DEUTSCHE NORM **Entwurf** Februar 2015

DIN IEC 62351-11

DIN

ICS 35.040 Einsprüche bis 2015-03-16

Entwurf

Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation – Teil 11: Sicherheit für XML-Dateien (IEC 57/1496/CD:2014); Text in Englisch

Power systems management and associated information exchange – Data and communications security – Part 11: Security for XML Files (IEC 57/1496/CD:2014); Text in English

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2015-01-16 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 48 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Documents
Document Sharing Hub

Full document details: E DIN IEC 62351-11:2015-02

Nationales Vorwort

Die englische Originalfassung des internationalen Dokuments IEC 57/1496/CD:2014 „Power systems management and associated information exchange – Data and communications security – Part 11: Security for XML Files“ (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden.

Das internationale Dokument wurde vom TC 57 „Power systems management and associated information exchange“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

Die IEC und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf prEN nur 2 Monate beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

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.

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

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

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen 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.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO [und/oder] IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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 den vorliegenden Normentwurf erfüllt.

Da sich die Benutzer des vorliegenden Normentwurfs der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der EN 62351-11 veröffentlicht. Zu deren Abschnitt 1, 5, 6, 7, und 8 wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA des vorliegenden Normentwurfs hinzugefügt. Für viele der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Dieser Normentwurf steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Es ist vorgesehen, auch bei der entsprechenden zukünftigen Deutschen Norm auf die deutsche Sprachfassung zu verzichten und diese in der englischsprachigen Fassung zu veröffentlichen.

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.

Documents
Document Sharing Hub
Full document details: E DIN IEC 62351-11:2015-02

Nationaler Anhang NA
(informativ)

Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation – Teil 11: Sicherheit für XML-Dateien

1 Anwendungsbereich und Zweck

1.1 Anwendungsbereich

Dieser Teil der IEC 62351 legt Schemas, Prozeduren und Algorithmen zur Sicherheit von XML-Dokumenten, die in den Anwendungsbereich von IEC TC 57 fallen, sowie von Dokumenten in anderen Bereichen (z. B. IEEE, proprietär, usw.) fest. Diese Spezifikation gilt mindestens für die in Tabelle 1 genannten Normen.

Tabelle 1 – Normen im Anwendungsbereich von IEC TC 57

Nummer	Titel
IEC 61850-6	Kommunikationsnetze und -systeme für die Automatisierung in der elektrischen Energieversorgung – Teil 6: Sprache für die Beschreibung der Konfiguration für die Kommunikation in Stationen mit intelligenten elektronischen Geräten (IED)
IEC 61970-552	Schnittstelle für Anwendungsprogramme für Netzführungssysteme (EMS-API) – Teil 552: CIM-XML-Modell Austauschformat

Das XML-Dokument und Endungen werden in dieser Norm festgelegt. Die in dieser Spezifikation festgelegten Endungen sind:

- Header (Kopf): Der Header enthält relevante Informationen zur Verkapselung, wie z. B. Datum und Zeit der Verkapselung (z. B. Dateierstellung).
- Option der Verkapselung des Original-XML-Dokuments in ein verschlüsseltes (chiffriertes) oder nicht verschlüsseltes (nicht chiffriertes) Format. Falls die Verschlüsselung gewählt wird, bietet ein Mechanismus die Möglichkeit, die notwenige Information bereitzustellen, um die Verschlüsselung auf interoperative Art durchzuführen (EncryptionInfo).
- AccessControl (Zugangskontrolle): Mechanismus zur Bereitstellung der Zugangskontrollinformation in Bezug auf Informationen, die im Original-XML-Dokument enthalten sind.
- Body (Körper): enthält das Original-XML-Dokument, das verkapselt wird.
- Signature (Unterschrift): Unterschrift zum Zwecke der Authentifizierung und Manipulationserkennung.

Der allgemeine Aufbau ist in Bild 1 dargestellt.

