

DIN EN 62351-11



ICS 35.030; 35.240.50

**Energiemanagementsysteme und zugehöriger Datenaustausch –
IT-Sicherheit für Daten und Kommunikation –
Teil 11: Sicherheit für XML-Dateien
(IEC 62351-11:2016);
Englische Fassung EN 62351-11:2017**

Power systems management and associated information exchange –
Data and communications security –
Part 11: Security for XML documents
(IEC 62351-11:2016);
English version EN 62351-11:2017

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);
Version anglaise EN 62351-11:2017

Gesamtumfang 43 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2016-11-02 angenommene Europäische Norm als DIN-Norm ist 2017-10-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 62351-11:2015-02.

Für dieses Dokument ist das nationale Arbeitsgremium K 952 „Netzleittechnik“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom TC 57 „Power systems management and associated information exchange“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu dieser Publikation angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden Deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Das Präsidium des DIN hat mit Präsidialbeschluss 1/2004 festgelegt, dass DIN-Normen, deren Inhalt sich auf internationale Arbeitsergebnisse der Informationsverarbeitung gründet, unter bestimmten Bedingungen allein in englischer Sprache veröffentlicht werden dürfen. Diese Bedingungen sind für die vorliegende Norm erfüllt.

Da sich die Anwender der vorliegenden Norm der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der EN 62351-11 veröffentlicht. Zu deren Abschnitt 1, der den Anwendungsbereich festlegt, und deren Abschnitt 3, der die Begriffe festlegt, wurde eine Übersetzung angefertigt und als Nationaler Anhang NA der vorliegenden Norm hinzugefügt. Für einige der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Diese Norm steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Nationaler Anhang NA (informativ)

Auszugsweise Übersetzung^{N1)}

1 Anwendungsbereich

Dieser Teil der IEC 62351 legt Schemata, Verfahren und Algorithmen zur Gewährleistung der Sicherheit von XML-Dokumenten im Anwendungsbereich der IEC fest sowie von Dokumenten in anderen Bereichen (z. B. IEEE, proprietär usw.). Auf diesen Teil soll in anderen Normen Bezug genommen werden, wenn ein sicherer Datenaustausch erforderlich ist, es sei denn, die Parteien haben sich auf andere anerkannte sichere Austauschmechanismen geeinigt.

Dieser Teil der IEC 62351 berücksichtigt bekannte W3C-Sicherheitsstandards für XML-Dokumente und enthält Profile dieser Standards sowie Erweiterungen. Durch die IEC-62351-11-Erweiterungen kann Folgendes zur Verfügung gestellt werden:

- Kopf (en: Header): Der Kopf enthält Informationen, die für die Erstellung des sicheren Dokuments relevant sind, beispielsweise das Datum und die Uhrzeit der Erstellung von IEC 62351-11.
- Option der Verkapselung des Original-XML-Dokuments in ein verschlüsseltes (en: Encrypted) oder nicht verschlüsseltes (en: nonEncrypted) Format. Falls das verschlüsselte Format gewählt wird, bietet ein Mechanismus die Möglichkeit, die notwendige Information bereitzustellen, um die Verschlüsselung auf interoperative Art durchzuführen (EncryptionInfo).
- Zugangskontrolle (en: AccessControl): Mechanismus zur Bereitstellung der Zugangskontrollinformation in Bezug auf Informationen, die im Original-XML-Dokument enthalten sind.
- Körper (en: Body): enthält das Original-XML-Dokument, das verkapselt wird.
- Signatur (en: Signature): Signatur zum Zwecke der Authentifizierung und Manipulationserkennung.

Der allgemeine Aufbau ist in Bild 1 dargestellt.

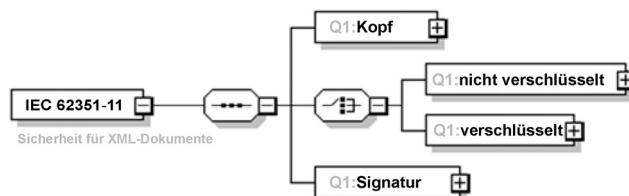


Bild 1 – Übersicht über den Aufbau von IEC 62351-11

Damit die in diesem Dokument beschriebenen Maßnahmen angewandt werden können, müssen sie in den Spezifikationen selbst anerkannt und referenziert werden. Dieses Dokument wurde erstellt, um diesen Prozess zu ermöglichen.

