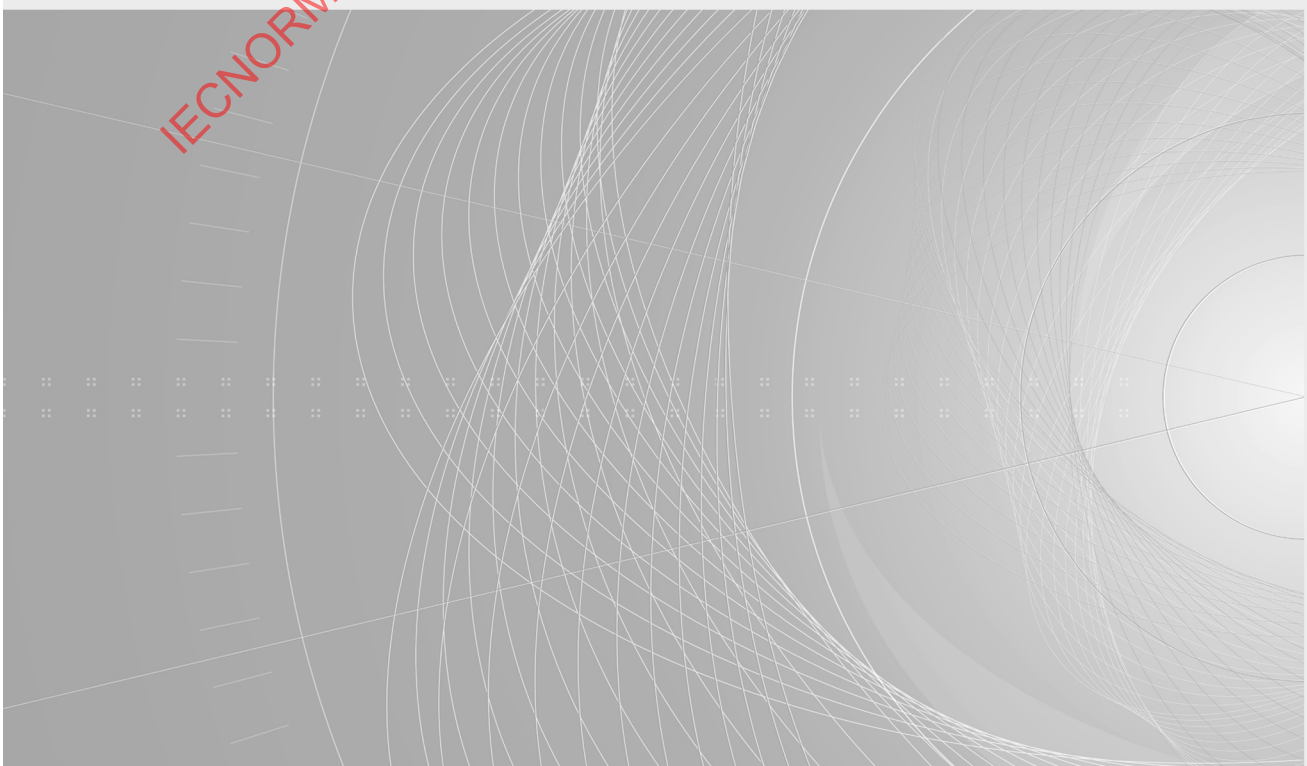
INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Power systems management and associated information exchange – Data and communications security – Part 11: Security for XML documents

Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 11: Sécurité des documents XML



IEC 62351-11:2016-09(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

IEC 62351-11

Edition 1.0 2016-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Power systems management and associated information exchange – Data and communications security – Part 11: Security for XML documents

Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 11: Sécurité des documents XML

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-3636-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 11: Security for XML documents

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62351-11 has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this standard is based on the following documents:

FDIS	Report on voting
57/1753/FDIS	57/1774/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security,* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 11: Security for XML documents

1 Scope

This part of IEC 62351 specifies schema, procedures, and algorithms for securing XML documents that are used within the scope of the IEC as well as documents in other domains (e.g. IEEE, proprietary, etc.). This part is intended to be referenced by standards if secure exchanges are required, unless there is an agreement between parties in order to use other recognized secure exchange mechanisms.

This part of IEC 62351 utilizes well-known W3C standards for XML document security and provides profiling of these standards and additional extensions. The IEC 62351-11 extensions provide the capability to provide:

- Header: the header contains information relevant to the creation of the secured document such as the Date and Time when IEC 62351-11 was created.
- A choice of encapsulating the original XML document in an encrypted (Encrypted) or non-encrypted (nonEncrypted) format. If encryption is chosen, there is a mechanism provided to express the information required to actually perform encryption in an interoperable manner (EncryptionInfo).
- AccessControl: a mechanism to express access control information regarding information contained in the original XML document.
- Body: is used to contain the original XML document that is being encapsulated.
- Signature: a signature that can be used for the purposes of authentication and tamper detection.

The general structure is shown in Figure 1.

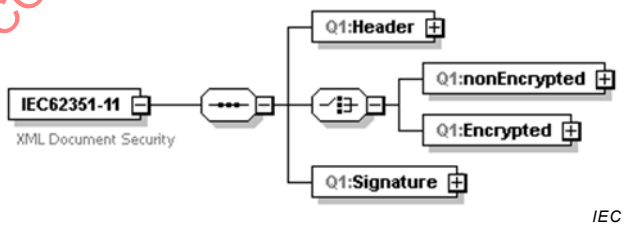


Figure 1 – Overview of IEC 62351-11 structure

For the measures described in this document to take effect, they must be accepted and referenced by the specifications themselves. This document is written to enable that process.

The subsequent audience for this part of IEC 62351 is intended to be the developers of products that implement these specifications.

Portions of this part of IEC 62351 may also be of use to managers and executives in order to understand the purpose and requirements of the work.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC TS 62351-8, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*

IEC TS 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

Recommended Canonical XML1.0 with comments, W3C,
http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments

Required Canonical XML 1.0, Omits comments, W3C,
http://www.w3.org/TR/2001/REC-xml-c14n-20010315

RFC 6931, *Additional XML Security Uniform Resource Identifiers (URIs)*

XML Encryption Syntax and Processing Version 1.1 April 11, 2013,
http://www.w3.org/TR/xmlenc-core1/

XML Signature Syntax and Processing W3C Recommendation 10 June 2008,
http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 62351-2 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
nonce
random or pseudo-random value used within an authentication system

[SOURCE: IEEE Std 1455-1999, IEEE Standard for Message Sets for Vehicle/Roadside Communications]

3.2
IANA
Internet Assigned Numbers Authority

Note 1 to entry: IANA is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources.

[SOURCE: http://www.iana.org]

4 Security issues addressed by this document

4.1 General

Within the industry and the IEC, XML document exchange is becoming more prevalent. Within the scope of the IEC, exchanges of XML documents are used for IEC 61970 as well as IEC 61850. Within other standards, such as IEEE 1815 and IEEE C37.111 (COMTRADE), XML is also utilized. For these standards and other XML-based documentss, the information contained in thedocument may:

1) be sensitive to inadvertant or malicious modifications of its contents that could result in mis-operation/misinterpretation if the exchanged information is used (e.g. a tamper security vulnerability);
2) contain confidential or private data;
3) contain subsets of information that may be considered sensitive by the document creation entity.

This part of IEC 62351 proposes to standardize mechanisms to protect the document contents from tampering/disclosure when the document is being exchanged (e.g. in transit). Additionally, this part of IEC 62351 proposes to standardize a mechanism to aid in the protection of the information when in transition (e.g. entity A trusts entity B; B trusts A and C, and B needs to exchange information with C. but A does not know of or trust C).

Although this document is intended to secure XML documents used within the scope of the IEC, the mechanism/methodologies specified within this document can be applied to any XML document.

4.2 Security threats countered

See IEC TS 62351-1 for a discussion of security threats and attack methods.

If encryption is not employed, then the specific threats countered in this part of IEC 62351 include:

- unauthorized modification (tampering) of information through XML document level authentication.

If encryption is employed, then the specific threats countered in this part of IEC 62351 include:

- unauthorized access to information through XML document level authentication and encryption of the documents;
- unauthorized modification (tampering) of information through XML document level authentication regardless if encryption is utilized.

4.3 Attack methods countered

The following security attack methods are intended to be countered through the appropriate implementation of the specification/recommendations found within this document:

- man-in-the-middle: this threat will be countered through the use of a Message Authentication Code (e.g. Signature) mechanism specified within this document;
- message tampering: These threats will be countered through the algorithm used to create the authentication mechanism as specified within this document.

5 XML Documents

In order to provide adequate security, there needs to be an understanding of the environment of use that this specification is addressing:

- Documents at rest: When XML documents are stored (e.g. at rest), tamper detection is a minimum requirement. If the document contains sensitive information, then the confidentiality of that information needs to be protected through the use of authenticated encryption. In order to accomplish both objectives, this means that the un-encrypted document needs a signature and the encrypted document also needs its own signature/integrity protection. The protection of XML documents at rest is out-of-scope of this standard and should be implemented through local means.
- Documents in transit: The protection of documents in transit requires tamper detection and authentication as minimum requirements. If the document contains sensitive information, then the confidentiality of that information needs to be protected through the use of authenticated encryption. In order to accomplish both objectives, this means that the un-encrypted document needs a signature and the encrypted document also needs its own signature/integrity protection.
- Documents in transition: In the domain of the IEC, the recipients of XML documents typically decrypt and parse the information from those documents into a database. The information from the database can then be re-exported to a third actor, in any form (including another XML document). If sensitive or confidential information was provided in the initial document, there is no technological mechanism to prevent the application from exporting that information and defining access controls.

  A real example use case is the transfer of power system topology information through the use of IEC 61970-552.

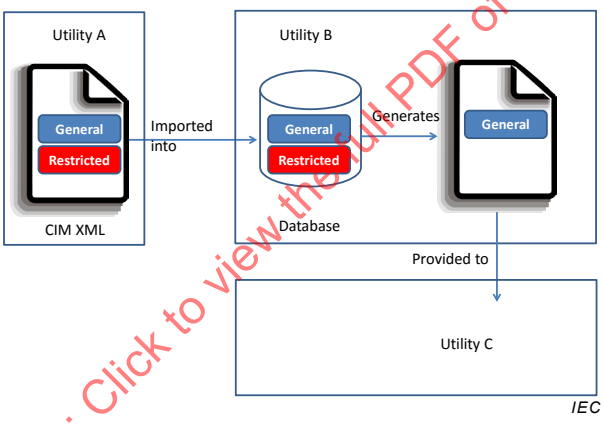


Figure 2 – Data in transition example

Figure 2 illustrates this potential problem with Data in Transition. Utility[1] A provides a CIM XML document to Utility B. The document contains the information that must be exchanged between Utility A and Utility B, based upon the trust/agreements between those utilities. Utility B imports the information into its database (e.g. EMS). A separate exchange of information then needs to occur between Utility B and Utility C. Utility A may have no knowledge that such a transfer may be needed and that some of the "restricted" information may be at risk for export by Utility B. The goal of the approach to handling data-in-transition recommended here is to allow Utility A to classify and label specific document content as being sensitive or confidential and therefore not to be re-exported to partners of Utility B.

Note that document signing, as described herein, is not sufficient for this purpose, as Utility B has a legitimate use for the restricted content and accordingly has the ability to decrypt it for import into an application database. Therefore, another solution needs to be provided – namely, the contractual access-control mechanism described in 6.3.3.

---

1 Actors in these scenarios are not confined to utilities, but may be RTOs, market exchanges/portals, consumer-program facilitators, etc.

Within the context of the IEC, there are at least two well-known XML document types that required protection: CIM XML and SCL documents. These documents have well formed XSDs/formats. As such, the mechanism specified in this standard are intended to allow the documents formats to be preserved. Therefore, encapsulation of the original documents is the design approach.

6 XML document encapsulation

6.1 General

The concept of security encapsulation for XML documents is shown in Figure 3.

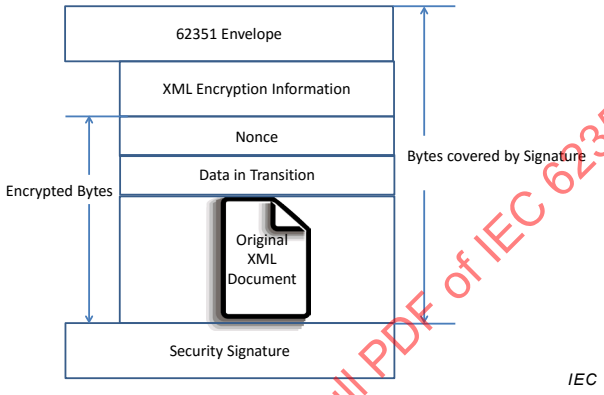


Figure 3 – Secure encapsulation for XML documents

The concept is to utilize previously standardized XML security techniques to provide a security header, signature, and document encryption capability. Within the “secure” document is the original XML document and extensions specified by this standard. The IEC 62351-11 extensions provide the capability to provide:

- IEC 62351 Envelope (Header): the header contains information relevant to the encapsulation such as the Date and Time of the encapsulation (e.g. document creation).
- XML Encryption Information: a choice of encapsulating the original XML document ACL in an encrypted (Encrypted) or non-encrypted (nonEncrypted) format. If encryption is chosen, there is a mechanism provided to express the information required to actually perform encryption in an interoperable manner (EncryptionInfo).
- Data in Transition: a mechanism to express access control information regarding information contained in the original XML document.
- Original XML Document (Body): is used to contain the original XML document that is being encapsulated.
- Signature: a signature that can be used for the purposes of authentication and tamper detection.

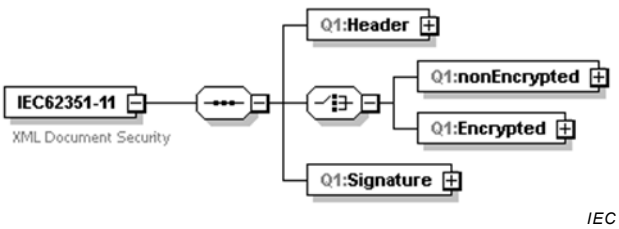


Figure 4 – General IEC 62351-11 XSD layout

Figure 4 depicts the general XSD structure of an IEC 62351-11 document. The definitions can be found in Table 1.

Table 1 – Definitions of general structure for an IEC 62351-11 document

Element	Optional (O)/ Mandatory (M)/ Conditional (C)	XSD Type	Description
Header	M	HeaderType (see 6.2)	The Header contains information regarding the creation of the IEC 62351-11 document and contact information should questions or issues arise with the document.
nonEncrypted	C	Information (see 6.3)	Provides access control and wrapping of the original document in a non-encrypted (e.g. original document contents can still be viewed). This choice should be utilized by a user should confidentiality of the information not be of concern or if confidentiality is being provided through an external mechanism. Either the nonEncrypted or Encrypted XSD element shall be present.
Encrypted	C	EncryptedType (see 6.4)	Provides encryption to the access control and wrapping of the original document. This choice should be utilized by the user should confidentiality of information be desired and is not provided through external mechanisms. Either the nonEncrypted or Encrypted XSD element shall be present.
Signature	M	SignatureType	Is a production of the W3C XML Signature information.

Any implementation claiming conformance to this standard shall implement all mandatory elements.

6.2 HeaderType

Figure 5 shows the XSD structure of the HeaderType.

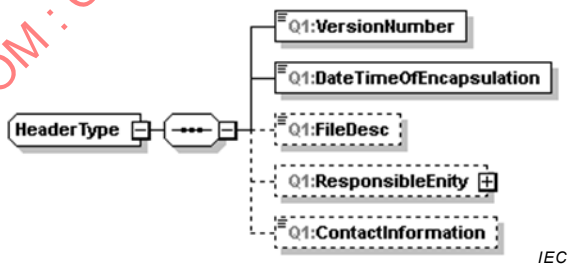


Figure 5 – XSD ComplexType definition of HeaderType

The HeaderType is a XSD complex type that consists of a sequence of XSD elements as described in Table 2.

Table 2 – Definition of HeaderType Element

Element	Optional (O)/ Mandatory (M)/ Conditional(C)	XSD Type	Description
VersionNumber	M	xs:float	Is the version number of the IEC 62351-11 standard being implemented. The floating point number shall specify <majorVersion>.<minorVersion>. The value shall be “1.0”
DateTimeOfEncapsulation	M	xs:DateTime	The value specifies the date and time at which the original document was wrapped.
FileDesc	O	xs:string	A user supplied description of the document and its contents. If the Body (e.g. original document) is encrypted or hexascii encoded, this element is mandatory since user will not be able to determine the contents of the document should questions arise. All encapsulated documents shall share this description.
ResponsibleEntity	O	NameSeqType (see 6.6.2)	A user supplied Entity name that can be used by a user of the document to know who to contact should there be issues or questions regarding the document.
ContactInformation	O	xs:string	Is a user supplied string that may contain phone or email information that could be used by a document user should problems or questions occur.

6.3 Information

6.3.1 General

Figure 6 shows the structure of the information type.