Documents
Document Sharing Hub

Full document details: E DIN IEC 62351-11:2015-02

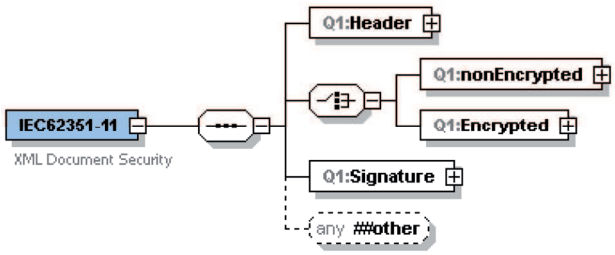


Bild 1 – Übersicht über den Aufbau von 62351-11

1.2 Zweck

Zielgruppe dieser Spezifikation sind in erster Linie die Mitglieder der Arbeitsgruppen, welche die in Tabelle 1 genannten Normen erarbeiten oder anwenden. Damit die in dieser Spezifikation beschriebenen Maßnahmen wirksam werden, müssen sie in den genannten Spezifikationen anerkannt und referenziert werden. Dazu soll das vorliegende Dokument beitragen.

Die anschließenden Anwender dieser Spezifikation sollen die Produktentwickler sein, die diese Normen umsetzen.

Teile dieser Spezifikation sind möglicherweise auch nützlich für Manager und Führungskräfte zum Verständnis von Zweck und Anforderungen der Arbeit.

5 Durch diese Spezifikation adressierte Sicherheitsfragen

Der XML-Dateiaustausch verbreitet sich innerhalb der Industrie und TC57 immer weiter. Innerhalb des Anwendungsbereichs von TC 57 wird der Austausch von XML-Dateien für IEC 61970 und IEC 61850 verwendet. XML wird auch innerhalb anderer Normen, IEEE 1815 und IEEE C37.111 (COMTRADE), angewandt. Die in den Dateien enthaltenen Informationen dürfen für diese Normen und für andere auf XML basierende Dateien:

1) sensibel gegenüber unbeabsichtigten oder böswilligen Änderungen ihrer Inhalte sein, die bei Verwendung der ausgetauschten Informationen zu Fehlfunktion/Fehlinterpretation führen könnte (z. B. eine Anfälligkeit der Sabotagesicherheit);
2) vertrauliche oder private Daten enthalten;
3) Informationsuntermengen enthalten, die durch die Dateierzeugungseinheit möglicherweise als kritisch erachtet werden.

Das Arbeitsprogramm schlägt vor, Mechanismen zu normieren, um die Dokumenteninhalte beim Dateiaustausch (z. B. beim Transit) und im Ruhezustand (z. B. gespeichert auf einem Computer) vor Sabotage/Offenlegung zu schützen. Zusätzlich schlägt das Arbeitsprogramm vor, Mechanismen zu normen, um beim Schutz der Informationen zu helfen, wenn sich diese in Überleitung befinden (z. B Einheit A vertraut Einheit B; B vertraut A und C und B muss Informationen mit C austauschen. Aber A weiß weder von C noch vertraut C.).

Obwohl dieses Dokument dafür gedacht ist, XML-Dokumente, die im Anwendungsbereich von IEC TC57 verwendet werden, zu schützen, können die Mechanismen/Methodologien, die in diesem Dokument festgelegt werden, auf jedes XML-Dokument angewandt werden.

5.1 Betriebsfragen, die sich auf die Wahl der Sicherheitsoptionen auswirken

5.2 Sicherheitsbedrohungen, denen entgegengewirkt wird

Siehe IEC 62351-1 für eine Diskussion zu Sicherheitsbedrohungen und Angriffsverfahren.

Falls keine Verschlüsselung eingesetzt wird, dann beinhalten die speziellen Bedrohungen, denen in diesem Teil entgegengewirkt wird:

Documents
Document Sharing Hub
Full document details: E DIN IEC 62351-11:2015-02

– unautorisierte Veränderung (Sabotage) der Informationen durch Authentifizierung auf XML-Dokumentenebene.

