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

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@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

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

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.

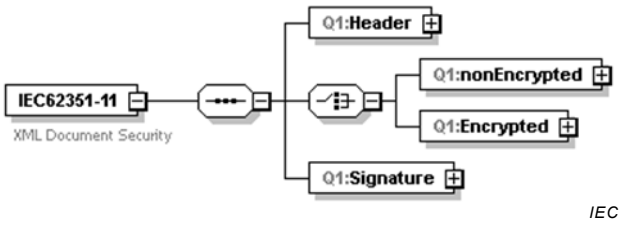

Figure 1 – Overview of IEC 62351-11 structure

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.

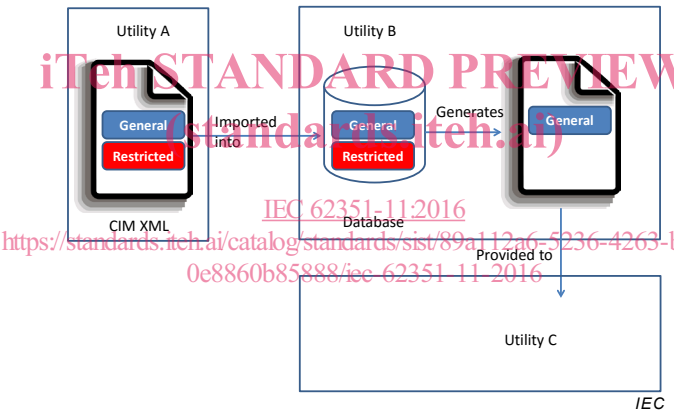

Figure 2 – Data in transition example

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.

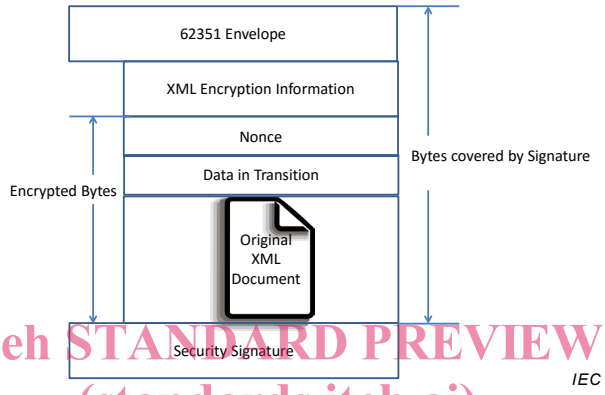

Figure 3 – Secure encapsulation for XML documents

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.

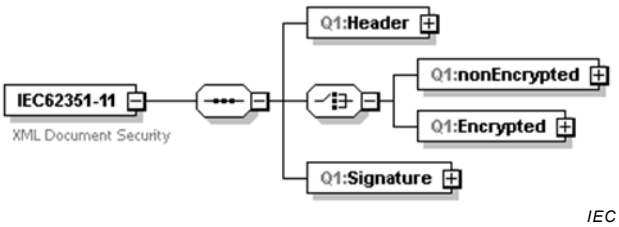

Figure 4 – General IEC 62351-11 XSD layout

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.

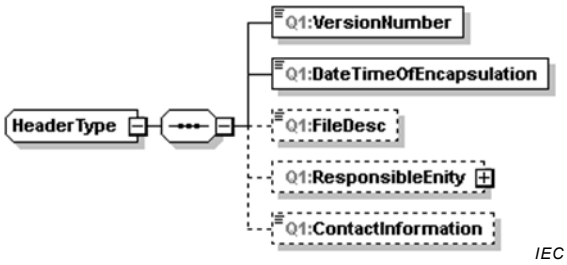

Figure 5 – XSD ComplexType definition of HeaderType

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.

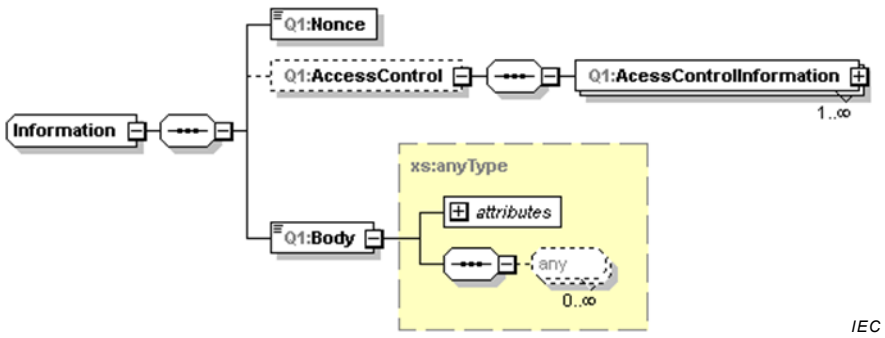

Figure 6 – XSD ComplexType definition of information

. 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.

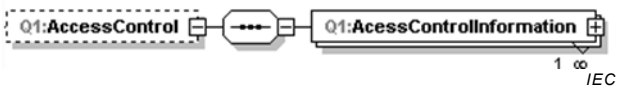

Figure 7 – XSD Complex Type Definition of AccessControl

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.