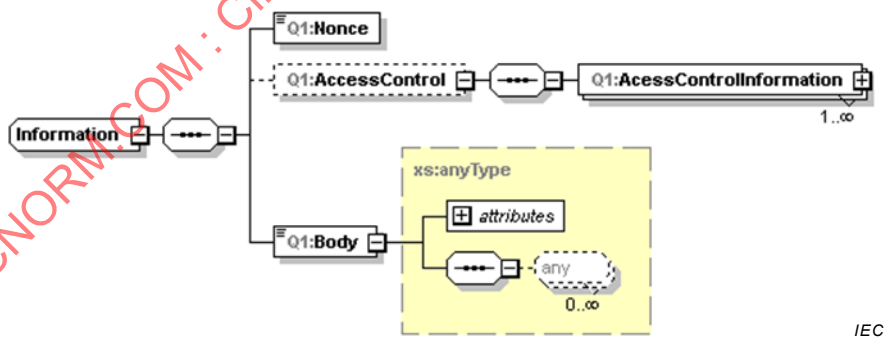


Figure 6 – XSD ComplexType definition of information

. It is an XSD Sequence of the following sub-elements: Nonce; AccessControl; and Body. The definition of these elements, and their types, can be found in Table 3.

Table 3 – Definition of information element

Element	Optional (O)/ Mandatory (M)/ Conditional(C)	XSD Type	Description
Nonce	M	xs:string	See 6.3.2.
AccessControl	O	AccessControlType See 6.3.3	This element allows for access control information to be expressed. The default value for AccessControl is Allow All if there is no AccessControl element present.
Body	M	xs:anyType	The element provides the capability to encapsulate one or more documents within the same IEC 62351-11 document.

6.3.2 Nonce

This element represents a security related attribute that ensures that if the same Body is using the same credentials, that at least the signature will be different. In many situations, a cryptographic nonce should be cryptographically random. However, for the purposes of this standard, randomness is not a requirement but some uniqueness is desired.

In order to prevent the same nonce value requiring cryptographic generation, it is suggested that an acceptable nonce value could contain a DateTime value and a UUID. The nonce must not be reused for any key and should be random.

6.3.3 AccessControl

6.3.3.1 General

AccessControl allows zero(0), because AccessControl is optional, or more sets of access information to be specified for the wrapped document(s). The XSD type for AccessControl is shown in Figure 7.

Figure 7 – XSD Complex Type Definition of AccessControl

The AccessControl element is an XSD Sequence that consists of one or more AccessControlInformation(s). Each AccessControlInformation is of an XSD type of AccessControlType whose structure is shown in Figure 8.

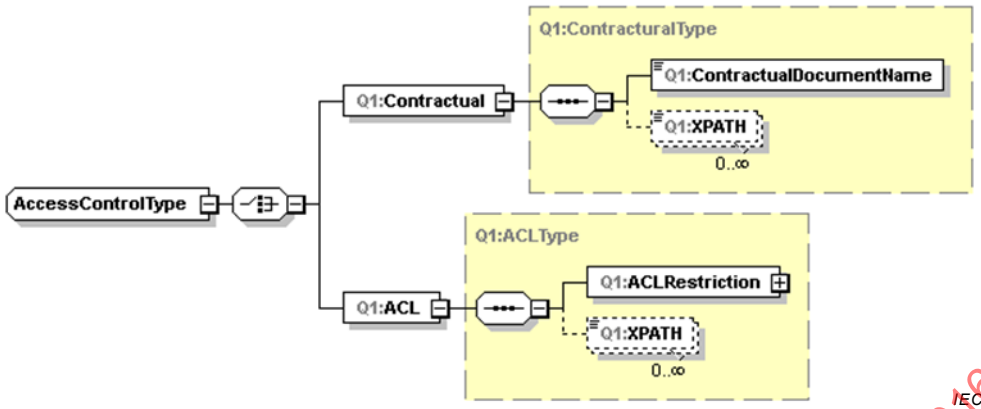


Figure 8 – XSD Complex Type definition of AccessControlType

AccessControlType allows a choice between a Contractual (e.g. legally binding document) restriction and the definition of the equivalent of an access control list (ACL). Each choice allows the governance of access (e.g. Contract or ACLRestriction) to be applied to one or more sets of information within the wrapped original document through the use of one or more XPATH statements.

The Contractual choice is a XSD Sequence that consists of the elements that are defined in Table 4.

Table 4 – Definition of Contractual and ACL Element

Element	Optional (O)/ Mandatory (M)/ Conditional(C)	XSD Type	Description
ContractualDocumentName	M	xs:normalizedString	A user supplied reference to a legal contract that contains information relevant to the allowed access rights/privileges regarding the information specified in the XPATH statements.
ACLRestriction	M	ACLRestriction Type (see 6.3.3.2)	A complex specification of access rights that allow the specification of allowance or denial of specific types of access based upon specific roles. The use of ACLRestriction allows the user to specify the equivalent of White or Black listing.
XPATH	O	xs:normalizedString (see 6.3.3.7)	This element contains the XPATH value that expresses the information contained in Body for which guidance is being given. If there is no XPATH defined, the entire Body is assumed.

6.3.3.2 AccessRestrictionType

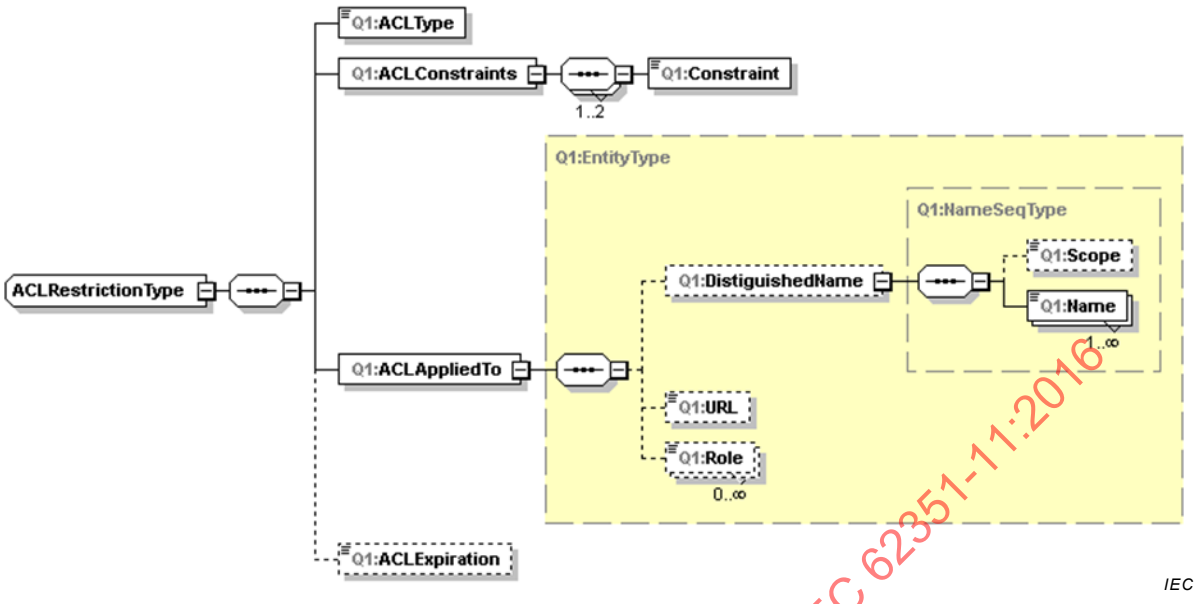


Figure 9 – XSD Complex Type Definition of ACLRestrictionType

Figure 9 shows the structure of the ACLRestrictionType. It is an XSD Complex Type that is a sequence of the XSD elements defined in Table 5.

Table 5 – Definition of ACLRestrictionType Element

Element	Optional (O)/ Mandatory (M)/ Conditional(C)	XSD Type	Description
ACLType	M	xs:string (see 6.3.3.3)	Specifies if the access restriction is Allow or Deny. As such, the allowed enumerated values for ACLType are: Allow and Deny.
ACLConstraints	M	Complex (see 6.3.3.4)	Allows a user to specify a sequence of rights that are allowed or denied. This capability is provided through a sequence of Constraint elements.
ACLAppliedTo	M	EntityType	Allows the user to express the type of definition used to specify what entity the ACL applies to.
ACLExpiration	O	xs:dateTime	Specifies the date and time at which access control is no longer required. If the value is not present, the ACL does not expire.

Since there may be multiple ACLs within a single IEC 62351-11 document, an ACLType value of Deny, shall have precedence for situations where there are common Constraint values and the same or overlapping ACLAppliedTo values.

6.3.3.3 ACLType

The ACLType is an xs:string whose values are restricted through enumeration. The definitions of the allowed enumerated values, and the order of enumeration, is shown in Table 6.

Table 6 – Definition of Enumerated Values for ACLType

Enumeration Value	Definition
Allow	Specifies that the ACLRestrictionType is being used to create a white list and that the specified ACLContstraints are allowed privileges for the specified ACLAppliedTo.
Deny	Specifies that the ACLRestrictionType is being used to create a black list and that the specified ACLContstraints are disallowed privileges for the specified ACLAppliedTo.

6.3.3.4 ACLConstraints and Constraint

ACLConstraints are a sequence of Constraint values as shown in Table 7.

The Constraint element is an xs:string whose values are restricted through enumeration. The use of the Constraint(s) is governed by the ACLType.

Unlike file privileges which are enforceable, the Constraint values represent guidance how Data in Transition should be handled. The values are shown in Table 7.

Table 7 – Definition of Enumerated Values for Constraint

Enumeration Value	Definition
All	Specifies that all privileges of Read, Write, and List are specified. Read privilege, if allowed, indicates the ability to provide the value/element to another entity. Write privilege, if allowed, indicates the ability for an entity to change the value/element. List privilege, if allowed, indicates the ability for an entity to determine if the value/element exists. Therefore, the All value is mutually exclusive from Read, Write, List, and Forward. If All is specified within a specific instance of ACLConstraints, no other enumerated values shall be used within that sequence.
TransmitValue	The permission specifies the ability to convey the value of the information, specified by XPATH, to another entity. The specification of Read implies List. As an example, a utility would be able to supply the information to another utility if Allow was the ACLType. This is the equivalent of Read and List.
Write	The permission specifies the ability to allow modification the value of the information specified by XPATH

6.3.3.5 EntityType

Figure 10 shows the structure of the EntityType.

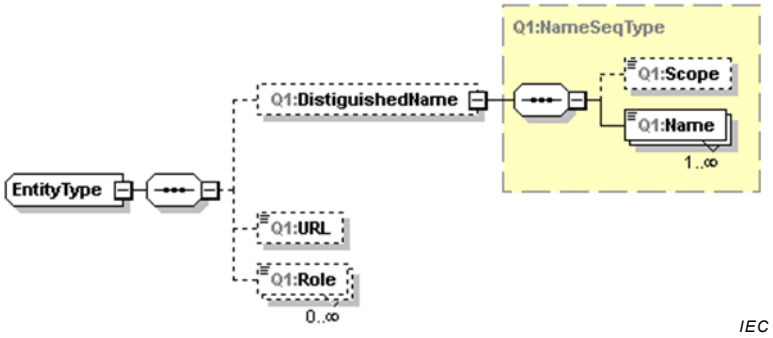


Figure 10 – XSD Complex Type definition of EntityType

It is a XSD sequence that allows a combination of entity specifications to be combined in order to determine entity to which the ACL applies. The XSD elements defined in EntityType are defined in Table 8.

Table 8 – Definition of EntityType Element

Element	Optional (O)/ Mandatory (M)/ Conditional(C)	XSD Type	Description
DistinguishedName	M	NameSeqType (see 6.6.2)	User supplied name that can be used by a user of the document to know who (e.g. organization or person) to contact and to whom the ACL should be applied.
URL	M	xs:anyURI	Allows the specification of a web address to which the ACL should be applied. In many cases, an organization may be referred to via URL or a particular FTP site may need to be restricted.
Role	O	xs:string (see 6.3.3.6)	Is a string value that specifies the type of security/work role grouping to which the ACL should be applied.

The combination of the values can be used to constrain access, As an example, the combination of DistinguishedName and Role could be used to constrain an ACL to a role within a given department of a company.

6.3.3.6 Role

The Role is an xs:string whose values are restricted through enumeration. The definitions of the allowed string values are defined per IEC TS 62351-8.

6.3.3.7 XPATH

This element contains the XPATH value that expresses the information contained in Body for which guidance is being given. If no XPATH is specified, for a specified constraint, the constraint shall apply to the entire Body element.

As an example:

```
<?xml version="1.0" encoding="UTF-8"?>
<Q1:IEC62351-11 xmlns:n1="http://www.altova.com/samplexml/other-namespace" xmlns:Q1="http://www.iec.ch/2014/01/62351-11#"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:enc="http://www.w3.org/2001/04/xmlenc#"  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://www.iec.ch/2014/01/62351-11# file:///C:/Users/root/Desktop/IEC62351-11/IEC62351-11.xsd">
        <Q1:Header>
                <Q1:DateTimeOfEncapsulation>2014-04-14T21:32:52</Q1:DateTimeOfEncapsulation>
                <Q1:Filedesc>Example IEC 62351-11 non-encrypted file</Q1:Filedesc>
        </Q1:Header>
        <Q1:nonEncrypted>
                <Q1:Nonce>85343410947jgfa8312b!</Q1:Nonce>
                <Q1:AccessControl>
                  <Q1:AcessControlInformation>
                    <Q1:ACL>
                          <Q1:ACLRestriction>
                                  <Q1:ACLType>Deny</Q1:ACLType>
                                  <Q1:ACLConstraints>
                                                  <Q1:Constraint>All</Q1:Constraint>
                                  </Q1:ACLConstraints>
                                  <Q1:ACLAppliedTo>
                                          <Q1:Role>Any</Q1:Role>
                                  </Q1:ACLAppliedTo>
                          </Q1:ACLRestriction>
                          <Q1:XPATH>//cim:PowerTransformer[@rdf:ID='_T_Z0568311_Z0568422_1_24574']</Q1:XPATH>
                    </Q1:ACL>
                  </Q1:AcessControlInformation>
                </Q1:AccessControl>
                <Q1:Body>
                        <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"    xmlns:cim="http://iec.ch/TC57/2009/CIM-schema-cim14#">
                        <cim:PowerTransformer rdf:ID="_T_Z0568311_Z0568422_1_24574">
                          <cim:IdentifiedObject.name>UNKNOWN     </cim:IdentifiedObject.name>
                          <cim:Equipment.MemberOf_EquipmentContainer
                                  rdf:resource="#_S_Z0568311Z0568422"/>
                        </cim:PowerTransformer>
                        <cim:BaseVoltage rdf:ID="_BS_9">
                          <cim:BaseVoltage.nominalVoltage>500</cim:BaseVoltage.nominalVoltage>
                                  <cim:BaseVoltage.isDC>false</cim:BaseVoltage.isDC>
                          <cim:IdentifiedObject.name>500</cim:IdentifiedObject.name>
                        </cim:BaseVoltage>
                        <cim:SubGeographicalRegion rdf:ID="_Z_X">
```

```
                    <cim:IdentifiedObject.name>XX</cim:IdentifiedObject.name>
                    <cim:SubGeographicalRegion.Region rdf:resource="#_H_XX"/>
                  </cim:SubGeographicalRegion>
            <cim:ControlArea rdf:ID="_CA_X">
              <cim:IdentifiedObject.name>ControlArea_XX</cim:IdentifiedObject.name>
              <cim:ControlArea.netInterchange>0</cim:ControlArea.netInterchange>
              <cim:ControlArea.pTolerance>0</cim:ControlArea.pTolerance>
            </cim:ControlArea>
            <cim:Substation rdf:ID="_S_1000085110000721">
              <cim:IdentifiedObject.name>SUBSTATION_2</cim:IdentifiedObject.name>
              <cim:Substation.Region rdf:resource="#_Z_1"/>
            </cim:Substation>
                    </rdf:RDF>
            </Q1:Body>
      </Q1:nonEncrypted>
      <Q1:Signature>
            <ds:SignedInfo>
                  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-
                        c14n-20010315#WithComments"/>
                  <ds:SignatureMethod Algorithm="2001/04/xmldsig-more#hmac-sha256">
                        <ds:HMACOutputLength>128</ds:HMACOutputLength>
                  </ds:SignatureMethod>
                  <ds:Reference>
                  <ds:DigestMethod Algorithm="2001/04/xmldsig-more#sha384"></ds:DigestMethod>
                  <DigestValue>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK</DigestValue>
                  </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK</ds:SignatureValue>
            <ds:KeyInfo>
                  <ds:X509Data>
                  <ds:X509IssuerSerial>
                        <ds:X509SerialNumber></ds:X509SerialNumber>
                  </ds:X509IssuerSerial>
                  </ds:X509Data>
            </ds:KeyInfo>
      </Q1:Signature>
</Q1:IEC62351-11>
```

Figure 11 – Example of AccessControl and XPATH

Figure 11 shows three examples of AccessControl and the use of XPATH. The example shows constraints on denying access to the information regarding a specific PowerTransformer.

The XPATH value shall be a value that does not include any of the IEC 62351-11 elements. It shall be an XPATH that is valid on the encapsulated document only. This is to facilitate enforcement of the AccessControl based upon the use of XPATH by an application that understands the semantics of the original document.

As an example, for the CIM document shown in Figure 11, other XPATH strings could be used to provide AccessControl to:

- the entire document: " //*"
- all substations: "//cim:Substation"
- a substation with a name of SUBSTATION_2: "//cim:Substation/cim:IdentifiedObject.name['SUBSTATION_2']"

6.3.4 Body

This element is the encapsulating element for the actual document that is being signed/encrypted. The Body shall encapsulate an XML document that shall not contain the <?xml…> value.