Falls Verschlüsselung eingesetzt wird, dann beinhalten die speziellen Bedrohungen, denen in diesem Teil entgegengewirkt wird:

– unautorisierter Zugriff auf die Informationen durch Authentifizierung auf XML-Dokumentenebene und Verschlüsselung der Dokumente;
– unautorisierte Veränderung (Sabotage) der Informationen durch Authentifizierung auf XML-Dokumentenebene.

5.3 Angriffsverfahren, denen entgegengewirkt wird

Es ist vorgesehen, dass den folgenden Sicherheitsangriffsverfahren durch die entsprechende Implementierung, der in diesem Dokumente vorgefundenen Spezifikation/Empfehlungen, entgegengewirkt wird:

– Mittelsmann (en: man-in-the-middle): Dieser Bedrohung wird durch Benutzung eines Mechanismus mit Nachrichtenauthentifizierungscode (z. B. Signatur) entgegengewirkt, der in diesem Dokument festgelegt ist;
– Sabotageerkennung/Nachrichtenintegrität: Diesen Bedrohungen wird durch Algorithmen entgegengewirkt, die verwendet werden, um den Authentifizierungsmechanismus zu erzeugen, der in diesem Dokument festgelegt ist;
– Wiedereinspielung (en: replay): Dieser Bedrohung wird durch Benutzung spezialisierter Prozessierungs-Zustandsmaschinen entgegengewirkt, die in diesem Dokument festgelegt sind.

6 XML-Dokumente

Um angemessene Sicherheit zu bieten, muss es ein Verständnis der verwendeten Umgebung geben, die diese Spezifikation adressiert:

– Dokumente im Ruhezustand: Die Sabotageerkennung ist eine Minimalanforderung, wenn XML-Dokumente gespeichert werden (z. B. im Ruhezustand). Wenn das Dokument kritische Informationen enthält, dann muss die Vertraulichkeit dieser Informationen durch Verwendung von Verschlüsselung geschützt werden. Um beide Ziele zu erreichen, bedeutet dies, dass das nicht-verschlüsselte Dokument eine Signatur benötigt, und dass das verschlüsselte Dokument ebenfalls seine eigene Signatur/seinen eigenen Integritätsschutz benötigt.
– Dokumente im Transit: Der Schutz von Dokumenten im Transit ist derselbe wie bei Dokumenten im Ruhezustand, mit dem Zusatz des ergänzten Bedarfs, um zu bestimmen, ob das Dokument bereits zuvor ausgeliefert wurde (z. B. Wiedereinspielungsschutz). Um diesen zusätzlichen Schutz zu bieten, ist ein Einmalwert (en: nonce) bereitzustellen. Dieser Einmalwert könnte im originalen XML-Dokument sein oder durch einen Mechanismus dieser Spezifikation bereitgestellt werden.
– Dokumente in Überleitung: In der Domäne des TC57 entschlüsseln und parsen die Empfänger von XML-Dokumenten die Informationen dieser Dokumente typischerweise in eine Datenbank. Die Informationen aus dieser Datenbank können dann durch einen dritten Akteur in jeglicher Form (einschließlich ein anderes XML-Dokument) erneut exportiert werden. Wenn im ursprünglichen Dokument kritische oder vertrauliche Informationen bereitgestellt wurden, gibt es keinen technologischen Mechanismus, der die Anwendung daran hindert, diese Informationen zu exportieren.

Ein echter TC57-Beispielanwendungsfall ist die Übertragung von Topologieinformationen eines Elektrizitätsversorgungssystems unter Anwendung der IEC 61970-552.