Die folgende Zielgruppe dieses Teils der IEC 62351 sind die Entwickler von Produkten, die diese Spezifikationen umsetzen.

Teile dieses Teils der IEC 62351 können auch Managern und Führungskräften dabei helfen, Zweck und Anforderungen der Arbeit zu verstehen.

^{N1)} Nationale Fußnote: Die Nummerierung aus IEC 62351-11:2016 wurde beibehalten.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC/TS 62351-2 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: unter <http://www.iso.org/obp>

3.1

Füllwert

(en: nonce)

Zufalls- oder Pseudozufallswert, der in einem Authentifikationssystem verwendet wird

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

3.2

IANA

Internet Assigned Numbers Authority

Anmerkung 1 zum Begriff: IANA ist verantwortlich für die globale Koordination der DNS-Root, IP-Addressing und anderen Internetprotokollquellen.

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

English Version

**Power systems management and associated information
exchange - Data and communications security - Part 11:
Security for XML documents
(IEC 62351-11:2016)**

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)

Energiemanagementsysteme und zugehöriger
Datenaustausch - IT-Sicherheit für Daten und
Kommunikation - Teil 11: Sicherheit für XML-Dateien
(IEC 62351-11:2016)

This European Standard was approved by CENELEC on 2016-11-02. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

The text of document 57/1753/FDIS, future edition 1 of IEC 62351-11, prepared by IEC/TC 57 "Power systems management and associated information exchange" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62351-11:2017.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2017-08-10
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2020-02-10

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62351-11:2016 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61850-6	NOTE	Harmonized as EN 61850-6.
IEC 61970-552	NOTE	Harmonized as EN 61970-552.
IEC 62351-1	NOTE	Harmonized as EN 62351-1.
IEC 62351-3	NOTE	Harmonized as EN 62351-3.

CONTENTS

European foreword	2
1 Scope.....	5
2 Normative references	6
3 Terms and definitions	6
4 Security issues addressed by this document	7
4.1 General.....	7
4.2 Security threats countered.....	7
4.3 Attack methods countered	7
5 XML Documents	7
6 XML document encapsulation	9
6.1 General.....	9
6.2 HeaderType	10
6.3 Information	11
6.3.1 General	11
6.3.2 Nonce.....	12
6.3.3 AccessControl.....	12
6.3.4 Body.....	19
6.4 Encrypted element	20
6.4.1 General	20
6.4.2 EncryptionMethod	20
6.4.3 CipherData	21
6.4.4 KeyInfo.....	22
6.5 SignatureType.....	22
6.5.1 General	22
6.5.2 SignedInfoType.....	23
6.6 Supporting XSD Types	26
6.6.1 General	26
6.6.2 NameSeqType	26
6.7 Security algorithm selection.....	27
7 Example files (informative).....	28
7.1 Non-encrypted example.....	28
7.2 Encrypted example.....	30
8 IANA list of signature, digest, and encryption methods (informative)	32
Bibliography	37
Annex ZA (normative) Normative references to international publications with their corresponding European publications.....	39
Figure 1 – Overview of IEC 62351-11 structure.....	5
Figure 2 – Data in transition example	8
Figure 3 – Secure encapsulation for XML documents.....	9
Figure 4 – General IEC 62351-11 XSD layout.....	9
Figure 5 – XSD ComplexType definition of HeaderType.....	10
Figure 6 – XSD ComplexType definition of information.....	11