As an example, if the Body contains a CIM XML instance file, the syntax of the Body element should be something similar to that shown in Figure 12:

```
<Q1:Body>
        <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
        xmlns:cim="http://iec.ch/TC57/2009/CIM-schema-cim14#">
                <cim:PowerTransformer rdf:ID="_T_Z0568311_Z0568422_1_24574">
                        <cim:IdentifiedObject.name>UNKNOWN     </cim:IdentifiedObject.name>
                        <cim:Equipment.MemberOf_EquipmentContainer
                                rdf:resource="#_S_Z0568311Z0568422"/>
                </cim:PowerTransformer>
                <cim:BaseVoltage rdf:ID="_BS_9">
                        <cim:BaseVoltage.nominalVoltage>500</cim:BaseVoltage.nominalVoltage>
                                <cim:BaseVoltage.isDC>false</cim:BaseVoltage.isDC>
                        <cim:IdentifiedObject.name>500</cim:IdentifiedObject.name>
                </cim:BaseVoltage>
                <cim:SubGeographicalRegion rdf:ID="_Z_X">
                        <cim:IdentifiedObject.name>XX</cim:IdentifiedObject.name>
                        <cim:SubGeographicalRegion.Region rdf:resource="#_H_XX"/>
                </cim:SubGeographicalRegion>
                <cim:ControlArea rdf:ID="_CA_X">
                  <cim:IdentifiedObject.name>ControlArea_XX</cim:IdentifiedObject.name>
                  <cim:ControlArea.netInterchange>0</cim:ControlArea.netInterchange>
                  <cim:ControlArea.pTolerance>0</cim:ControlArea.pTolerance>
                </cim:ControlArea>
                <cim:Substation rdf:ID="_S_1000085110000721">
                  <cim:IdentifiedObject.name>SUBSTATION_2</cim:IdentifiedObject.name>
                  <cim:Substation.Region rdf:resource="#_Z_1"/>
                </cim:Substation>
        </rdf:RDF>
</Q1:Body>
```

Figure 12 – Example of an IEC 62351-11 Body with a CIM document

6.4 Encrypted element

6.4.1 General

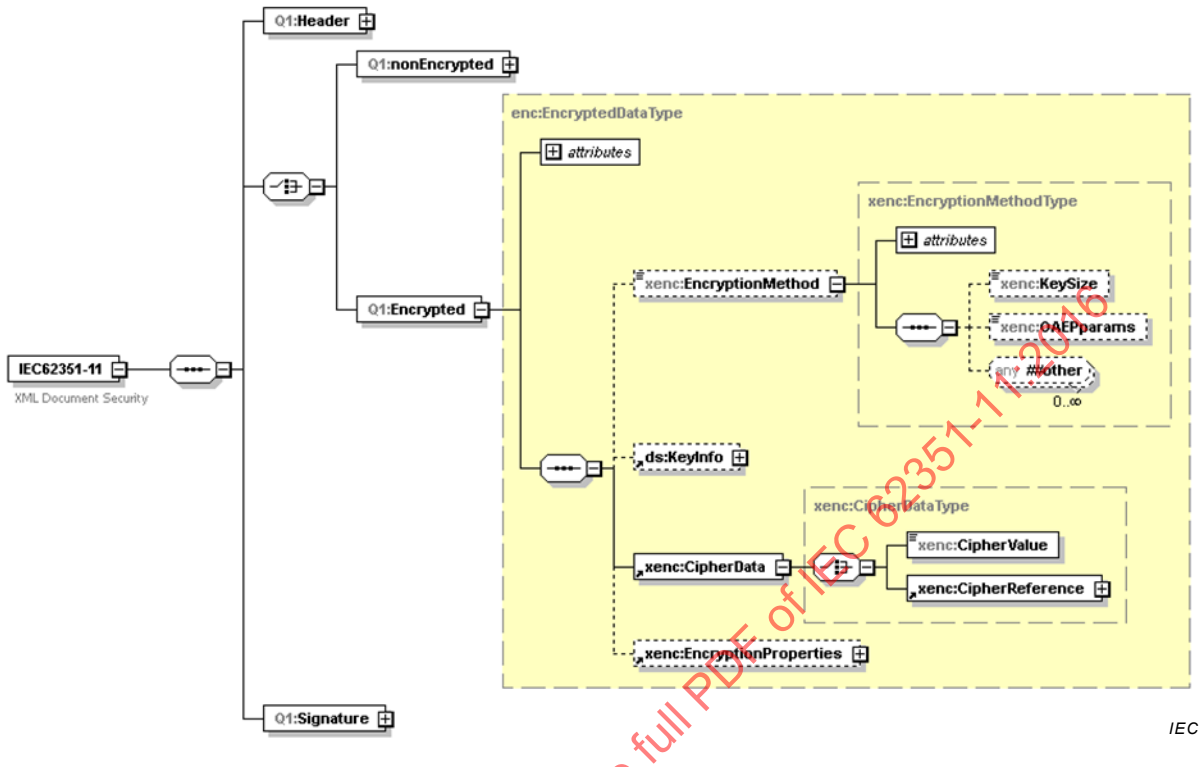


Figure 13 – Structure of the IEC 62351-11 Encrypted element

The IEC 62351-11 Encrypted element has the structure shown in Figure 13. The structure, and the EncryptedDataType are defined by the W3C specification for XML Encryption.

For use within the context of IEC 62351-11, the following constraints shall be applied to the contents of the EncryptedDataType:

- The Type attribute shall have a value of: http://www.w3.org/2001/04/xmlenc#Element.
- The MimeType attribute shall not be present.
- The Encoding attribute shall not be present.

6.4.2 EncryptionMethod

The EncryptionMethod element has the structure as specified by the W3C EncryptionMethodType which is shown in Figure 14. This element is optional within the context of W3C, but shall be mandatory for IEC 62351-11.

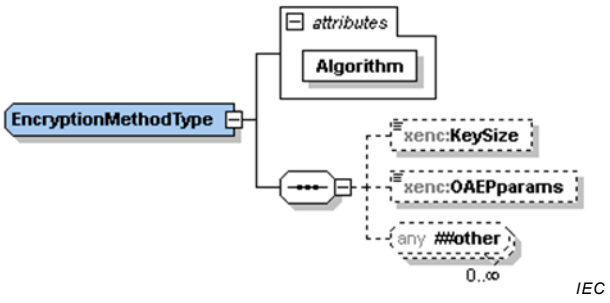


Figure 14 – Structure of EncryptionMethodType

The optional EncryptionMethod shall be present. The values shall be as specified by IANA (see Clause 8). The allowed algorithm values are:

2009/xmlenc11#aes128-gcm
2009/xmlenc11#aes192-gcm
2009/xmlenc11#aes256-gcm

The optional KeySize element shall also be present and have a non-NULL/not-empty value. *The optional support for 1024 bit key length is intended for backward compatibility. 2048 bit key length shall be supported and is the preferred key length to be used.*

The OAEPparams element is not required due to the encryption algorithms selected for use within IEC 62351-11 and therefore shall not be present.

6.4.3 CipherData

The CipherData element has the structure as specified by the W3C CipherDataType which is shown in Figure 15.

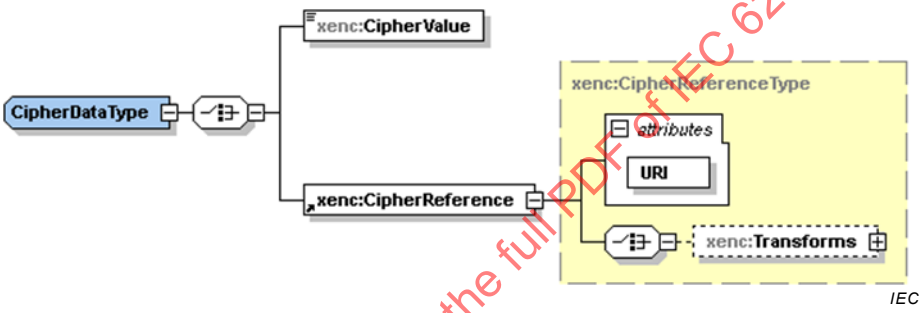


Figure 15 – Structure of CipherDataType

Within the context of IEC 62351-11, only the CipherValue shall be used.

The CipherValue shall be the value produced by encrypting the EncryptedData element. The element has the structure shown in Figure 16.

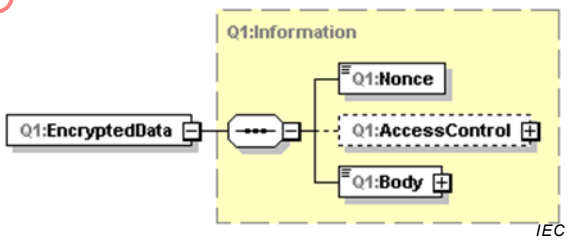


Figure 16 – EncryptedData element definition

The Information type is defined in 6.3.

6.4.4 KeyInfo

If the KeyInfo element, within the EncryptedDataType is not present, then the values of the Signature KeyInfo element shall be used for encryption/decryption.

The value constraints on the EncryptionDataType KeyInfo element are the same as for the Signature and are defined in 6.5.2.5.

6.5 SignatureType

6.5.1 General

The Signature element is a complex type of ds:SignatureType where the SignatureType is defined by W3C.

The schema to be used is defined at: http://www.w3.org/2000/09/xmldsig#. The actual XML Signature specification can be found at: http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/.

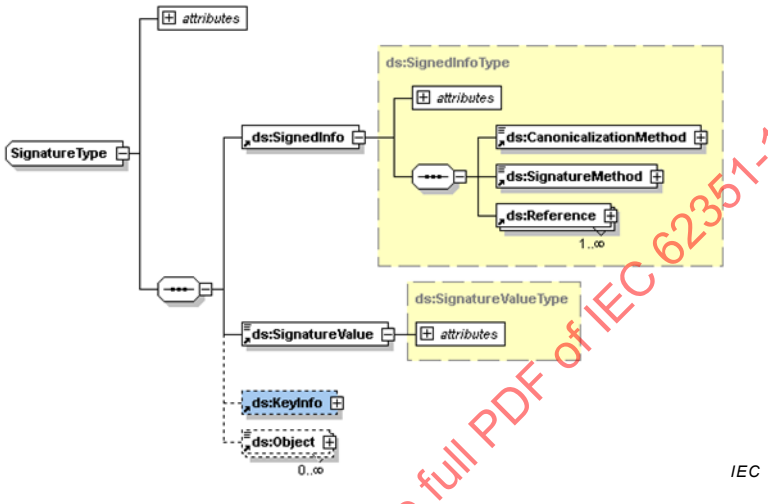


Figure 17 – W3C SignatureType definition

Figure 17 shows the structure of the Signature element is defined as the SignatureType defined by W3C. Subclause 6.5 specifies further constraints of usage of the structure and elements in the structure.

6.5.2 SignedInfoType

6.5.2.1 General

The following clauses detail the selection of specific values that can be used within the SignedInfoType when used for IEC 62351-11. The structure of the SignedInfoType is shown in Figure 18.

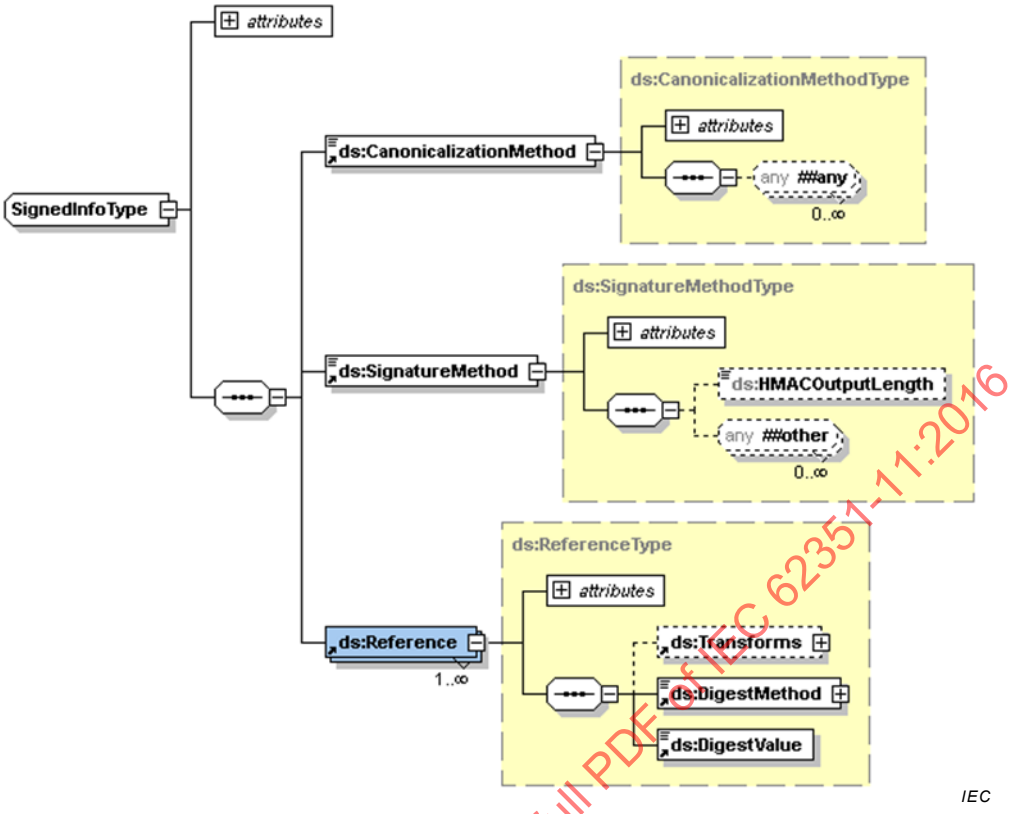


Figure 18 – SignedInfotype XML structure

6.5.2.2 CanonicalizationMethod

There are one mandatory and three recommended canonicalization methods in the W3C signature specification document. The method that shall be used is one of the recommended methods: http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments

The use of this method shall also include existing whitespaces as well as XML comments.

6.5.2.3 SignatureMethod

The defined structure of the SignatureMethod element is shown in Figure 19.

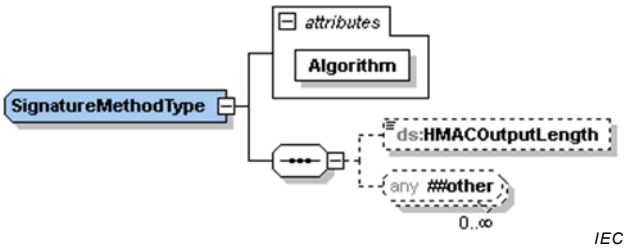


Figure 19 – SignatureMethodType structure

Although the W3C standard allows any registered URI to be utilized, this standard restricts the allowed list to those SignatureMethods registered on IANA (*http://www.iana.org/assignments/xml-security-uris/xml-security-uris.txt).*

Furthermore, only the following are required to be supported for IEC 62351-11:

The Algorithm for the DigestMethod shall be one of the following (per RFC 6931):

2001/04/xmldsig-more#hmac-sha256
2001/04/xmldsig-more#hmac-sha384
2001/04/xmldsig-more#hmac-sha512

All other signatures are out-of-scope of this standard.

Additionally, the calculated HMAC value may be truncated, per RFC 2104 for SHA-256 and SHA-512[2]. The allowed truncations are 80, 128, and 256 bits. These are the only allowed values for HMACOutputLength. If the HMACOutputLength is not present, the HMAC shall be the maximum size per the algorithm.

6.5.2.4 Reference

The defined structure of the SignatureMethod element is shown in Figure 20.

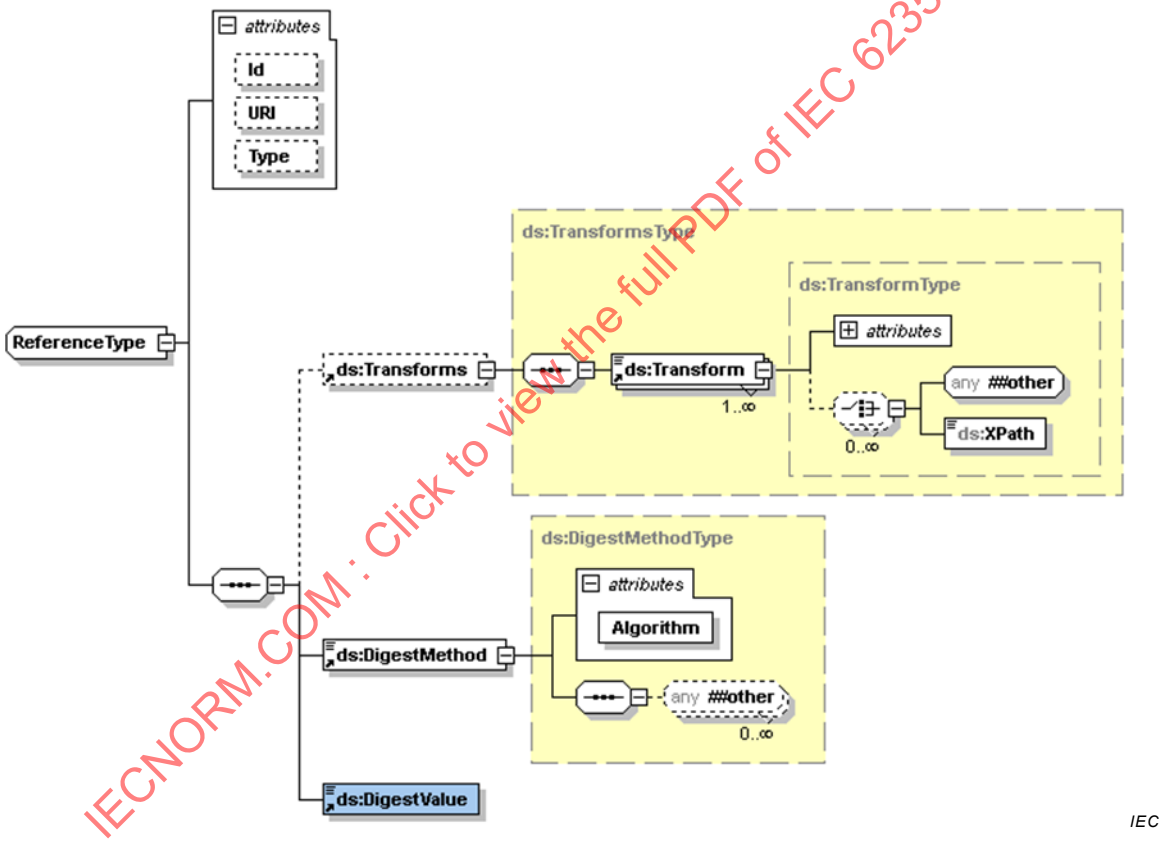


Figure 20 – ReferenceType structure

Within the scope of IEC 62351-11:

- ReferenceType attribute use is out-of-scope of this document and shall be ignored in processing.
- ReferenceType Transforms shall not be specified.
- The Algorithm for the DigestMethod shall be one of the following (per RFC 4051):

  2001/04/xmldsig-more#sha224
  2001/04/xmldsig-more#sha384

2 Per FIPS 180-4.

The DigestValue element is specified by W3C to be:

```
<element name="DigestValue" type="ds:DigestValueType"/>
<simpleType name="DigestValueType">
  <restriction base="base64Binary"/>
</simpleType>
```

The DigestValue shall be calculated on all elements of the IEC 62351-11 document with the exceptions of:

- The SignatureType DigestValue element, as defined by W3C Signature Syntax and Processing.