Documents
Document Sharing Hub
Full document details: E DIN IEC 62351-11:2015-02

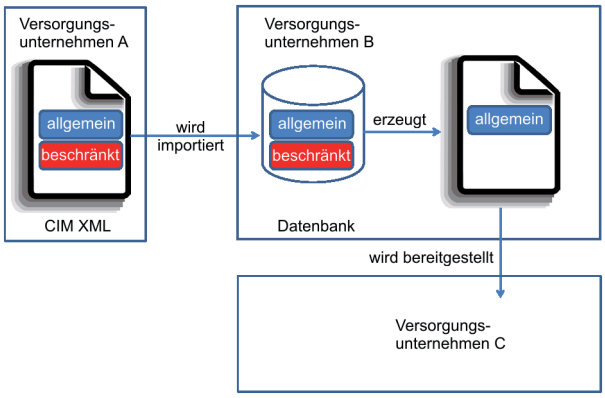


Bild 2 – Beispiel für Datenüberleitung

In Bild 1 wird dieses potentielle Problem anhand der Datenüberleitung verdeutlicht. Versorgungsunternehmen[1)] A stellt Versorgungsunternehmen B ein CIM-XML-Dokument zur Verfügung. Die Datei enthält die Informationen, die zwischen Versorgungsunternehmen A und Versorgungsunternehmen B, aufgrund des Vertrauens/der Vereinbarungen zwischen diesen Versorgungsunternehmen, ausgetauscht werden müssen. Versorgungsunternehmen B importiert die Informationen in seine Datenbank (z. B. EMS). Es muss dann ein separater Informationsaustausch zwischen Versorgungsunternehmen B und Versorgungsunternehmen C erfolgen. Versorgungsunternehmen A hat möglicherweise kein Wissen darüber, dass eine solche Übertragung erforderlich ist, und dass einige der „beschränkten“ Informationen möglicherweise durch den Export durch Versorgungsunternehmen B gefährdet sind. Das Ziel des hier empfohlenen Ansatzes zur Behandlung der Daten-in-Überleitung ist es, es Versorgungsunternehmen A zu ermöglichen, spezifische Dokumenteninhalte als kritisch oder vertraulich zu klassifizieren und zu markieren; die daher nicht erneut an andere Partner des Versorgungsunternehmens B exportiert werden.

Es ist anzumerken, dass das hier beschriebene Signieren von Dokumenten für diesen Zweck nicht ausreichend ist, da Versorgungsunternehmen B rechtmäßigen Zugriff auf den beschränkten Inhalt hat, und demnach die Fähigkeit hat, diesen für den Import in eine Anwendungsdatenbank zu entschlüsseln. Daher muss eine andere Lösung zur Verfügung gestellt werden – und zwar der unten in Abschnitt 7.2.2 beschriebene vertragliche Zugriffskontrollmechanismus.

Im Kontext von IEC TC57 gibt es wenigsten zwei wohlbekannte XML-Dokumententypen, die Schutz erfordern: CIM-XML- und SCL-Dateien. Diese Dateien haben wohlgeformte XSDs/Formate. Die in dieser Norm festgelegten Mechanismen sind als solche dafür gedacht, es den Dokumentformaten zu ermöglichen, erhalten zu bleiben. Daher ist die Verkapselung der Originaldokumente der Entwurfsansatz.

[1)] Aktoren in diesen Szenarien sind nicht auf Versorgungsunternehmen beschränkt, sondern dürfen auch RTOs, Börsen/Marktportale, Kundenprogrammvermittler, usw. sein.