Figure 7 – XSD Complex Type Definition of AccessControl	12
Figure 8 – XSD Complex Type definition of AccessControlType	13
Figure 9 – XSD Complex Type Definition of ACLRestrictionType.....	14
Figure 10 – XSD Complex Type definition of EntityType	16
Figure 11 – Example of AccessControl and XPATH	18
Figure 12 – Example of an IEC 62351-11 Body with a CIM document	19
Figure 13 – Structure of the IEC 62351-11 Encrypted element	20
Figure 14 – Structure of EncryptionMethodType	21
Figure 15 – Structure of CipherDataType	21
Figure 16 – EncryptedData element definition	22
Figure 17 – W3C SignatureType definition	22
Figure 18 – SignedInfotype XML structure.....	23
Figure 19 – SignatureMethodType structure	24
Figure 20 – ReferenceType structure	25
Figure 21 – KeyInfoType Structure.....	26
Figure 22 – Definition of NameSeqType	27
 Table 1 – Definitions of general structure for an IEC 62351-11 document.....	 10
Table 2 – Definition of HeaderType Element.....	11
Table 3 – Definition of information element.....	12
Table 4 – Definition of Contractual and ACL Element.....	13
Table 5 – Definition of ACLRestrictionType Element.....	14
Table 6 – Definition of Enumerated Values for ACLType.....	15
Table 7 – Definition of Enumerated Values for Constraint	15
Table 8 – Definition of EntityType Element.....	16

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.

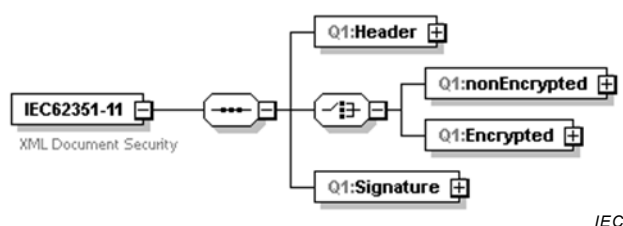


Figure 1 – Overview of IEC 62351-11 structure

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 XML 1.0 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 documents, the information contained in the document may:

- 1) be sensitive to inadvertent or malicious modifications of its contents that could result in misoperation/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.

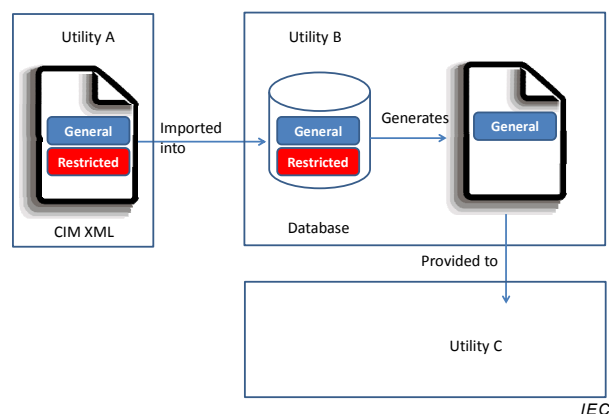


Figure 2 – Data in transition example

Figure 2 illustrates this potential problem with Data in Transition. Utility¹ 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.

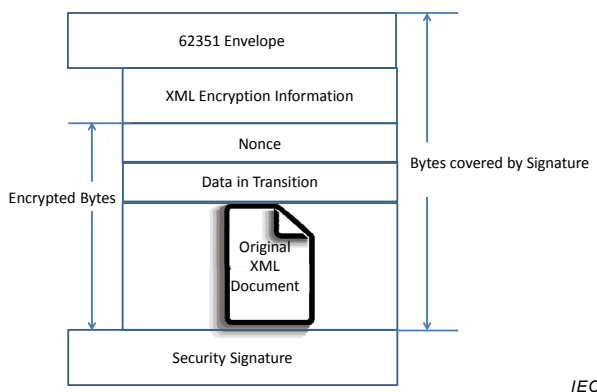


Figure 3 – Secure encapsulation for XML documents

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.

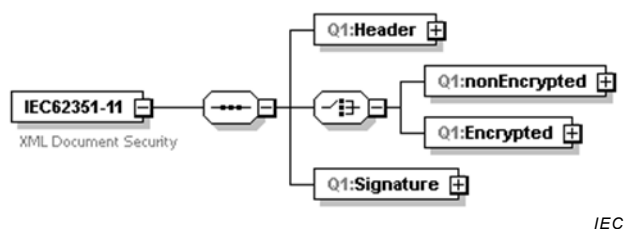


Figure 4 – General IEC 62351-11 XSD layout