  The SignatureType SignatureValue element, as defined by W3C Signature Syntax and Processing.

  The SignatureValue shall be calculated including the Header, and nonEncrypted or Encrypted XML elements as shown in Figure 4. Encryption of the original XML document shall occur after the calculation of the Signature using the original (e.g. non-encrypted) document.
- Any SignatureType keyinfo element or Object element
- The IEC 62351-11 tags (e.g <IEC62351-11> and </IEC62351-11>). XML attributes within the IEC62351-11 tag shall be ignored as well.
- The <xml> declaration

6.5.2.5 KeyInfo

The structure of KeyInfo is shown in Figure 21. The KeyInfo element shall be present within the context of IEC 62351-11.

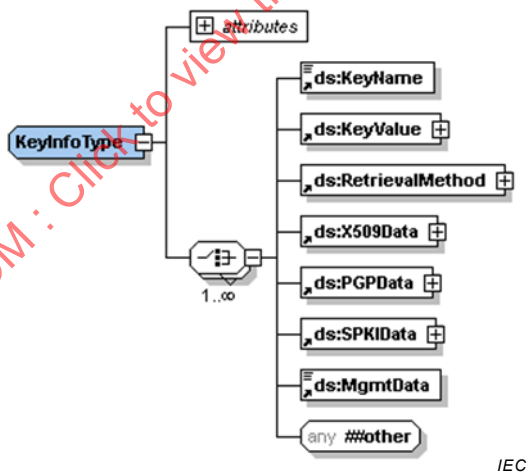


Figure 21 – KeyInfoType Structure

Within the scope, only the following choices shall be allowed:

- KeyValue
- X509Data
- PGPData

6.5.2.6 Object

The ds:Object element shall not appear within the scope of IEC 62351-11.

6.6 Supporting XSD Types

6.6.1 General

This clause provides the XSD definitions for reused XSD types.

6.6.2 NameSeqType

The NameSeqType is used to express a sequence of Name(s). The semantics of the sequence of Name(s) is out of scope of this document. However, its interpretation needs to be well understood by the party that created the IEC 62351-11 document.

Its recommended use is to provide a sequence that is a DistiguishedName or RelativeDistinguishedName, as shown in Figure 22.

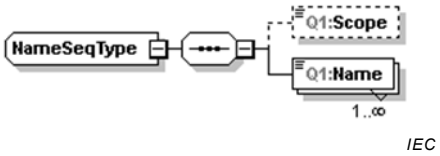


Figure 22 – Definition of NameSeqType

The Scope element is of the xs:string type. There may only be a single value of Scope and the value is used to provide a context to the list of Name(s). The value may be used to detail if the Name(s) are based upon IEC codes or others. The value provided is a local issue.

The Name element is of the xs:string type.

6.7 Security algorithm selection

The selection of the security algorithms follows the approach taken in different part of IEC 62351 for the specific security services. The following list provides the security algorithms per security service should constitute the minimum strength of utilized cryptographic algorithms.

- signature: RSA 2048 with SHA 256 or ECDSA256 with SHA 256
- digest: SHA 256
- keyed digest: HMAC-SHA 256
- encryption: AES-128

The application of algorithms with lower cryptographic strength shall not be supported. The IANA listing provided in the document lists general available algorithms for signature, digest and encryption. The recommended algorithms complying to the list above are marked bold in this list.

7 Example files (informative)

7.1 Non-encrypted example

This subclause shows an example of an IEC 62351-11 XML document using a CIM original document. The DigestValue and SignatureValues are not cryptographically correct.

```
<?xml version="1.0" encoding="UTF-8"?>
<Q1:IEC62351-11 xmlns:Q1="http://www.iec.ch/2014/01/62351-11#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
        xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://www.iec.ch/2014/01/62351-11# file:///C:/Users/root/Desktop/IEC62351-11/IEC62351-11.xsd">
        <Q1:Header>
                <Q1:DateTimeOfEncapsulation>2014-04-14T21:32:52</Q1:DateTimeOfEncapsulation>
                <Q1:Filedesc>Example IEC 62351-11 non-encrypted file</Q1:Filedesc>
        </Q1:Header>
        <Q1:nonEncrypted>
                <Q1:Nonce>85343410947jgfa8312b!</Q1:Nonce>
                <Q1:AccessControl>
                  <Q1:AcessControlInformation>
                    <Q1:ACL>
                          <Q1:ACLRestriction>
                                <Q1:ACLType>Deny</Q1:ACLType>
                                <Q1:ACLConstraints>
                                                <Q1:Constraint>All</Q1:Constraint>
                                </Q1:ACLConstraints>
                                <Q1:ACLAppliedTo>
                                        <Q1:Role>Any</Q1:Role>
                                </Q1:ACLAppliedTo>
                          </Q1:ACLRestriction>
                          <Q1:XPATH>//cim:PowerTransformer[@rdf:ID='_T_Z0568311_Z0568422_1_24574']</Q1:XPATH>
                    </Q1:ACL>
                  </Q1:AcessControlInformation>
                </Q1:AccessControl>
                <Q1:Body>
                        <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#" xmlns:cim="http://iec.ch/TC57/2009/CIM-schema-
                                cim14#">
```

```
            <cim:PowerTransformer rdf:ID="_T_Z0568311_Z0568422_1_24574">
              <cim:IdentifiedObject.name>UNKNOWN     </cim:IdentifiedObject.name>
              <cim:Equipment.MemberOf_EquipmentContainer rdf:resource="#_S_Z0568311Z0568422"/>
            </cim:PowerTransformer>
            <cim:BaseVoltage rdf:ID="_BS_9">
              <cim:BaseVoltage.nominalVoltage>500</cim:BaseVoltage.nominalVoltage>
                    <cim:BaseVoltage.isDC>false</cim:BaseVoltage.isDC>
              <cim:IdentifiedObject.name>500</cim:IdentifiedObject.name>
            </cim:BaseVoltage>
            <cim:SubGeographicalRegion rdf:ID="_Z_X">
              <cim:IdentifiedObject.name>XX</cim:IdentifiedObject.name>
              <cim:SubGeographicalRegion.Region rdf:resource="#_H_XX"/>
            </cim:SubGeographicalRegion>
      <cim:ControlArea rdf:ID="_CA_X">
        <cim:IdentifiedObject.name>ControlArea_XX</cim:IdentifiedObject.name>
        <cim:ControlArea.netInterchange>0</cim:ControlArea.netInterchange>
        <cim:ControlArea.pTolerance>0</cim:ControlArea.pTolerance>
      </cim:ControlArea>
      <cim:Substation rdf:ID="_S_1000085110000721">
        <cim:IdentifiedObject.name>SUBSTATION_2</cim:IdentifiedObject.name>
        <cim:Substation.Region rdf:resource="#_Z_1"/>
      </cim:Substation>
            </rdf:RDF>
      </Q1:Body>
</Q1:nonEncrypted>
<Q1:Signature>
      <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
            <ds:SignatureMethod Algorithm="2001/04/xmldsig-more#hmac-sha256">
                  <ds:HMACOutputLength>128</ds:HMACOutputLength>
            </ds:SignatureMethod>
            <ds:Reference>
              <ds:DigestMethod Algorithm="2001/04/xmldsig-more#sha384"></ds:DigestMethod>
              <ds:DigestValue>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK</ds:DigestValue>
            </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK</ds:SignatureValue>
      <ds:KeyInfo>
```

```
                    <ds:X509Data>
                    <ds:X509IssuerSerial>
                            <ds:X509SerialNumber></ds:X509SerialNumber>
                    </ds:X509IssuerSerial>
                    </ds:X509Data>
            </ds:KeyInfo>
    </Q1:Signature>
</Q1:IEC62351-11>
```

7.2 Encrypted example

This subclause shows an example of an IEC 62351-11 XML document using a CIM original document. The DigestValue, SignatureValue, and the value of CipherData are not cryptographically correct.

```
<?xml version="1.0" encoding="UTF-8"?>
<Q1:IEC62351-11 xmlns:n1=http://www.altova.com/samplexml/other-namespace xmlns:Q1="http://www.iec.ch/2014/01/62351-11#"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://www.iec.ch/2014/01/62351-11# file:///C:/Users/root/Desktop/IEC62351-11/IEC62351-11.xsd">
        <Q1:Header>
                <Q1:DateTimeOfEncapsulation>2014-04-14T21:32:52</Q1:DateTimeOfEncapsulation>
                <Q1:Filedesc>Example IEC 62351-11 non-encrypted file</Q1:Filedesc>
        </Q1:Header>
        <Q1:Encrypted Type="http://www.w3.org/2001/04/xmlenc#Element">
          <enc:EncryptionMethod Algorithm="2009/xmlenc11#aes128-gcm">
            <enc:KeySize>2048</enc:KeySize>
          </enc:EncryptionMethod>
                <enc:CipherData>
                        <enc:CipherValue>
                           TWFuIGlzIGRpc3Rpbmd1aXNoZWQsIG5vdCBvbmx5IGJ5IGhpcyByZWFzb24sIGJ1dCBieSB0aGlz
                           IHNpbmd1bGFyIHBhc3Npb24gZnJvbSBvdGhlciBhbmltYWxzLCB3aGljaCBpcyBhIGx1c3Qgb2Yg
                           dGhlIG1pbmQsIHRoYXQgYnkgYSBwZXJzZXZlcmFuY2Ugb2YgZGVsaWdodCBpbiB0aGUgY29udGlu
                           dWVkIGFuZCBpbmRlZmF0aWdhYmxlIGdlbmVyYXRpb24gb2Yga25vd2xlZGdlLCBleGNlZWRzIHRo
                           ZSBzaG9ydCB2ZWhlbWVuY2Ugb2YgYW55IGNhcm5hbCBwbGVhc3VyZS4=
                </enc:CipherData>
        </Q1:Encrypted>
```

```
<Q1:Signature>
    <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
        <ds:SignatureMethod Algorithm="2001/04/xmldsig-more#hmac-sha256">
            <ds:HMACOutputLength>128</ds:HMACOutputLength>
        </ds:SignatureMethod>
        <ds:Reference>
            <ds:DigestMethod Algorithm="2001/04/xmldsig-more#sha384"></ds:DigestMethod>
            <ds:DigestValue>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK</ds:SignatureValue>
    <ds:KeyInfo>
        <ds:X509Data>
        <ds:X509IssuerSerial>
        <ds:X509IssuerName>IEC</ds:X509IssuerName>
            <ds:X509SerialNumber>0123</ds:X509SerialNumber>
        </ds:X509IssuerSerial>
        </ds:X509Data>
    </ds:KeyInfo>
</Q1:Signature>
</Q1:IEC62351-11>
```

8 IANA list of signature, digest, and encryption methods (informative)

Normative information may be found at: *http://www.iana.org/assignments/xml-security-uris/xml-security-uris.txt*, as shown below:

In order to provide a comparable security / similar selection of cryptographic algorithms as recommended for other parts of IEC 62351 (especially in the profiling of TLS in IEC 62351-3), the recommended cryptographic algorithms are marked **bold**), Note, that this recommendation should not limit the application of stronger algorithms.

The initial "http://www.w3.org/" part of the URI is not included below.

URI	Type	Reference
2000/09/xmldsig#base64	Transform	[RFC3275]
2000/09/xmldsig#DSAKeyValue	Retrieval type	[RFC3275]
2000/09/xmldsig#dsa-sha1	SignatureMethod	[RFC3275]
2000/09/xmldsig#enveloped-signature	Transform	[RFC3275]
2000/09/xmldsig#hmac-sha1	SignatureMethod	[RFC3275]
2000/09/xmldsig#MgmtData	Retrieval type	[RFC3275]
2000/09/xmldsig#minimal	Canonicalization	[RFC6931], section 2.4
2000/09/xmldsig#PGPData	Retrieval type	[RFC3275]
2000/09/xmldsig#rawX509Certificate	Retrieval type	[RFC3275]
2000/09/xmldsig#rsa-sha1	SignatureMethod	[RFC3275]
2000/09/xmldsig#RSAKeyValue	Retrieval type	[RFC3275]
2000/09/xmldsig#sha1	DigestAlgorithm	[RFC3275]
2000/09/xmldsig#SPKIData	Retrieval type	[RFC3275]
2000/09/xmldsig#X509Data	Retrieval type	[RFC3275]
2001/04/xmldsig-more#arcfour	EncryptionMethod	[RFC6931], section 2.6.1
2001/04/xmldsig-more#camellia128-cbc	EncryptionMethod	[RFC6931], section 2.6.2
2001/04/xmldsig-more#camellia192-cbc	EncryptionMethod	[RFC6931], section 2.6.2
2001/04/xmldsig-more#camellia256-cbc	EncryptionMethod	[RFC6931], section 2.6.2
2001/04/xmldsig-more#ecdsa-sha1	SignatureMethod	[RFC6931], section 2.3.6
2001/04/xmldsig-more#ecdsa-sha224	SignatureMethod	[RFC6931], section 2.3.6
2001/04/xmldsig-more#ecdsa-sha256	**SignatureMethod**	**[RFC6931], section 2.3.6**
2001/04/xmldsig-more#ecdsa-sha384	SignatureMethod	[RFC6931], section 2.3.6
2001/04/xmldsig-more#ecdsa-sha512	SignatureMethod	[RFC6931], section 2.3.6
2001/04/xmldsig-more#esign-sha1	SignatureMethod	[RFC6931], section 2.3.7
2001/04/xmldsig-more#esign-sha224	SignatureMethod	[RFC6931], section 2.3.7
2001/04/xmldsig-more#esign-sha256	SignatureMethod	[RFC6931], section 2.3.7
2001/04/xmldsig-more#esign-sha384	SignatureMethod	[RFC6931], section 2.3.7
2001/04/xmldsig-more#esign-sha512	SignatureMethod	[RFC6931], section 2.3.7
2001/04/xmldsig-more#hmac-md5	SignatureMethod	[RFC6931], section 2.2.1
2001/04/xmldsig-more#hmac-ripemd160	SignatureMethod	[RFC6931], section 2.2.3
2001/04/xmldsig-more#hmac-sha224	SignatureMethod	[RFC6931], section 2.2.2
2001/04/xmldsig-more#hmac-sha256	**SignatureMethod**	**[RFC6931], section 2.2.2**
2001/04/xmldsig-more#hmac-sha384	SignatureMethod	[RFC6931], section 2.2.2
2001/04/xmldsig-more#hmac-sha512	SignatureMethod	[RFC6931], section 2.2.2
2001/04/xmldsig-more#KeyName	Retrieval type	[RFC6931], section 3.2
2001/04/xmldsig-more#KeyValue	Retrieval type	[RFC6931], section 3.2
2001/04/xmldsig-more#kw-camellia128	EncryptionMethod	[RFC6931], section 2.6.3
2001/04/xmldsig-more#kw-camellia192	EncryptionMethod	[RFC6931], section 2.6.3
2001/04/xmldsig-more#kw-camellia256	EncryptionMethod	[RFC6931], section 2.6.3
2001/04/xmldsig-more#md5	DigestAlgorithm	[RFC6931], section 2.1.1
2001/04/xmldsig-more#PKCS7signedData	Retrieval type	[RFC6931], section 3.2
2001/04/xmldsig-more#psec-kem	EncryptionMethod	[RFC6931], section 2.6.4
2001/04/xmldsig-more#rawPGPKeyPacket	Retrieval type	[RFC6931], section 3.2
2001/04/xmldsig-more#rawPKCS7signedData	Retrieval type	[RFC6931], section 3.2
2001/04/xmldsig-more#rawSPKISexp	Retrieval type	[RFC6931], section 3.2
2001/04/xmldsig-more#rawX509CRL	Retrieval type	[RFC6931], section 3.2

2001/04/xmldsig-more#RetrievalMethod Retrieval type [RFC6931], section 3.2
2001/04/xmldsig-more#rsa-md5 SignatureMethod [RFC6931], section 2.3.1
2001/04/xmldsig-more#rsa-sha256 SignatureMethod [RFC6931], section 2.3.2
2001/04/xmldsig-more#rsa-sha384 SignatureMethod [RFC6931], section 2.3.3
2001/04/xmldsig-more#rsa-sha512 SignatureMethod [RFC6931], section 2.3.4
2001/04/xmldsig-more#rsa-ripemd160 SignatureMethod [RFC6931], section 2.3.5
2001/04/xmldsig-more#sha224 DigestAlgorithm [RFC6931], section 2.1.2
2001/04/xmldsig-more#sha384 DigestAlgorithm [RFC6931], section 2.1.3
2001/04/xmldsig-more#xptr Transform [RFC6931], section 2.5.1
2001/04/xmldsig-more#PKCS7signedData KeyInfo child [RFC6931], section 3.1
2001/04/xmlenc#aes128-cbc EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2001/04/xmlenc#aes192-cbc EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2001/04/xmlenc#aes256-cbc EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2001/04/xmlenc#dh AgreementMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2001/04/xmlenc#kw-aes128 EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2001/04/xmlenc#kw-aes192 EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2001/04/xmlenc#kw-aes256 EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2001/04/xmlenc#ripemd160 DigestAlgorithm ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2001/04/xmlenc#rsa-1_5 EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2001/04/xmlenc#rsa-oaep-mgf1p EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2001/04/xmlenc#sha256 DigestAlgorithm ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2001/04/xmlenc#sha512 DigestAlgorithm ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2001/04/xmlenc#tripledes-cbc EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
["XML-Signature XPath Filter 2.0"], J. Boyer, M. Huges, J. Reagle, 8 November 2002.
2002/06/xmldsig-filter2 Transform ["XML Path Language (XPath) 2.0 (Second Edition)"], A. Berglund, S. Boag, D. Chamberlin, M. Fernandez, M. Kay, J. Robie, J. Simeon, W3C Recommendation 14 December 2010.
2002/07/decrypt#XML Transform ["Decryption Transform for XML Signature"], M. Hughes, T. Imamura, H. Maruyama, W3C Recommendation 10 December 2002.
2002/07/decrypt#Binary Transform ["Decryption Transform for XML Signature"], M. Hughes, T. Imamura, H. Maruyama, W3C Recommendation 10 December 2002.