Documents
Document Sharing Hub
Full document details: E DIN IEC 62351-11:2015-02

7 Verkapselung von XML-Dokumenten

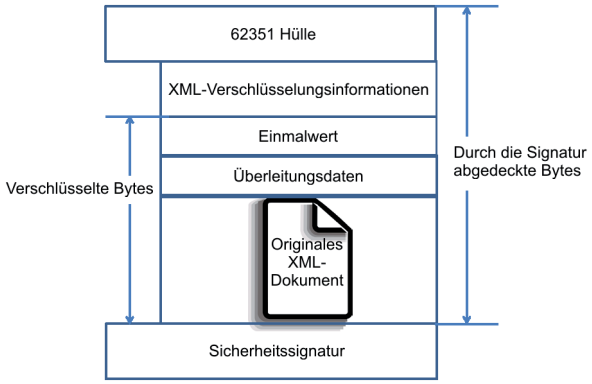


Bild 3 – Sicherheitsverkapselung von XML-Dokumenten

In Bild 2 wird das Konzept der Sicherheitsverkapselung von XML-Dokumenten dargestellt. Das Konzept ist es, die zuvor normierten XML-Sicherheitstechniken zu verwenden, um einen Sicherheitsheader, eine Signatur und die Fähigkeit zur Dokumentenverschlüsselung bereitzustellen. Das originale XML-Dokument und durch diese Norm festgelegte Erweiterungen befinden sich innerhalb des „sicheren“ Dokumentes. Die 62351-11-Erweiterungen weisen die Fähigkeit auf, folgendes bereitzustellen:

– Header: der Header enthält Informationen, die für die Verkapselung relevant sind wie beispielsweise das Datum und die Uhrzeit der Verkapselung (z. B. Dateierzeugung);

– eine Wahl, ob das originale XML-Dokument in einem verschlüsselten (verschlüsselt, en: Encrypted) oder nicht-verschlüsselten (nicht-verschlüsselt, en: nonEncrypted) Format verkapselt wird. Wenn die Verschlüsselung gewählt wird, ist ein Mechanismus bereitzustellen, um die erforderlichen Informationen auszudrücken, um die Verschlüsselung tatsächlich auf interoperable Weise durchzuführen (Verschlüsselungsinformationen, en: EncryptionInfo).

– Zugriffskontrolle: ein Mechanismus, um Zugriffskontrollinformationen in Bezug auf die im originalen XML-Dokument enthaltenen Informationen auszudrücken;

– Körper (Body): wird verwendet, um das originale XML-Dokument, das verkapselt wird, zu enthalten;

– Signatur: eine Signatur, die für Authentifizierungszwecke und zur Sabotageerkennung verwendet werden kann.

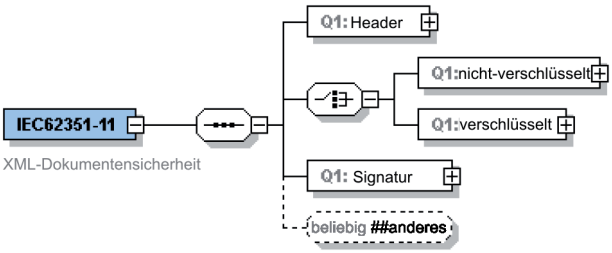


Bild 4 – Allgemeines IEC 62351-11-XSD-Layout

In Bild 3 wird die allgemeine XSD-Struktur eines IEC 62351-11-Dokumentes dargestellt. Die Definitionen können in Tabelle 2 gefunden werden.

Documents
Document Sharing Hub
Full document details: E DIN IEC 62351-11:2015-02

Tabelle 2: Definitionen der allgemeinen Struktur der Elemente einer IEC 62351-11-Datei

