



INTERNATIONAL STANDARD

NORME INTERNATIONALE



**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

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.

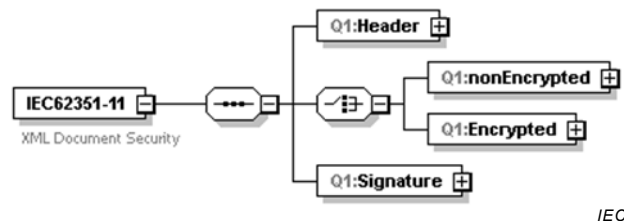


Figure 1 – Overview of IEC 62351-11 structure

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-xmlsig-core-20080610/>

SOMMAIRE

AVANT-PROPOS.....	42
1 Domaine d'application	44
2 Références normatives	45
3 Termes et définitions	45
4 Questions de sécurité abordées dans le présent document.....	46
4.1 Généralités	46
4.2 Contournement des menaces à la sécurité.....	46
4.3 Contournement des méthodes d'attaque	47
5 Documents XML	47
6 Encapsulation des documents XML.....	48
6.1 Généralités	48
6.2 HeaderType	50
6.3 Information	51
6.3.1 Généralités	51
6.3.2 Nonce.....	52
6.3.3 AccessControl.....	52
6.3.4 Body.....	60
6.4 Élément Encrypted	61
6.4.1 General	61
6.4.2 EncryptionMethod	61
6.4.3 CipherData	62
6.4.4 KeyInfo	63
6.5 SignatureType.....	63
6.5.1 General	63
6.5.2 SignedInfoType.....	64
6.6 Prise en charge des types XSD	67
6.6.1 General	67
6.6.2 NameSeqType	67
6.7 Choix de l'algorithme de sécurité	68
7 Exemples de fichiers (Informative)	69
7.1 Exemple de fichier non chiffré	69
7.2 Exemple de fichier chiffré	71
8 Liste des méthodes de signature, de résumé et de chiffrement de l'IANA (informative).....	73
Bibliographie	78
Figure 1 – Présentation de la structure de l'IEC 62351-11.....	44
Figure 2 – Exemple de données en transition	48
Figure 3 – Encapsulation sécurisée des documents XML	49
Figure 4 – Disposition XSD générale de l'IEC 62351-11.....	50
Figure 5 – Définition du type complexe XSD de l'élément HeaderType	51
Figure 6 – Définition du type complexe XSD de l'élément Information	52
Figure 7 – Définition du type complexe XSD de l'élément AccessControl.....	53
Figure 8 – Définition du type complexe XSD de l'élément AccessControlType	53

Figure 9 – Définition du type complexe XSD de l'élément ACLRestrictionType	54
Figure 10 – Définition du type complexe XSD de l'élément EntityType	56
Figure 11 – Exemple de l'élément AccessControl et de la valeur XPATH.....	59
Figure 12 – Exemple d'un Body de l'IEC 62351-11 avec un document CIM.....	60
Figure 13 – Structure de l'élément Encrypted de l'IEC 62351-11	61
Figure 14 – Structure de l'élément EncryptionMethodType.....	62
Figure 15 – Structure de l'élément CipherDataType	62
Figure 16 – Définition de l'élément EncryptedData.....	63
Figure 17 – Définition du SignatureType du W3C.....	63
Figure 18 – Structure XML de l'élément SignedInfoType	64
Figure 19 – Structure de l'élément SignatureMethodType	65
Figure 20 – Structure de l'élément ReferenceType	66
Figure 21 – Structure de l'élément KeyInfoType.....	67
Figure 22 – Définition de l'élément NameSeqType.....	68
Tableau 1 – Définitions de la structure générale pour un document IEC 62351-11	50
Tableau 2 – Définition de l'élément HeaderType.....	51
Tableau 3 – Définition de l'élément Information	52
Tableau 4 – Définition des éléments Contractual et ACL.....	54
Tableau 5 – Définition de l'élément ACLRestrictionType	55
Tableau 6 – Définition des valeurs énumérées pour ACLType.....	55
Tableau 7 – Définition des valeurs énumérées pour Constraint	56
Tableau 8 – Définition de l'élément EntityType	57

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

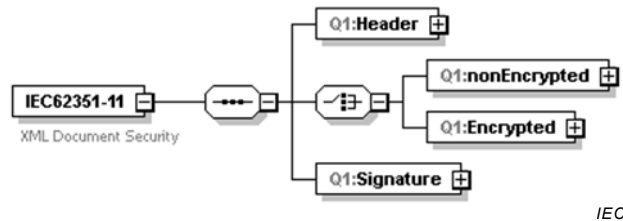
1 Domaine d'application

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 (nonEncrypted). Si le chiffrement est choisi, un mécanisme rend possible le chiffrement des informations exigées de manière interopérable (EncryptionInfo).
- AccessControl: mécanisme permettant d'explicitier 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-xmlsig-core-20080610/>