2006/12/xmlc12n11# Canonicalization ["Canonical XML Version 1.1"], J. Boyer, G. Marcy, W3C Recommendation 2 May 2008.
2006/12/xmlc14n11#WithComments Canonicalization ["Canonical XML Version 1.1"], J. Boyer, G. Marcy, W3C Recommendation 2 May 2008.
2007/05/xmldsig-more#ecdsa-ripemd160 SignatureMethod [RFC6931], section 2.3.6
2007/05/xmldsig-more#ecdsa-whirlpool SignatureMethod [RFC6931], section 2.3.5
2007/05/xmldsig-more#kw-seed128 EncryptionMethod [RFC6931], section 2.6.6
2007/05/xmldsig-more#md2-rsa-MGF1 SignatureMethod [RFC6931], section 2.3.10
2007/05/xmldsig-more#md5-rsa-MGF1 SignatureMethod [RFC6931], section 2.3.10
2007/05/xmldsig-more#MGF1 SignatureMethod [RFC6931], section 2.3.9
2007/05/xmldsig-more#ripemd128-rsa-MGF1 SignatureMethod [RFC6931], section 2.3.10
2007/05/xmldsig-more#ripemd160-rsa-MGF1 SignatureMethod [RFC6931], section 2.3.10
2007/05/xmldsig-more#rsa-pss SignatureMethod [RFC6931], section 2.3.9
2007/05/xmldsig-more#rsa-sha224 SignatureMethod [RFC6931], section 2.3.11
2007/05/xmldsig-more#rsa-whirlpool SignatureMethod [RFC6931], section 2.3.5
2007/05/xmldsig-more#seed128-cbc EncryptionMethod [RFC6931], section 2.6.5
2007/05/xmldsig-more#sha1-rsa-MGF1 SignatureMethod [RFC6931], section 2.3.10
2007/05/xmldsig-more#sha224-rsa-MGF1 SignatureMethod [RFC6931], section 2.3.10
2007/05/xmldsig-more#sha256-rsa-MGF1 SignatureMethod [RFC6931], section 2.3.10
2007/05/xmldsig-more#sha3-224 DigestAlgorithm [RFC6931], section 2.1.5
2007/05/xmldsig-more#sha3-224-rsa-MGF1 SignatureMethod [RFC6931], section 2.3.10
2007/05/xmldsig-more#sha3-256 DigestAlgorithm [RFC6931], section 2.1.5
2007/05/xmldsig-more#sha3-256-rsa-MGF1 SignatureMethod [RFC6931], section 2.3.10
2007/05/xmldsig-more#sha3-384 DigestAlgorithm [RFC6931], section 2.1.5
2007/05/xmldsig-more#sha3-384-rsa-MGF1 SignatureMethod [RFC6931], section 2.3.10
2007/05/xmldsig-more#sha3-512 DigestAlgorithm [RFC6931], section 2.1.5
2007/05/xmldsig-more#sha3-512-rsa-MGF1 SignatureMethod [RFC6931], section 2.3.10
2007/05/xmldsig-more#sha384-rsa-MGF1 SignatureMethod [RFC6931], section 2.3.10
2007/05/xmldsig-more#sha512-rsa-MGF1 SignatureMethod [RFC6931], section 2.3.10
2007/05/xmldsig-more#whirlpool DigestAlgorithm [RFC6931], section 2.1.4
2007/05/xmldsig-more#whirlpool-rsa-MGF1 SignatureMethod [RFC6931], section 2.3.10
2009/xmlenc11#kw-aes-128-pad EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F.
Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2009/xmlenc11#kw-aes-192-pad EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F.
Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2009/xmlenc11#kw-aes-256-pad EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F.
Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
["XML Signature Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, D.
2009/xmldsig11#dsa-sha256 SignatureMethod Solo, F. Hirsch, M. Nystrom, T. Roessler, K. Yiu, Proposed Recommendation 24 January
2013.
["XML Signature Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, D.
2009/xmldsig11#ECKeyValue Retrieval type Solo, F. Hirsch, M. Nystrom, T. Roessler, K. Yiu, Proposed Recommendation 24 January
2013.
["XML Signature Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, D.
2009/xmldsig11#DEREncodedKeyValue Retrieval type Solo, F. Hirsch, M. Nystrom, T. Roessler, K. Yiu, Proposed Recommendation 24 January
2013.
2009/xmlenc11#aes128-gcm EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F.
Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.
2009/xmlenc11#aes192-gcm EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F.
Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.

2009/xmlenc11#aes256-gcm EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.

2009/xmlenc11#ConcatKDF EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.

2009/xmlenc11#mgf1sha1 SignatureMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.

2009/xmlenc11#mgf1sha224 SignatureMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.

2009/xmlenc11#mgf1sha256 SignatureMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.

2009/xmlenc11#mgf1sha384 SignatureMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.

2009/xmlenc11#mgf1sha512 SignatureMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.

2009/xmlenc11#pbkdf2 EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.

2009/xmlenc11#rsa-oaep EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.

2009/xmlenc11#ECDH-ES EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.

2009/xmlenc11#dh-es EncryptionMethod ["XML Encryption Syntax and Processing Version 1.1"], D. Eastlake, J. Reagle, F. Hirsch, T. Roessler, Proposed Recommendation 24 January 2013.

2010/xmlsec-ghc#generic-hybrid Generic Hybrid ["XML Security Generic Hybrid Ciphers"], M. Nystrom, F. Hirsch, 24 January 2013.

2010/xmlsec-ghc#rsaes-kem Generic Hybrid ["XML Security Generic Hybrid Ciphers"], M. Nystrom, F. Hirsch, 24 January 2013.

2010/xmlsec-ghc#ecies-kem Generic Hybrid ["XML Security Generic Hybrid Ciphers"], M. Nystrom, F. Hirsch, 24 January 2013.

["XML-Signature XPath Filter 2.0"], J. Boyer, M. Huges, J. Reagle, 8 November 2002.

TR/1999/REC-xpath-19991116 Transform ["XML Path Language (XPath) 2.0 (Second Edition)"], A. Berglund, S. Boag, D. Chamberlin, M. Fernandez, M. Kay, J. Robie, J. Simeon, W3C Recommendation 14 December 2010.

TR/1999/REC-xslt-19991116 Transform ["XSL Transformations (XSLT) Version 2.0"], M. Saxonica, W3C Recommendation 23 January 2007.

TR/2001/06/xml-exc-c14n# Canonicalization ["Exclusive XML Canonicalization Version 1.0"], D. Eastlake, J. Reagle, W3C Recommendation 18 July 2002.

TR/2001/06/xml-exc-c14n#WithComments Canonicalization ["Exclusive XML Canonicalization Version 1.0"], D. Eastlake, J. Reagle, W3C Recommendation 18 July 2002.

TR/2001/REC-xml-c14n-20010315 Canonicalization ["Canonical XML Version 1.0"], J. Boyer, W3C Recommendation 15 March 2001.

TR/2001/REC-xml-c14n-20010315#WithComments Canonicalization ["Canonical XML Version 1.0"], J. Boyer, W3C Recommendation 15 March 2001.

["XML Schema Part 1: Structures Second Edition"], H. Thompson, D. Beech, M. Maloney,

TR/2001/REC-xmlschema-1-20010502 Transform N. Mendelsohn, W3 Recommendation 28 October 2004. ["XML Schema Part 2: Datatypes Second Edition"], P. Biron, A. Malhotra, W3C Recommendation 28 October 2004.

Bibliography

IEC 61850-6, *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs*

IEC 61970-552, *Energy management system application program interface (EMS-API) – Part 552: CIM XML Model exchange format*

IEC TS 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC 62351-3, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*

RFC 4301, *Security Architecture for the Internet Protocol*

RFC 2437, *PKCS #1: RSA Cryptography Specifications Version 2.0*

RFC 3174, *Secure Hash Algorithm (SHA1)*

RFC 3275, (Extensible Markup Language) XML-Signature Syntax and Processing

RFC 6234, US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)

RFC 4051, Additional XML Security Uniform Resource Identifiers (URIs)

[XML-C14N] RFC 3076, *Canonical XML Version 1.0*, March 2001, <http://www.ietf.org/rfc/rfc3076.txt>

[XML-DSIG] RFC 3275, *XML-Signature Syntax and Processing*, March 2002, <http://www.ietf.org/rfc/rfc3275.txt>

[SMIME-EX] RFC 4134, *Examples of S/MIME Messages*, July 2005, <http://www.ietf.org/rfc/rfc4134.txt>

XML Signature WG <http://www.w3.org/Signature/>:

- *XML-Signature Syntax and Processing* <http://www.w3.org/TR/xmldsig-core/>
- *Canonical XML Version 1.0*, <http://www.w3.org/TR/2001/REC-xml-c14n-20010315/>
- *Exclusive XML Canonicalization Version 1.0*, <http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/>

[GUTM04] Peter Gutmann, *Why XML Security is Broken*, October 2004, <http://www.cs.auckland.ac.nz/~pgut001/pubs/xmlsec.txt>

http://www.iana.org/assignments/xml-security-uris/xml-security-uris.txt

XML Signature references the following documents. However it is considered that it is not necessary to reference these documents, as they do not directly impact X.893./
W3C Document Object Model (DOM) Level 1 Specification, W3C 1998./
NIST FIPS PUB 186-2, Digital Signature Standard (DSS), NIST 2001./
IETF RFC 2104, Keyed-Hashing for Message Authentication, IETF 1997

IETF RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1, IETF Standard, January 1996
IETF RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, IETF Standard 1997
IETF RFC 2253, Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names, IETF 1997
IETF RFC 1321, The MD5 Digest Algorithm, IETF 1992
IETF RFC 2045, Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, IETF 1996
Unicode TR15, Unicode Normalization Forms, Unicode Consortium 1999
Normalization Corrigendum, Unicode Consortium 2003
IETF RFC 2240, OpenPGP Message Format, IETF 1998
IETF RFC 1750, Randomness Recommendations for Security, IETF 1994
W3C Resource Description Framework (RDF) Schema Specification 1.0, W3C 2002
IEEE 1363, Standard Specifications for Public Key Cryptography, IEEE August 2000
IETF RFC 2437, PKCS #1: RSA Cryptography Specifications Version 2.0, IETF 1998
NIST FIPS 180-1, Secure Hash Standard, NIST 1995
W3C Simple Object Access Protocol (SOAP) 1.1, W3C 2001
The Unicode Standard, Unicode Consortium 2000
IETF RFC 2781, UTF-16, an encoding of ISO 10646, IETF Standard 2000
IETF RFC 2279, UTF-8, a transformation format of ISO 10646, IETF Standard 1998
IETF RFC 2396, Uniform Resource Identifiers (URI): Generic Syntax, IETF Standard, 1998
IETF RFC 2732, Format for Literal IPv6 Addresses in URL's, IETF Standard 1999
IETF RFC 1738, Universal Resource Locators (URL), IETF Standard, December 1994
IETF RFC 2141, URN Syntax, IETF Standard, May 1997
ITU-T X.509 version 3, The Directory Authentication Framework, ITU-T 1997
W3C XHTML™ 1.0: The Extensible Hypertext Markup Language, W3C 2000
W3C XML Linking Language (XLink) Version 1.0, W3C 2001
W3C XML 1.0, Extensible Markup Language (XML) 1.0 (Second Edition), W3C 2000
W3C Canonical XML, W3C 2001
IETF RFC 2376, XML Media Types, IETF 1998
W3C XML Namespaces 1.0, Namespaces in XML, W3C 1999
W3C XML Schema Part 1, XML Schema Part 1: Structures, W3C 2001
W3C XML Schema Part 2, XML Schema Part 2: Datatypes, W3C 2001
W3C XML Path Language (XPath), W3C 1999

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES D'INFORMATIONS ASSOCIÉS – SÉCURITÉ DES COMMUNICATIONS ET DES DONNÉES –

Partie 11: Sécurité des documents XML

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62351-11 a été établie par le comité d'études 57 de l'IEC: Gestion des systèmes de puissance et échanges d'informations associés.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
57/1753/FDIS	57/1774/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62351, publiées sous le titre général *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. À cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES D'INFORMATIONS ASSOCIÉS – SÉCURITÉ DES COMMUNICATIONS ET DES DONNÉES –

Partie 11: Sécurité des documents XML

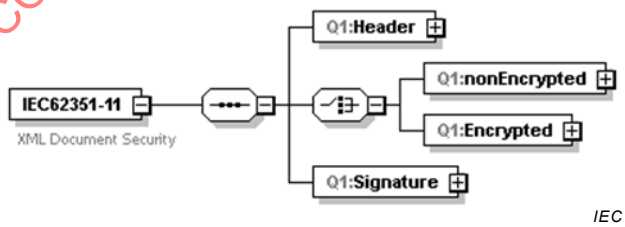
1 Domaine d'application

La présente partie de l'IEC 62351 spécifie un schéma, des procédures et des algorithmes permettant de sécuriser les documents XML qui sont utilisés dans le cadre du domaine d'application de l'IEC ainsi que les documents utilisés dans d'autres domaines (par exemple, IEEE, propriétaire, etc.). La présente partie est destinée à être citée en référence par les normes si des échanges sécurisés sont exigés, à moins qu'un accord existe entre les parties donnant lieu à l'utilisation d'autres mécanismes reconnus d'échanges sécurisés.

La présente partie de l'IEC 62351 s'appuie sur des normes W3C reconnues pour la sécurité des documents XML et en fournit un profilage ainsi que des extensions supplémentaires. Les extensions de l'IEC 62351-11 permettent d'obtenir les éléments suivants:

- Header: l'en-tête contient des informations relatives à la création du document sécurisé, telles que la date et l'heure de création de l'IEC 62351-11.
- La possibilité d'encapsuler le document XML original dans un format chiffré (Encrypted) ou non chiffré (nonEncryped). Si le chiffrement est choisi, un mécanisme rend possible le chiffrement des informations exigées de manière interopérable (EncryptionInfo).
- AccessControl: mécanisme permettant d'expliciter les informations de contrôle d'accès relatives aux informations contenues dans le document XML original.
- Body: est utilisé pour contenir le document XML original qui est encapsulé.
- Signature: signature qui peut être utilisée à des fins d'authentification et de détection des altérations.

La structure générale est représentée à la Figure 1.



Anglais	Français
XML Document Security	Sécurité du document XML

Figure 1 – Présentation de la structure de l'IEC 62351-11

Pour que les mesures décrites dans le présent document soient mises en œuvre, elles doivent être acceptées et référencées dans les spécifications elles-mêmes. Le présent document est rédigé afin de permettre ce processus.

Les premiers utilisateurs auxquels s'adresse la présente partie de l'IEC 62351 sont censés être les concepteurs de produits qui mettent en œuvre ces spécifications.

Des segments de la présente partie de l'IEC 62351 peuvent aussi être utiles aux gestionnaires et aux dirigeants pour comprendre l'objectif d'une activité et les exigences correspondantes.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms* (disponible en anglais seulement)

IEC TS 62351-8, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control* (disponible en anglais seulement)

IEC TS 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment* (disponible en anglais seulement)

Recommandation XML Canonique 1.0 avec commentaires, W3C, http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments

Exigence XML Canonique 1.0 sans commentaires, W3C, http://www.w3.org/TR/2001/REC-xml-c14n-20010315

RFC 6931, *Additional XML Security Uniform Resource Identifiers (URIs)*

Traitement et Syntaxe de Cryptage XML, Version 1.1, 11 avril 2013, http://www.w3.org/TR/xmlenc-core1/

Recommandation Traitement et Syntaxe des Signatures XML du W3C, 10 juin 2008, http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de IEC TS 62351-2 ainsi que les suivants, s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1
nonce
valeur aléatoire ou pseudo-aléatoire utilisée dans un système d'authentification

[SOURCE: Norme IEEE 1455-1999, IEEE Standard for Message Sets for Vehicle/Roadside Communications]

3.2
IANA
Internet Assigned Numbers Authority

Note 1 à l'article: IANA est responsable de la coordination globale de la zone racine du DNS, de l'adressage IP et d'autres ressources de protocole Internet.