Element	Wahlfrei (O)/ Vorgeschrieben (M)/ Abhängig (C)	XSD-Typ	Beschreibung
Header	M	Header-Typ (en: HeaderType) (siehe Abschnitt 7.1)	Der Header enthält Informationen, die mit der Erzeugung der Datei in Bezug stehen, und Kontaktinformationen, sollten sich Fragen oder Probleme bezüglich der Datei ergeben.
nicht-verschlüsselt (en: nonEncrypted)	C	Informationen (siehe Abschnitt 7.2)	Bietet Zugriffskontrolle und das Verpacken des originalen Dokumentes in ein nicht-verschlüsseltes Dokument (z. B. können die Inhalte des originalen Dokuments immer noch gesehen werden). Diese Wahlmöglichkeit sollte von einem Anwender genutzt werden, sollte die Vertraulichkeit der Informationen nicht von Belang sein, oder falls die Vertraulichkeit durch einen externen Mechanismus geboten wird. Es darf entweder das XSD-Element nicht-verschlüsselt (en: nonEncrypted) oder verschlüsselt (en: Encrypted) vorliegen.
verschlüsselt (en: Encrypted)	C	Verschlüsselungs-Typ (en: EncryptedType) (siehe Abschnitt 7.3)	Bietet Verschlüsselung der Zugriffskontrolle und das Verpacken des originalen Dokumentes. Diese Wahlmöglichkeit sollte von einem Anwender genutzt werden, sollte die Vertraulichkeit der Informationen gewünscht sein, und falls die Vertraulichkeit nicht durch einen externen Mechanismus geboten wird. Es darf entweder das XSD-Element nicht-verschlüsselt (en: nonEncrypted) oder verschlüsselt (en: Encrypted) vorliegen.
Signatur	M	xs:string	Ist eine vom Anwender bereitgestellte Zeichenkette (en: string), die Telefon- oder E-Mail-Informationen enthalten darf, die von einem Dateianwender verwendet werden könnten, sollten Probleme oder Fragen auftreten.
beliebig (en: any)	O	anderes (en: other)	Ermöglicht zukünftige Erweiterungen während die Abwärtskompatibilität bewahrt wird.

8 Schutz von nicht-XML-Dokumenten

Obwohl die IEC 62351-11 primär dafür gedacht ist, Schutz für XML-Dokumente zu bieten, dokumentiert dieser Abschnitt, wie sie verwendet werden kann, um nicht-XML-Dokumente zu schützen. Um nicht-XML-Dokumente zu schützen, muss das nicht-XML-Dokument in einen XML-Elementwert kodiert werden, sodass die normale IEC 62351-11-Verarbeitung stattfinden kann.

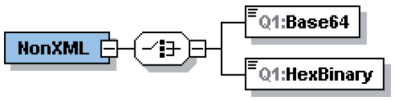


Bild 22 – Verpackungselement für nicht-XML-Dokumente

Es muss das Element NonXML verwendet werden. Die in Bild 21 dargestellte Struktur von NonXML, ermöglicht es der nicht-XML-Datei entweder als Base64 oder HexBinary kodiert zu werden. Der Schutz von nicht-XML-Dokument bedeutet jedoch, dass die Nebenbedingungen der XPATH-Zugriffskontrolle sehr viel Granularität verlieren. Die XPATH-Ausdrücke können nur noch wirklich auf den gesamten Inhalt der nicht-XML-Datei angewandt werden.

Documents
Document Sharing Hub
Full document details: E DIN IEC 62351-11:2015-02

CONTENTS

1 Scope and object 6
1.1 Scope 6
1.2 Object 7
2 Normative references 7
Additional XML Security Uniform Resource Identifiers (URIs) 7
3 Informative References 7
4 Definitions 8
5 Security issues addressed by this specification 8
5.1 Operational issues affecting choice of security options 8
5.2 Security threats countered 8
5.3 Attack methods countered 8
6 XML Documents 9
7 XML Document Encapsulation 10
7.1 HeaderType 12
7.2 Information 12
7.2.1 Nonce 14
7.2.2 AccessControl 14
7.2.3 Body 20
7.3 Encrypted Element 21
7.3.1 EncryptionMethod 22
7.3.2 CipherData 22
7.3.3 KeyInfo 23
7.4 SignatureType 24
7.4.1 SignedInfoType 24
7.5 Supporting XSD Types 28
7.5.1 NameSeqType 28
8 Protection of non-XML documents 28
9 Example Files (Informative) 2
9.1 Non-Encrypted Example 2
9.2 Encrypted Example 2
10 IANA List of Signature, Digest, and Encryption Methods (Informative) 2
11 Bibliography (Informative) 8

