

© Copyright SEK. Reproduction in any form without permission is prohibited.

Styrning av kraftsystem och tillhörande informationsutbyte – IT-säkerhet – Del 11: Specifikation av säkerhet för XML-dokument

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

Som svensk standard gäller europastandarden EN 62351-11:2017. Den svenska standarden innehåller den officiella engelska språkversionen av EN 62351-11:2017.

Nationellt förord

Europastandarden EN 62351-11:2017

består av:

- **europastandardens ikraftsättningsdokument**, utarbetat inom CENELEC
- **IEC 62351-11, First edition, 2016 - Power systems management and associated information exchange - Data and communications security - Part 11: Security for XML documents**

utarbetad inom International Electrotechnical Commission, IEC.

ICS 33.200.00

Denna standard är fastställd av SEK Svensk Elstandard,
som också kan lämna upplysningar om **sakinnehållet** i standarden.
Postadress: Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00.
E-post: sek@elstandard.se. Internet: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a mätning, säkerhet och provning och för utförande, skötsel och dokumentation av elprodukter och elanläggningar.

Genom att utforma sådana standarder blir säkerhetsfordringar tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard

Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

ICS 33.200

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.

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 62351-9	-	Power systems management and-associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment		-
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		-
IETF RFC 6931	-	Additional XML Security Uniform Resource-Identifiers (URIs)		-
W3C Recommended Canonical XML 1.0	-		-	-
W3C Required- Canonical XML1.0	-		-	-
W3C XML 1.1	-	Signature Syntax and Processing_-- Version 1.1		-
W3C Signature	XML-	XML Signature Syntax and Processing	-	-

CONTENTS

FOREWORD.....	4
1 Scope.....	6
2 Normative references	7
3 Terms and definitions	7
4 Security issues addressed by this document	8
4.1 General.....	8
4.2 Security threats countered.....	8
4.3 Attack methods countered	8
5 XML Documents	8
6 XML document encapsulation	10
6.1 General.....	10
6.2 HeaderType	11
6.3 Information	12
6.3.1 General	12
6.3.2 Nonce.....	13
6.3.3 AccessControl.....	13
6.3.4 Body.....	20
6.4 Encrypted element	21
6.4.1 General	21
6.4.2 EncryptionMethod	21
6.4.3 CipherData	22
6.4.4 KeyInfo	22
6.5 SignatureType.....	23
6.5.1 General	23
6.5.2 SignedInfoType.....	23
6.6 Supporting XSD Types	27
6.6.1 General	27
6.6.2 NameSeqType	27
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
Figure 1 – Overview of IEC 62351-11 structure.....	6
Figure 2 – Data in transition example	9
Figure 3 – Secure encapsulation for XML documents.....	10
Figure 4 – General IEC 62351-11 XSD layout.....	10
Figure 5 – XSD ComplexType definition of HeaderType.....	11
Figure 6 – XSD ComplexType definition of information.....	12
Figure 7 – XSD Complex Type Definition of AccessControl	13
Figure 8 – XSD Complex Type definition of AccessControlType	14
Figure 9 – XSD Complex Type Definition of ACLRestrictionType.....	15

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

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.

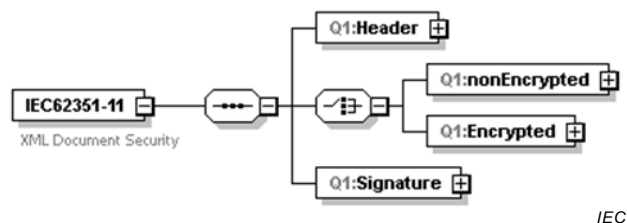


Figure 1 – Overview of IEC 62351-11 structure

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/>