[SOURCE: http://www.iana.org]

4 Questions de sécurité abordées dans le présent document

4.1 Généralités

Au sein du secteur et de l'IEC, l'échange de documents XML devient de plus en plus fréquent. Dans le cadre du domaine d'application de l'IEC, les échanges de documents XML sont utilisés pour l'IEC 61970 ainsi que pour l'IEC 61850. Au sein des autres normes, telles que l'IEEE 1815 et l'IEEE C37.111 (COMTRADE), le XML est également utilisé. Les informations contenues dans ces normes et dans d'autres documents basés sur le XML peuvent:

1) être sensibles à des modifications involontaires ou malveillantes de leur contenu, lesquelles sont susceptibles de donner lieu à un mauvais fonctionnement ou à une interprétation erronée si les informations échangées sont utilisées (par exemple, une vulnérabilité en matière de sécurité);
2) comporter des données confidentielles ou privées;
3) comprendre des sous-ensembles d'informations qui peuvent être considérés comme sensibles par l'entité ayant créé le document.

La présente partie de l'IEC 62351 propose de normaliser les mécanismes dans le but de protéger le contenu des documents contre toute altération ou divulgation lorsque ces documents sont échangés (par exemple, en transit). De plus, la présente partie de l'IEC 62351 suggère de normaliser un mécanisme permettant de faciliter la protection des informations lorsque les documents sont en transition (par exemple, l'entité A fait confiance à l'entité B, B fait confiance à A et à C, et B a besoin d'échanger des informations avec C, mais A ne connaît pas C ou ne lui fait pas confiance).

Bien que l'objet du présent document soit de sécuriser les documents XML utilisés dans le cadre du domaine d'application de l'IEC, le mécanisme/les méthodologies définis dans ce document peuvent être appliqués à n'importe quel document XML.

4.2 Contournement des menaces à la sécurité

Voir l'IEC TS 62351-1 pour une présentation des menaces à la sécurité et des méthodes d'attaque.

Si le chiffrement n'est pas employé, les menaces particulières contournées dans la présente partie de l'IEC 62351 comprennent:

- la modification non autorisée (altération) des informations à travers l'authentification au niveau du document XML.

Si le chiffrement est employé, les menaces particulières contournées dans la présente partie de l'IEC 62351 comprennent:

- l'accès non autorisé à des informations à travers l'authentification au niveau du document XML et le chiffrement des documents;
- la modification non autorisée (altération) des informations à travers l'authentification au niveau du document XML, que le chiffrement soit employé ou non.

4.3 Contournement des méthodes d'attaque

La mise en œuvre appropriée des spécifications et recommandations contenues dans le présent document a pour objet de contourner les méthodes d'attaque suivantes:

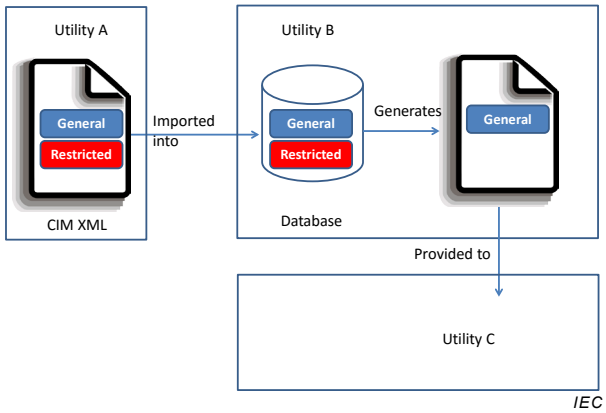
- attaque de l'homme du milieu: cette menace est contournée via l'utilisation d'un mécanisme de code d'authentification de message (par exemple, Signature) spécifié dans le présent document;
- altération du message: ces menaces sont contournées via l'algorithme utilisé pour créer le mécanisme d'authentification tel que spécifié dans le présent document.

5 Documents XML

Afin d'assurer une sécurité adaptée, il est nécessaire de comprendre l'environnement d'utilisation visé par la présente spécification:

- Documents inactifs: Lorsque les documents XML sont stockés (par exemple, inactifs), la détection des altérations est une exigence minimale. Si le document contient des informations sensibles, il est alors nécessaire d'en protéger la confidentialité par l'intermédiaire d'un chiffrement authentifié. Pour satisfaire à ces deux objectifs, cela implique que le document non chiffré a besoin d'une signature et que le document chiffré a aussi besoin de sa propre signature/protection de l'intégrité. La protection des documents XML inactifs ne relève pas du domaine d'application de la présente norme et il convient de la mettre en œuvre par des moyens locaux.
- Documents en transit: La protection des documents en transit exige au minimum la détection des altérations et l'authentification. Si le document contient des informations sensibles, il est alors nécessaire d'en protéger la confidentialité par l'intermédiaire d'un chiffrement authentifié. Pour satisfaire à ces deux objectifs, cela implique que le document non chiffré a besoin d'une signature et que le document chiffré a aussi besoin de sa propre signature/protection de l'intégrité.
- Documents en transition: Dans le domaine de l'IEC, les destinataires des documents XML déchiffrent et analysent généralement les informations contenues dans ces documents dans une base de données. Les informations issues de la base de données peuvent ensuite être exportées de nouveau vers un tiers, sous quelque forme que ce soit (y compris un autre document XML). Si des informations sensibles ou confidentielles étaient fournies dans le document initial, aucun mécanisme technologique ne peut empêcher l'application d'exporter ces informations et de définir des contrôles d'accès.

  Un exemple de cas d'utilisation représentatif est le transfert d'informations sur la topologie des systèmes de puissance à travers l'utilisation de l'IEC 61970-552.



Anglais	Français
Utility {A; B; C}	Fournisseur {A; B; C}
General	Général
Restricted	Restreint

Anglais	Français
CIM XML	CIM XML
Imported into	Importé dans
Generates	Génère
Database	Base de données
Provided to	Fourni à

Figure 2 – Exemple de données en transition

La Figure 2 représente ce problème potentiel avec les données en transition. Le Fournisseur[1] A fournit un document CIM XML au Fournisseur B. Le document contient les informations qui doivent être échangées entre le Fournisseur A et le Fournisseur B en fonction de la confiance ou des accords existant entre eux. Le Fournisseur B importe les informations dans sa base de données (par exemple, EMS). Un échange séparé d'informations doit ensuite avoir lieu entre le Fournisseur B et le Fournisseur C. Le Fournisseur A peut ne pas avoir connaissance de la nécessité d'un tel transfert ni savoir que certaines des informations faisant l'objet d'un accès «restreint» peuvent être exposées à un risque lors de l'exportation par le Fournisseur B. Le but de l'approche recommandée ici pour la gestion des données en transition est de permettre au Fournisseur A de classer et de marquer comme sensibles ou confidentielles certaines parties du document afin que celles-ci ne soient pas exportées de nouveau vers des partenaires du Fournisseur B.

À noter que la signature du document, telle que décrite dans la présente norme, n'est pas suffisante à cet égard, dans la mesure où le Fournisseur B est en droit d'utiliser le contenu faisant l'objet d'un accès restreint et par conséquent de le déchiffrer en vue de l'importer dans une base de données d'application. Il est donc nécessaire de proposer une autre solution, à savoir le mécanisme de contrôle d'accès contractuel décrit en 6.3.3.

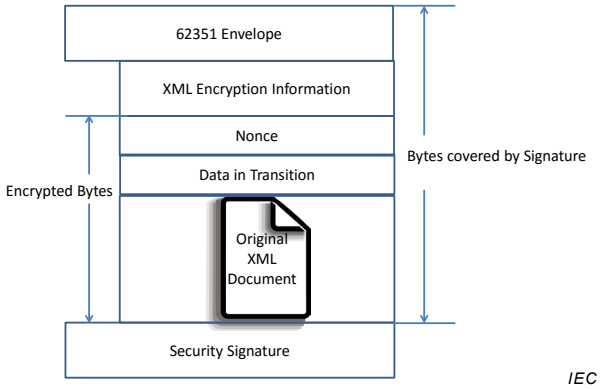
Dans le contexte de l'IEC, au moins deux types connus de documents XML exigent une protection: les documents CIM XML et les documents SCL. Ces documents ont des formats et des définitions de schéma XML (XSD) bien formés. De ce fait, les mécanismes spécifiés dans la présente norme visent à préserver les formats des documents. L'encapsulation des documents originaux est donc l'approche à adopter.

6 Encapsulation des documents XML

6.1 Généralités

Le concept d'encapsulation de la sécurité pour les documents XML est représenté à la Figure 3.

[1] Les acteurs présentés dans ces scénarios ne se limitent pas aux fournisseurs et peuvent aussi inclure les RTO, les échanges et portails commerciaux, les animateurs de programme pour les consommateurs, etc.

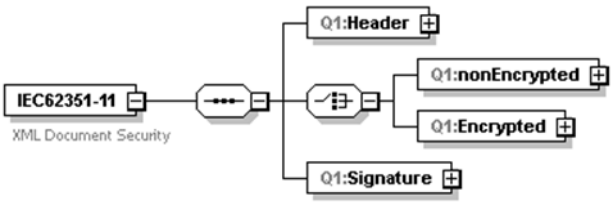


Anglais	Français
62351 Envelope	Enveloppe de l'IEC 62351
XML Encryption Information	Informations de chiffrement XML
Nonce	Nonce
Data in Transition	Données en transition
Original XML Document	Document XML original
Security Signature	Signature de sécurité
Encrypted Bytes	Octets chiffrés
Bytes covered by Signature	Octets couverts par la Signature

Figure 3 – Encapsulation sécurisée des documents XML

Le concept consiste à utiliser des techniques de sécurité XML déjà normalisées en vue de chiffrer l'en-tête, la signature et le document en toute sécurité. Le document «sécurisé» contient le document XML original et les extensions spécifiées par la présente norme. Les extensions de l'IEC 62351-11 permettent d'obtenir les éléments suivants:

- L'enveloppe de l'IEC 62351 (Header): l'en-tête contient des informations relatives à l'encapsulation telles que la date et l'heure de l'encapsulation (par exemple, la création du document).
- Des informations sur le chiffrement XML: la possibilité d'encapsuler la liste de contrôle d'accès (ACL) du document XML original dans un format chiffré (Encrypted) ou non chiffré (nonEncrypted). Si le chiffrement est choisi, un mécanisme rend possible le chiffrement des informations exigées de manière interopérable (EncryptionInfo).
- Données en transition: mécanisme permettant d'expliciter les informations de contrôle d'accès relatives aux données contenues dans le document XML original.
- Document XML original (Body): est utilisé pour contenir le document XML original qui est encapsulé.
- Signature: signature qui peut être utilisée à des fins d'authentification et de détection des altérations.



Anglais	Français
XML Document Security	Sécurité du document XML

Figure 4 – Disposition XSD générale de l'IEC 62351-11

La Figure 4 représente la structure XSD générale d'un document IEC 62351-11. Les définitions sont indiquées dans le Tableau 1.

Tableau 1 – Définitions de la structure générale pour un document IEC 62351-11

Élément	Facultatif (O) / Obligatoire (M) / Conditionnel (C)	Type XSD	Description
Header	M	HeaderType (voir 6.2)	L'en-tête contient des informations sur la création du document IEC 62351-11 ainsi que des informations de contact en cas de questions ou de problèmes en lien avec le document.
nonEncrypted	C	Information (voir 6.3)	Permet de contrôler l'accès et d'intégrer le document original dans un format non chiffré (par exemple, le contenu du document original peut toujours être consulté). Il convient qu'un utilisateur fasse un tel choix si la confidentialité des informations n'est pas concernée ou si la confidentialité est assurée par un mécanisme externe. L'un ou l'autre des éléments XSD, à savoir nonEncrypted ou Encrypted, doit être présent.
Encrypted	C	EncryptedType (voir 6.4)	Permet de chiffrer le contrôle d'accès et l'intégration du document original. Il convient que l'utilisateur fasse un tel choix si la confidentialité des informations est souhaitée et si celle-ci n'est pas assurée par des mécanismes externes. L'un ou l'autre des éléments XSD, à savoir nonEncrypted ou Encrypted, doit être présent.
Signature	M	SignatureType	Est une production des informations sur la Signature XML du W3C.

Toute mise en œuvre se déclarant conforme à la présente norme doit appliquer tous les éléments obligatoires.

6.2 HeaderType

La Figure 5 représente la structure XSD du HeaderType.

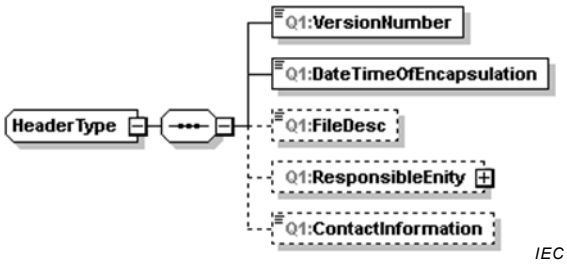


Figure 5 – Définition du type complexe XSD de l'élément HeaderType

Le HeaderType est un type complexe XSD qui comprend une série d'éléments XSD tels que décrits dans le Tableau 2.

Tableau 2 – Définition de l'élément HeaderType

Élément	Facultatif (O) / Obligatoire (M) / Conditionnel (C)	Type XSD	Description
VersionNumber	M	xs:float	Est le numéro de version de la norme IEC 62351-11 qui est mise en œuvre. Le nombre à virgule flottante doit spécifier <majorVersion>.<minorVersion>. La valeur doit être «1.0»
DateTimeOfEncapsulation	M	xs:DateTime	La valeur spécifie la date et l'heure d'intégration du document original.
FileDesc	O	xs:string	La description du document et de son contenu fournie par un utilisateur. Si le Body (par exemple, le document original) est chiffré ou codé en hexa ou ascii, cet élément est obligatoire, car son absence empêcherait l'utilisateur de déterminer le contenu du document en cas de questions. Tous les documents encapsulés doivent partager cette description.
ResponsibleEntity	O	NameSeqType (voir 6.6.2)	Le nom d'une entité fourni et pouvant être utilisé par un utilisateur du document afin de savoir qui contacter en cas de problème ou de question concernant le document.
ContactInformation	O	xs:string	Est une chaîne fournie par un utilisateur et pouvant contenir des informations sur le téléphone ou le courriel dont l'utilisateur d'un document peut faire usage en cas de problème ou de question.

6.3 Information

6.3.1 Généralités

La Figure 6 représente la structure du type Information.

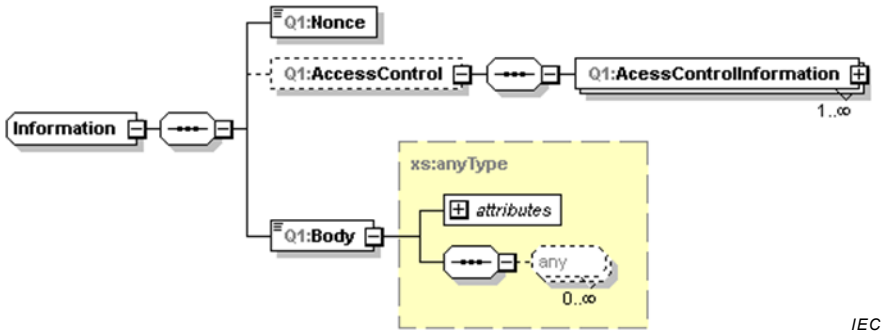


Figure 6 – Définition du type complexe XSD de l'élément Information

Il s'agit d'une séquence XSD des sous-éléments suivants: Nonce, AccessControl et Body. La définition de ces éléments ainsi que leurs types sont présentés dans le Tableau 3.

Tableau 3 – Définition de l'élément Information

Élément	Facultatif (O) / Obligatoire (M) / Conditionnel (C)	Type XSD	Description
Nonce	M	xs:string	Voir 6.3.2.
AccessControl	O	AccessControlType Voir 6.3.3	Cet élément permet d'expliciter les informations relatives au contrôle d'accès. La valeur par défaut pour AccessControl est Allow All si aucun élément AccessControl n'est présent.
Body	M	xs:anyType	L'élément permet d'encapsuler un ou plusieurs documents dans le même document IEC 62351-11.

6.3.2 Nonce

Cet élément représente un attribut relatif à la sécurité qui garantit au moins une signature différente si le même Body utilise les mêmes identifiants. Dans de nombreuses situations, il convient qu'un nonce cryptographique soit cryptographiquement aléatoire. Cependant, pour les besoins de la présente norme, le caractère aléatoire n'est pas exigé et le caractère unique est souhaité.

Afin que la génération cryptographique ne soit pas exigée par la même valeur de nonce, il est suggéré qu'une valeur de nonce acceptable puisse contenir une valeur DateTime et un UUID. Le nonce ne doit pas être réutilisé pour une clé quelconque et il convient que sa valeur soit aléatoire.

6.3.3 AccessControl

6.3.3.1 General

De par son caractère facultatif, l'élément AccessControl autorise la valeur zéro (0) et permet de spécifier un plus grand nombre d'informations sur l'accès au(x) document(s) intégré(s). Le type XSD pour AccessControl est représenté à la Figure 7.