Figure 1: Data in Transition Example 9
Figure 2: Secure Encapsulation for XML Documents 10
Figure 3: General IEC 62351-11 XSD Layout 11
Figure 4: XSD ComplexType Definition of HeaderType 12
Figure 5: XSD ComplexType Definition of Information 13
Figure 6: XSD Complex Type Definition of AccessControl 14
Figure 7: XSD Complex Type Definition of AccessControlType 15
Figure 8: XSD Complex Type Definition of ACLRestrictionType 16
Figure 9: XSD Complex Type Definition of EntityType 17
Figure 10: Example of AccessControl and XPATH 20
Figure 11: Example of an IEC 62351-11 Body with a CIM file 21

DRAFT
AVA Documents Document Sharing Hub
Full document details: E DIN IEC 62351-11:2015-02

Figure 12: Structure of the IEC 62351-11 Encrypted Element 21
Figure 13: Structure of EncryptionMethodType 22
Figure 14: Structure of CipherDataType 22
Figure 15: EncryptedData Element Definition 23
Figure 16: W3C SignatureType Definition 24
Figure 17: SignedInfotype XML structure 25
Figure 18: SignatureMethodType Structure 25
Figure 19: ReferenceType Structure 26
Figure 20: KeyInfoType Structure 27
Figure 21: Wrapping Element for Non-XML documents 28

Table 1 – Scope of application to standards 6
Table 2: Definitions of general structure for an IEC 62351-11 file Elements 11
Table 3: Definition of HeaderType Elements 12
Table 4: Definition of Information Elements 14
Table 5: Definition of Contractual and ACL Elements 15
Table 6: Definition of Elements of ACLRestrictionType 16
Table 7: Definition of Enumerated Values for ACLType 17
Table 8: Definition of Enumerated Values for Constraint 17
Table 9: Definition of Elements of EntityType 18
Table 10: Definition of Enumerated Values for Role 19

DRAFT

Documents
Document Sharing Hub
Full document details: E DIN IEC 62351-11:2015-02

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 11: Security for XML files

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.

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.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62351-11, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

DRAFT

AVA Documents
Document Sharing Hub
Full document details: E DIN IEC 62351-11:2015-02

126 The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
57/805/DTS	57/859/RVC

127
128 Full information on the voting for the approval of this technical specification can be found in
129 the report on voting indicated in the above table.

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

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

134 The committee has decided that the contents of this publication will remain unchanged until
135 the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the
136 data related to the specific publication. At this date, the publication will be

137 • transformed into an International standard,
138 • reconfirmed,
139 • withdrawn,
140 • replaced by a revised edition, or
141 • amended.

142 A bilingual version of this publication may be issued at a later date.

143 **Document history**

144 Any person intervening in the present document is invited to complete the table below before
145 sending the document elsewhere. The purpose is to allow all actors to see all changes
146 introduced and the intervening persons.

147 Any important message to IEC editors should also be included in the table below.

Name of intervening person	Document received		Brief description of the changes introduced	Document sent	
	From	Date		To	Date
Margareta Nöth	Herbert Falk	2014-07-25	CD document	CO	2014-07-28

148

149 This table will be removed by IEC editors before FDIS circulation (in case of IS) or before final
150 publication (in case of TS or TR).

151

DRAFT

Documents
Document Sharing Hub
Full document details: E DIN IEC 62351-11:2015-02

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

Part 11: Security for XML files

1 Scope and object

1.1 Scope

This part of IEC 62351 specifies schema, procedures, and algorithms for securing XML documents that are used within the scope of IEC TC57 as well as documents in other domains (e.g. IEEE, proprietary, etc.). This specification applies to at least those standards listed in Table 1.

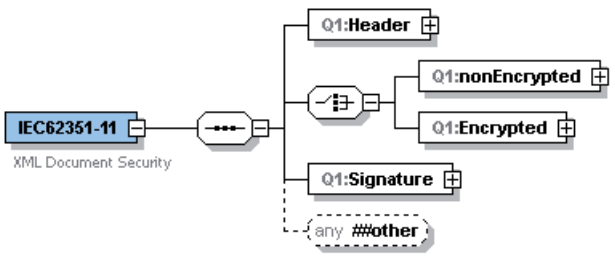
Table 1 – Scope of application to standards within IEC TC57

Number	Name
IEC 61850-6	Communication networks and systems for power utility automation - Part 6: Configuration description language for communication in electrical substations related to IEDs.
IEC 61970-552	Power systems management and associated information exchange - Energy Management System Application Program Interface (EMS-API) - Part 552: CIM XML Model Exchange Format

XML document and extensions specified by this standard. The 62351-11 extensions provide the capability to provide:

- Header: the header contains information relevant to the encapsulation such as the Date and Time of the encapsulation (e.g. file creation).
- a choice of encapsulating the original XML document in 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.



DRAFT
Documents
Document Sharing Hub
Full document details: E DIN IEC 62351-11:2015-02

183 **Figure 1: Overview of 62351-11 structure**

184

185 ### 1.2 Object

186 The initial audience for this specification is intended to be the members of the working groups
187 developing or making use of the standards listed in Table 1. For the measures described in
188 this specification to take effect, they must be accepted and referenced by the specifications
189 themselves. This document is written to enable that process.

190 The subsequent audience for this specification is intended to be the developers of products
191 that implement these specifications.

192 Portions of this specification may also be of use to managers and executives in order to
193 understand the purpose and requirements of the work.

194 ## 2 Normative references
195

Recommended Cononical XML1.0 with Comments	W3C: http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments
Required Cononical XML 1.0	Omits comments. W3C :http://www.w3.org/TR/2001/REC-xml-c14n-20010315
RFC 2401	Security Architecture for the Internet Protocol
RFC 6931	Additional XML Security Uniform Resource Identifiers (URIs)
XML Encryption Syntax and Processing W3C Recommendation 10 December 2002	http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/
XML Signature Syntax and Processing W3C Recommendation 10 June 2008.	http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/

196

197 ## 3 Informative References

198 The following referenced documents are indispensable for the application of this document.
199 For dated references, only the edition cited applies. For undated references, the latest edition
200 of the referenced document (including any amendments) applies.

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

203 IEC 61970-552, Power systems management and associated information exchange - Energy
204 Management System Application Program Interface (EMS-API) - Part 552: CIM XML Model Exchange
205 Format
206

207 *RFC 3275,* (Extensible Markup Language) XML-Signature Syntax and Processing
208

209 RFC 4634, *US Secure Hash Algorithms (SHA and HMAC-SHA)*

DRAFT
Documents
Document Sharing Hub
Full document details: E DIN IEC 62351-11:2015-02

4 Definitions

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

Nonce — "A random or pseudo-random value used within an authentication system." IEEE Std 1455-1999 IEEE Standard for Message Sets for Vehicle/Roadside Communications

5 Security issues addressed by this specification

Within the industry and TC57, XML file exchange is becoming more prevalent. Within the scope of TC57 exchanges of XML files are used for IEC 61970 as well as IEC 61850. Within other standards, IEEE 1815 and IEEE C37.111 (COMTRADE), XML is also being utilized. For these standards and other XML-based files, the information contained in the file may:

1). be sensitive to inadvertant or malicious modifications of its contents that could result in mis-operation/mis-interpretation if the exchanged informaiton is used (e.g. a tamper secuirty vulnerability)

2) contain confidential or private data.

3) contain subsets of information that may be considered critical by the file creation entity.

The work item proposes to standardize mechanisms to protect the document contents from tampering/disclosure when the file is being exchanged (e.g. in transit) and at rest (e.g. stored on a computer). Additionally, the work item 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 IEC TC57, the mechanism/methodologies specified within this document can be applied to any XML document.

5.1 Operational issues affecting choice of security options

5.2 Security threats countered

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

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

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

If encryption is employed, then the specific threats countered in this part 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.

5.3 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;

DRAFT
AVA Documents Document Sharing Hub
Full document details: E DIN IEC 62351-11:2015-02