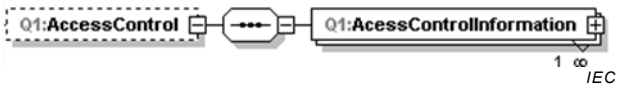


Figure 7 – Définition du type complexe XSD de l'élément AccessControl

L'élément AccessControl est une séquence XSD composée d'un ou de plusieurs éléments AccessControlInformation(s). Chaque AccessControlInformation est d'un type XSD d'AccessControlType, dont la structure est représentée à la Figure 8.

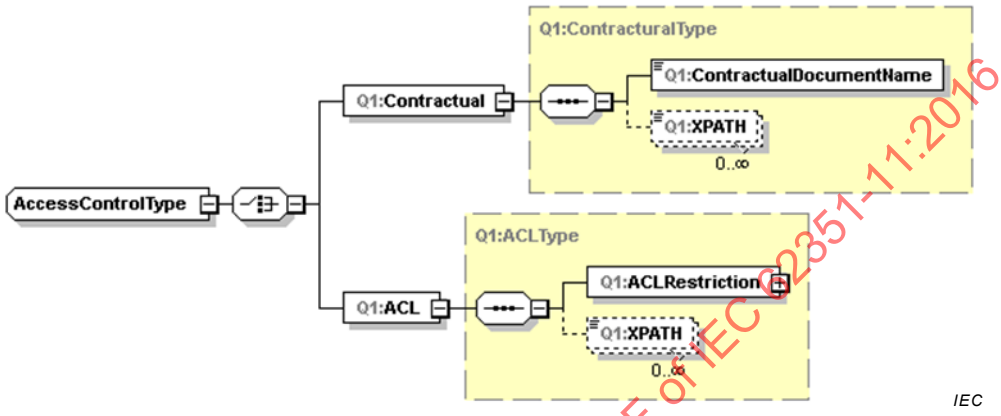


Figure 8 – Définition du type complexe XSD de l'élément AccessControlType

L'élément AccessControlType permet de choisir entre une restriction Contractual (par exemple, un document juridiquement contraignant) et la définition de l'équivalent d'une liste de contrôle d'accès (ACL). Chaque choix permet d'appliquer la gouvernance d'accès (par exemple, Contract ou ACLRestriction) à un ou plusieurs ensembles d'informations dans le document original intégré en utilisant une ou plusieurs déclarations XPATH.

Le choix Contractual est une séquence XSD composée des éléments définis dans le Tableau 4.

Tableau 4 – Définition des éléments Contractual et ACL

Élément	Facultatif (O) / Obligatoire (M) / Conditionnel (C)	Type XSD	Description
ContractualDocumentName	M	xs:normalizedString	Référence à un contrat juridique fournie par un utilisateur et contenant des informations relatives aux droits ou autorisations d'accès aux informations spécifiées dans les déclarations XPATH.
ACLRestriction	M	ACLRestriction Type (voir 6.3.3.2)	Une spécification complexe des droits d'accès qui permet d'indiquer l'autorisation ou le refus de certains types d'accès en fonction de rôles spécifiques. L'utilisation de l'élément ACLRestriction permet à l'utilisateur de spécifier l'équivalent des listes blanches ou noires.
XPATH	O	xs:normalizedString (voir 6.3.3.7)	Cet élément contient la valeur XPATH qui explicite les informations contenues dans le Body, pour lequel des lignes directrices sont données. Si aucune valeur XPATH n'est définie, le Body entier est pris en compte par hypothèse.

6.3.3.2 AccessRestrictionType

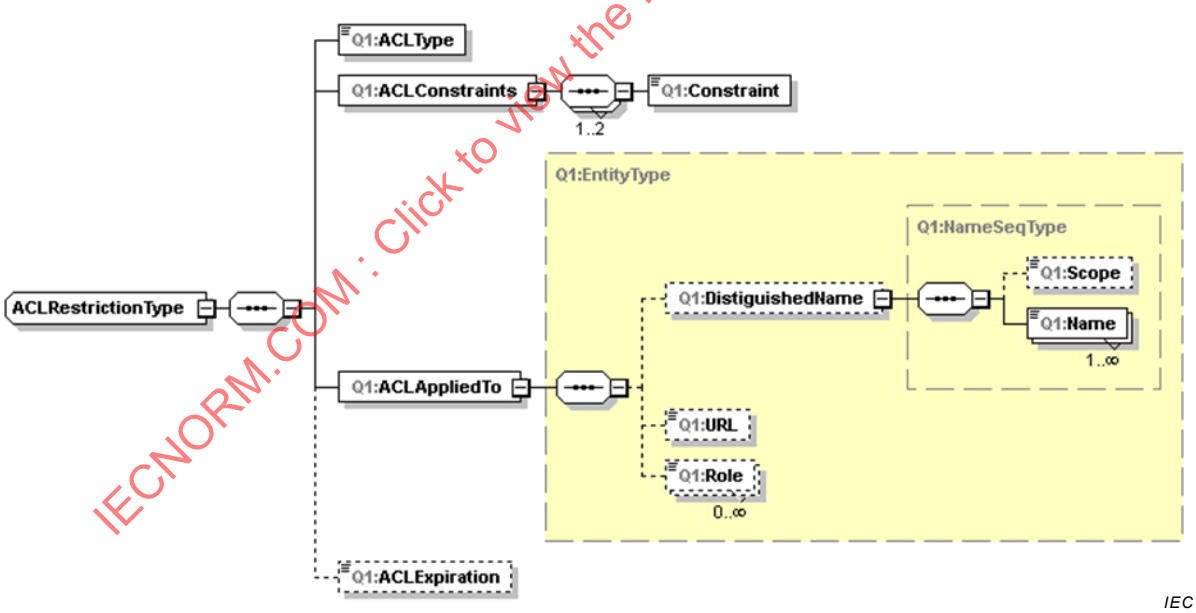


Figure 9 – Définition du type complexe XSD de l'élément ACLRestrictionType

La Figure 9 représente la structure de l'élément ACLRestrictionType. Il s'agit d'un type complexe XSD qui est une séquence des éléments XSD définis dans le Tableau 5.

Tableau 5 – Définition de l'élément ACLRestrictionType

Élément	Facultatif (O) / Obligatoire (M) / Conditionnel (C)	Type XSD	Description
ACLType	M	xs:string (voir 6.3.3.3)	Spécifie si la restriction d'accès est Allow ou Deny. De ce fait, les valeurs énumérées autorisées pour ACLType sont Allow et Deny.
ACLConstraints	M	Complex (voir 6.3.3.4)	Permet à l'utilisateur de spécifier une séquence de droits qui sont autorisés ou refusés. Cette capacité est assurée par une séquence d'éléments Constraint.
ACLAppliedTo	M	EntityType	Permet à l'utilisateur d'expliciter le type de définition utilisé pour indiquer l'entité à laquelle s'applique la liste de contrôle d'accès (ACL).
ACLExpiration	O	xs:dateTime	Spécifie la date et l'heure auxquelles le contrôle d'accès n'est plus exigé. Si la valeur n'est pas présente, la liste de contrôle d'accès n'expire pas.

Étant donné qu'il peut y avoir plusieurs listes de contrôle d'accès (ACL) dans un même document IEC 62351-11, une valeur ACLType de Deny doit prévaloir dans les situations où il existe à la fois des valeurs Constraint courantes et des valeurs ACLAppliedTo qui sont identiques ou se chevauchent.

6.3.3.3 ACLType

L'élément ACLType est un type xs:string dont les valeurs sont restreintes au moyen d'une énumération. Les définitions des valeurs énumérées autorisées ainsi que l'ordre de l'énumération sont présentés dans le Tableau 6.

Tableau 6 – Définition des valeurs énumérées pour ACLType

Valeur d'énumération	Définition
Allow	Indique que l'élément ACLRestrictionType est utilisé pour créer une liste blanche et que des privilèges sont accordés à l'élément ACLConstraints spécifié pour l'élément ACLAppliedTo spécifié.
Deny	Indique que l'élément ACLRestrictionType est utilisé pour créer une liste noire et que des privilèges sont refusés à l'élément ACLConstraints spécifié pour l'élément ACLAppliedTo spécifié.

6.3.3.4 ACLConstraints et Constraint

Les éléments ACLConstraints sont une séquence de valeurs Constraint, telles que présentées au Tableau 7.

L'élément Constraint est un type xs:string dont les valeurs sont restreintes au moyen d'une énumération. L'utilisation d'un ou de plusieurs éléments Contraint(s) est régie par l'élément ACLType.

Contrairement aux privilèges d'accès aux fichiers qui sont applicables, les valeurs Contraint indiquent la manière dont il convient de traiter les données en transition. Les valeurs sont présentées au Tableau 7.

Tableau 7 – Définition des valeurs énumérées pour Constraint

Valeur d'énumération	Définition
All	Indique que tous les privilèges de lecture (Read), d'écriture (Write) et d'énumération (List) sont spécifiés. Le privilège de lecture, s'il est autorisé, indique la capacité à fournir la valeur ou l'élément à une autre entité. Le privilège d'écriture, s'il est autorisé, indique la capacité d'une entité à modifier la valeur ou l'élément. Le privilège d'énumération, s'il est autorisé, indique la capacité d'une entité à déterminer si la valeur ou l'élément existe. Par conséquent, la valeur All est incompatible avec Read, Write, List et Forward. Si la valeur All est spécifiée dans une occurrence particulière de l'élément ACLConstraints, aucune autre valeur énumérée ne doit être utilisée à l'intérieur de cette séquence.
TransmitValue	La permission traduit la capacité de transmettre la valeur de l'information, spécifiée par XPATH, à une autre entité. La spécification de Read implique List. À titre d'exemple, un fournisseur serait en mesure de fournir l'information à un autre fournisseur si Allow était l'élément ACLType. Il s'agit de l'équivalent de Read et de List.
Write	La permission traduit la capacité d'autoriser la modification de la valeur de l'information spécifiée par XPATH.

6.3.3.5 EntityType

La Figure 10 représente la structure de l'élément EntityType.

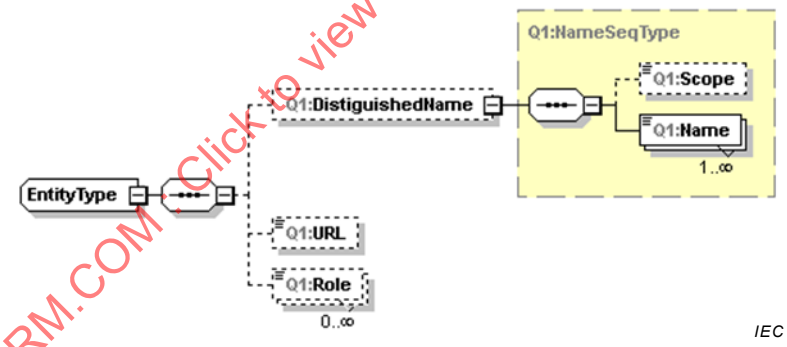


Figure 10 – Définition du type complexe XSD de l'élément EntityType

Il s'agit d'une séquence XSD qui autorise l'association de plusieurs spécifications d'entités afin de déterminer l'entité à laquelle la liste de contrôle d'accès (ACL) s'applique. Les éléments XSD définis dans EntityType sont présentés dans le Tableau 8.

Tableau 8 – Définition de l'élément EntityType

Élément	Facultatif (O) / Obligatoire (M) / Conditionnel (C)	Type XSD	Description
DistinguishedName	M	NameSeqType (voir 6.6.2)	Nom fourni et pouvant être utilisé par un utilisateur du document afin de savoir qui contacter (par exemple, une organisation ou une personne) et à qui il convient d'appliquer la liste de contrôle d'accès (ACL).
URL	M	xs:anyURI	Permet de spécifier une adresse web à laquelle il convient d'appliquer la liste de contrôle d'accès (ACL). Dans de nombreux cas, une organisation peut être désignée via une URL, ou il peut être nécessaire de restreindre l'accès à un site FTP particulier.
Role	O	xs:string (voir 6.3.3.6)	Est une valeur de chaîne qui spécifie le type de groupe sécurité/fonction auquel il convient d'appliquer la liste de contrôle d'accès (ACL).

L'ensemble des valeurs peut être utilisé pour limiter l'accès. À titre d'exemple, l'association de DistinguishedName et de Role peut servir à restreindre une liste de contrôle d'accès (ACL) à une fonction particulière dans le service donné d'une entreprise.

6.3.3.6 Role

L'élément Role est un type xs:string dont les valeurs sont restreintes au moyen d'une énumération. Les valeurs de chaîne admises sont définies conformément à l'IEC TS 62351-8.

6.3.3.7 XPATH

Cet élément contient la valeur XPATH qui explicite les informations contenues dans le Body, pour lequel des lignes directrices sont données. Si aucune valeur XPATH n'est spécifiée pour une contrainte donnée, la contrainte doit s'appliquer à l'ensemble de l'élément Body.

À titre d'exemple:

```
<?xml version="1.0" encoding="UTF-8"?>
<Q1:IEC62351-11 xmlns:n1="http://www.altova.com/samplexml/other-namespace" xmlns:Q1="http://www.iec.ch/2014/01/62351-11#"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:enc="http://www.w3.org/2001/04/xmlenc#"  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://www.iec.ch/2014/01/62351-11# file:///C:/Users/root/Desktop/IEC62351-11/IEC62351-11.xsd">
        <Q1:Header>
                <Q1:DateTimeOfEncapsulation>2014-04-14T21:32:52</Q1:DateTimeOfEncapsulation>
                <Q1:Filedesc>Example IEC 62351-11 non-encrypted file</Q1:Filedesc>
        </Q1:Header>
        <Q1:nonEncrypted>
                <Q1:Nonce>85343410947jgfa8312b!</Q1:Nonce>
                <Q1:AccessControl>
                  <Q1:AcessControlInformation>
                    <Q1:ACL>
                          <Q1:ACLRestriction>
                                <Q1:ACLType>Deny</Q1:ACLType>
                                <Q1:ACLConstraints>
                                                <Q1:Constraint>All</Q1:Constraint>
                                </Q1:ACLConstraints>
                                <Q1:ACLAppliedTo>
                                        <Q1:Role>Any</Q1:Role>
                                </Q1:ACLAppliedTo>
                        </Q1:ACLRestriction>
                        <Q1:XPATH>//cim:PowerTransformer[@rdf:ID='_T_Z0568311_Z0568422_1_24574']</Q1:XPATH>
                    </Q1:ACL>
                  </Q1:AcessControlInformation>
                </Q1:AccessControl>
                <Q1:Body>
                        <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"    xmlns:cim="http://iec.ch/TC57/2009/CIM-schema-cim14#">
                        <cim:PowerTransformer rdf:ID="_T_Z0568311_Z0568422_1_24574">
                          <cim:IdentifiedObject.name>UNKNOWN    </cim:IdentifiedObject.name>
                          <cim:Equipment.MemberOf_EquipmentContainer
                                rdf:resource="#_S_Z0568311Z0568422"/>
                        </cim:PowerTransformer>
                        <cim:BaseVoltage rdf:ID="_BS_9">
                          <cim:BaseVoltage.nominalVoltage>500</cim:BaseVoltage.nominalVoltage>
                                <cim:BaseVoltage.isDC>false</cim:BaseVoltage.isDC>
                          <cim:IdentifiedObject.name>500</cim:IdentifiedObject.name>
                        </cim:BaseVoltage>
                        <cim:SubGeographicalRegion rdf:ID="_Z_X">
```

```
                    <cim:IdentifiedObject.name>XX</cim:IdentifiedObject.name>
                    <cim:SubGeographicalRegion.Region rdf:resource="#_H_XX"/>
                  </cim:SubGeographicalRegion>
            <cim:ControlArea rdf:ID="_CA_X">
              <cim:IdentifiedObject.name>ControlArea_XX</cim:IdentifiedObject.name>
              <cim:ControlArea.netInterchange>0</cim:ControlArea.netInterchange>
              <cim:ControlArea.pTolerance>0</cim:ControlArea.pTolerance>
            </cim:ControlArea>
            <cim:Substation rdf:ID="_S_1000085110000721">
              <cim:IdentifiedObject.name>SUBSTATION_2</cim:IdentifiedObject.name>
              <cim:Substation.Region rdf:resource="#_Z_1"/>
            </cim:Substation>
                    </rdf:RDF>
            </Q1:Body>
      </Q1:nonEncrypted>
      <Q1:Signature>
            <ds:SignedInfo>
                  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-
                        c14n-20010315#WithComments"/>
                  <ds:SignatureMethod Algorithm="2001/04/xmldsig-more#hmac-sha256">
                        <ds:HMACOutputLength>128</ds:HMACOutputLength>
                  </ds:SignatureMethod>
                  <ds:Reference>
                  <ds:DigestMethod Algorithm="2001/04/xmldsig-more#sha384"></ds:DigestMethod>
                  <DigestValue>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK</DigestValue>
                  </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK</ds:SignatureValue>
            <ds:KeyInfo>
                  <ds:X509Data>
                  <ds:X509IssuerSerial>
                        <ds:X509SerialNumber></ds:X509SerialNumber>
                  </ds:X509IssuerSerial>
                  </ds:X509Data>
            </ds:KeyInfo>
      </Q1:Signature>
</Q1:IEC62351-11>
```

Figure 11 – Exemple de l'élément AccessControl et de la valeur XPATH

La Figure 11 représente trois exemples de l'élément AccessControl et l'utilisation de la valeur XPATH. L'exemple indique les contraintes sur les interdictions d'accès aux informations relatives à un transformateur de puissance particulier.

La valeur XPATH est une valeur qui ne doit contenir aucun des éléments de l'IEC 62351-11. Il doit s'agir d'une valeur XPATH qui est valable uniquement dans le document encapsulé. Cela a pour but de faciliter l'exécution de l'élément AccessControl en fonction de l'utilisation de XPATH par une application qui comprend la sémantique du document original.

À titre d'exemple, pour le document CIM représenté à la Figure 11, d'autres chaînes XPATH peuvent être utilisées pour contrôler l'accès à:

- l'ensemble du document: " //*"
- tous les postes: "//cim:Substation"
- un poste nommé SUBSTATION_2: "//cim:Substation/cim:IdentifiedObject.name['SUBSTATION_2']"

6.3.4 Body

Cet élément est l'élément d'encapsulation du document actuellement signé/chiffré. Le Body doit encapsuler un document XML qui ne doit pas contenir la valeur <?xml...>.

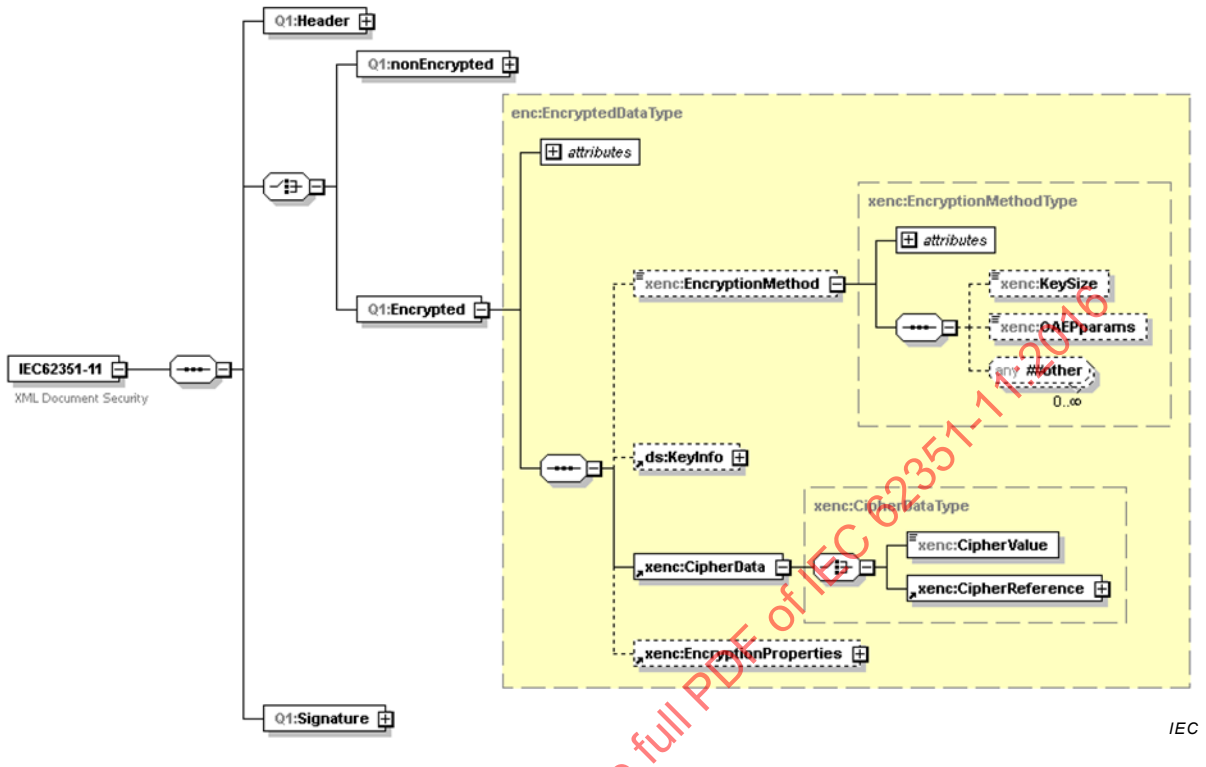
À titre d'exemple, si le Body contient un exemple de fichier CIM XML, il convient que la syntaxe de l'élément Body ressemble à peu de choses près à celle représentée à la Figure 12:

```
<Q1:Body>
        <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
        xmlns:cim="http://iec.ch/TC57/2009/CIM-schema-cim14#">
                <cim:PowerTransformer rdf:ID="_T_Z0568311_Z0568422_1_24574">
                        <cim:IdentifiedObject.name>UNKNOWN     </cim:IdentifiedObject.name>
                        <cim:Equipment.MemberOf_EquipmentContainer
                                rdf:resource="#_S_Z0568311Z0568422"/>
                </cim:PowerTransformer>
                <cim:BaseVoltage rdf:ID="_BS_9">
                        <cim:BaseVoltage.nominalVoltage>500</cim:BaseVoltage.nominalVoltage>
                                <cim:BaseVoltage.isDC>false</cim:BaseVoltage.isDC>
                        <cim:IdentifiedObject.name>500</cim:IdentifiedObject.name>
                </cim:BaseVoltage>
                <cim:SubGeographicalRegion rdf:ID="_Z_X">
                        <cim:IdentifiedObject.name>XX</cim:IdentifiedObject.name>
                        <cim:SubGeographicalRegion.Region rdf:resource="#_H_XX"/>
                </cim:SubGeographicalRegion>
                <cim:ControlArea rdf:ID="_CA_X">
                  <cim:IdentifiedObject.name>ControlArea_XX</cim:IdentifiedObject.name>
                  <cim:ControlArea.netInterchange>0</cim:ControlArea.netInterchange>
                  <cim:ControlArea.pTolerance>0</cim:ControlArea.pTolerance>
                </cim:ControlArea>
                <cim:Substation rdf:ID="_S_1000085110000721">
                  <cim:IdentifiedObject.name>SUBSTATION_2</cim:IdentifiedObject.name>
                  <cim:Substation.Region rdf:resource="#_Z_1"/>
                </cim:Substation>
        </rdf:RDF>
</Q1:Body>
```

Figure 12 – Exemple d'un Body de l'IEC 62351-11 avec un document CIM

6.4 Élément Encrypted

6.4.1 General



Anglais	Français
XML Document Security	Sécurité du document XML

Figure 13 – Structure de l'élément Encrypted de l'IEC 62351-11

L'élément Encrypted de l'IEC 62351-11 a la structure représentée à la Figure 13. La structure et l'élément EncryptedDataType sont définis par la spécification du W3C pour le Cryptage XML.

À des fins d'utilisation dans le contexte de l'IEC 62351-11, les contraintes suivantes doivent être appliquées au contenu de l'élément EncryptedDataType:

- L'attribut Type doit avoir une valeur de: http://www.w3.org/2001/04/xmlenc#Element.
- L'attribut MimeType ne doit pas être présent.
- L'attribut Encoding ne doit pas être présent.

6.4.2 EncryptionMethod

L'élément EncryptionMethod a la structure spécifiée par l'élément EncryptionMethodType du W3C, qui est représentée à la Figure 14. Cet élément est facultatif dans le contexte du W3C, mais doit être obligatoire pour l'IEC 62351-11.

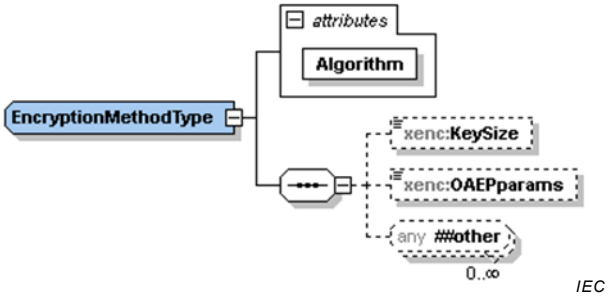


Figure 14 – Structure de l'élément EncryptionMethodType

L'élément facultatif EncryptionMethod doit être présent. Les valeurs doivent être telles que spécifiées par l'IANA (voir Article 8). Les valeurs admises de l'algorithme sont:

2009/xmlenc11#aes128-gcm
2009/xmlenc11#aes192-gcm
2009/xmlenc11#aes256-gcm

L'élément facultatif KeySize doit également être présent et avoir une valeur non-NULL/not-empty. *La prise en charge facultative des clés de 1 024 bits est prévue pour la compatibilité ascendante. Les clés de 2 048 bits doivent être prises en charge, cette longueur de clé étant à privilégier.*

L'élément OAEPparams n'est pas exigé en raison des algorithmes de chiffrement retenus pour l'IEC 62351-11 et ne doit donc pas être présent.

6.4.3 CipherData

L'élément CipherData a la structure spécifiée par l'élément CipherDataType du W3C, qui est représentée à la Figure 15.

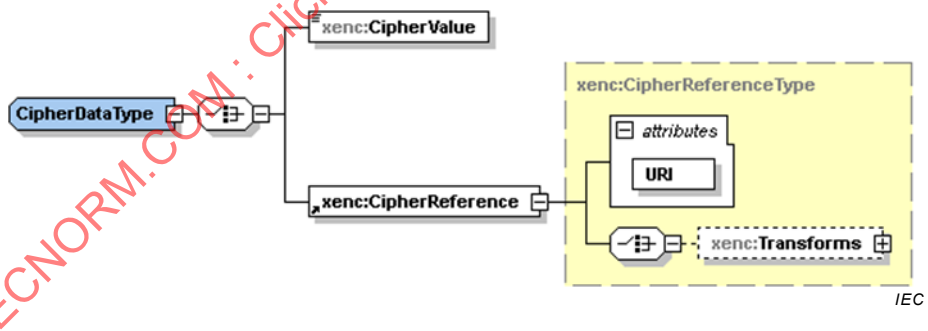


Figure 15 – Structure de l'élément CipherDataType

Dans le contexte de l'IEC 62351-11, seul l'élément CipherValue doit être utilisé.

L'élément CipherValue doit être la valeur produite par le chiffrement de l'élément EncryptedData. L'élément a la structure représentée à la Figure 16.

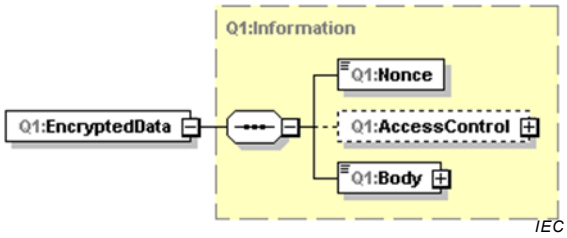


Figure 16 – Définition de l'élément EncryptedData

Le type Information est défini en 6.3.

6.4.4 KeyInfo

Si l'élément keyInfo n'est pas présent dans l'élément EncryptedDataType, les valeurs de l'élément Signature KeyInfo doivent alors être utilisées pour le chiffrement/déchiffrement.

Les contraintes de valeur sur l'élément EncryptionDataType KeyInfo sont les mêmes que pour l'élément Signature et sont définies en 6.5.2.5.

6.5 SignatureType

6.5.1 General

L'élément Signature est un type complexe de ds:SignatureType pour lequel le SignatureType est défini par le W3C.

Le schéma à utiliser est défini à l'adresse http://www.w3.org/2000/09/xmldsig#. La spécification actuelle de la Signature XML est disponible à l'adresse http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/.

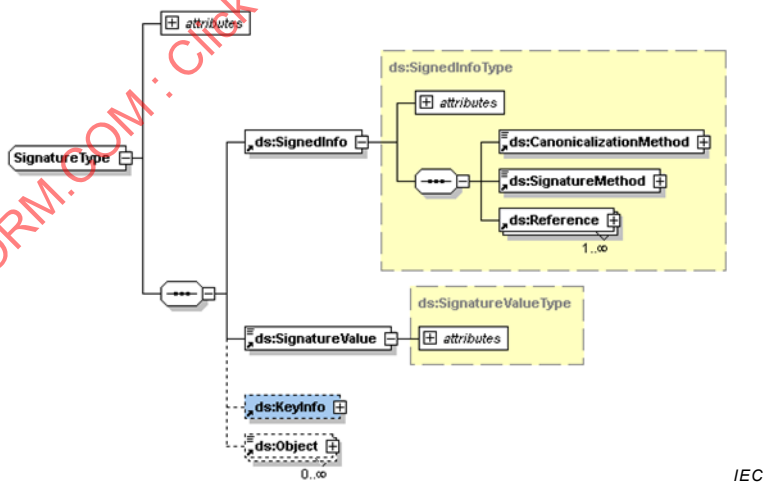


Figure 17 – Définition du SignatureType du W3C

La Figure 17 indique que la structure de l'élément Signature est définie comme le SignatureType du W3C. Le paragraphe 6.5 précise des contraintes d'usage supplémentaires de la structure et des éléments contenus dans la structure.

6.5.2 SignedInfoType

6.5.2.1 General

Les articles suivants donnent des informations détaillées sur les valeurs particulières qui peuvent être utilisées dans l'élément SignedInfoType dans le cas d'une utilisation pour l'IEC 62351-11. La structure de l'élément SignedInfoType est représentée à la Figure 18.

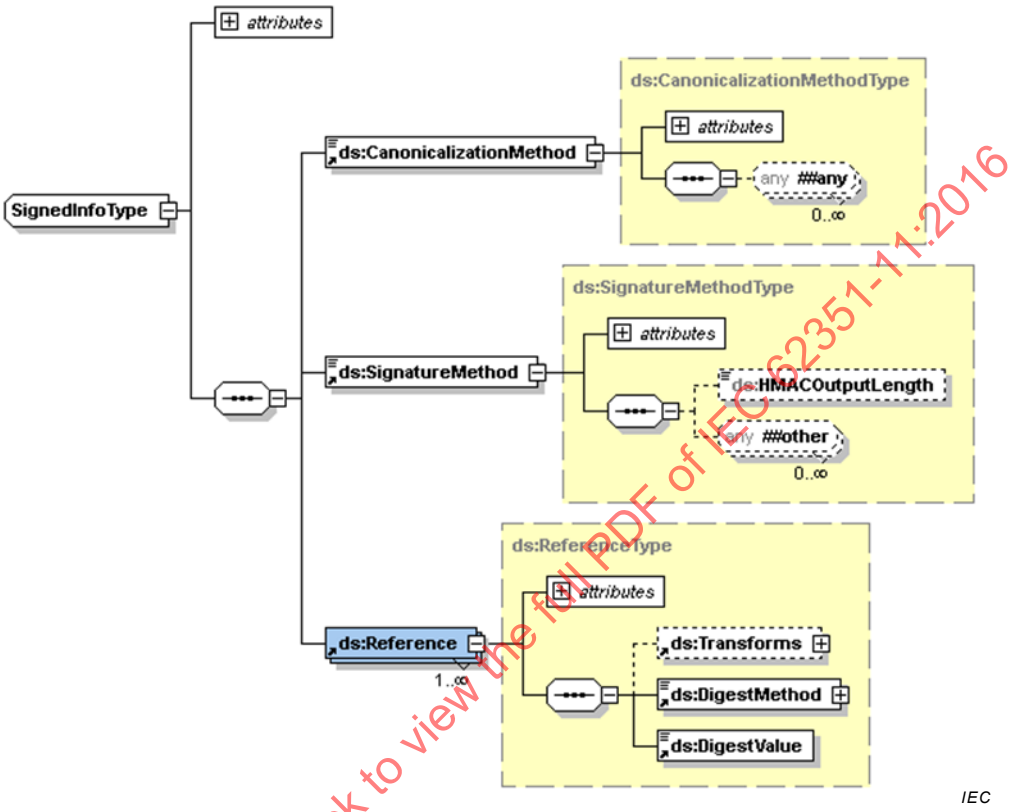


Figure 18 – Structure XML de l'élément SignedInfoType

6.5.2.2 CanonicalizationMethod

Le document du W3C sur la spécification de la signature présente une méthode de canonisation obligatoire et trois méthodes de canonisation recommandées. La méthode qui doit être utilisée est l'une des méthodes recommandées: http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments

Cette méthode doit également inclure les espaces blancs existants ainsi que les commentaires XML.

6.5.2.3 SignatureMethod

La structure définie de l'élément SignatureMethod est représentée à la Figure 19.

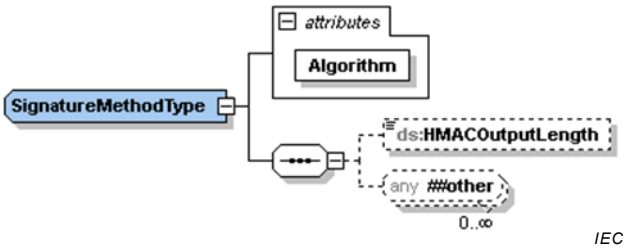


Figure 19 – Structure de l'élément SignatureMethodType

Bien que la norme W3C permette d'utiliser n'importe quel URI enregistré, la présente norme limite la liste autorisée aux éléments SignatureMethods enregistrés auprès de l'IANA (*http://www.iana.org/assignments/xml-security-uris/xml-security-uris.txt*).

De plus, il est exigé que seul ce qui suit soit pris en charge pour l'IEC 62351-11:

L'algorithme pour l'élément DigestMethod doit être l'un des suivants (conformément à la RFC 6931):

2001/04/xmldsig-more#hmac-sha256
2001/04/xmldsig-more#hmac-sha384
2001/04/xmldsig-more#hmac-sha512

Toutes les autres signatures ne relèvent pas du domaine d'application de la présente norme.

De plus, la valeur HMAC calculée peut être tronquée conformément aux prescriptions SHA-256 et SHA-512[2] de la recommandation RFC 2104. Les troncations autorisées sont 80, 128 et 256 bits. Ces valeurs sont les seules valeurs autorisées pour l'élément HMACOutputLength. Si l'élément HMACOutputLength n'est pas présent, la valeur HMAC doit être la taille maximale conformément à l'algorithme.

6.5.2.4 Reference

La structure définie de l'élément SignatureMethod est représentée à la Figure 20.

2 Conformément à la norme FPIS 180-4.