

2017

Řízení energetických soustav a přidružená výměna informací –
Bezpečnost dat a komunikací –
Část 11: Bezpečnost pro soubory XML

ČSN
EN 62351-11

33 5011

idt IEC 62351-11:2016

Power systems management and associated information exchange – Data and communication security –

Part 11: Security for XML documents

Gestion des systemes de puissance et échanges d'informations associés – Sécurité des communications et des données –

Partie 11: Sécurité des documents XML

Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation –

Teil 11: Sicherheit für XML-Dateien

Tato norma je českou verzí evropské normy EN 62351-11:2017. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN 62351-11:2017. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

IEC 62351-9 dosud nezavedena

IEC/TS 62351-2 dosud nezavedena

IEC/TS 62351-8 dosud nezavedena

W3C, Recommended Conical XML 1.0 nezaveden

W3C, Required Canonical XML 1.0 nezaveden

RFC 6931, *Additional XML Security Uniform Resource Identifiers (URIs)* nezaveden

XML Encryption Syntax and Processing Version 1.1 April 11, 2013 nezaveden

W3C Recommendation 10 June 2008 nezaveden

Souvisící ČSN

ČSN EN 61850-6 (33 4850) Komunikační sítě a systémy pro automatizaci v energetických společnostech – Část 6: Konfigurační popisový jazyk pro komunikaci v elektrických stanicích týkající se IED

ČSN EN 61970-552 (33 4910) Rozhraní aplikačního programu pro systémy řízení elektrické energie (EMS-API) – Část 552: Formát výměny modelu CIMXML

ČSN EN 62351-3 (33 5011) Řízení energetických soustav a přidružená výměna informací – Bezpečnost dat a komunikací – Část 3: Komunikační síť a systémová bezpečnost – Profily zahrnující TCP/IP

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v člancích „Informace o citovaných dokumentech“ a „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

Informativní údaje z IEC 62351-11:2016

Mezinárodní normu vypracovala technická komise IEC/TC 57 *Řízení energetických soustav a přidružená výměna informací*.

Text této normy se zakládá na těchto dokumentech:

FDIS	Zpráva o hlasování
57/1753/FDIS	57/1774/RVD

Úplnou informaci o hlasování při schvalování této normy lze najít ve zprávě o hlasování ve výše uvedené tabulce.

Tato publikace byla vypracována v souladu se směrnicemi ISO/IEC, část 2.

Seznam všech částí souboru IEC 62351 se společným názvem *Řízení energetických soustav a přidružená výměna informací – Bezpečnost dat a komunikací* je možno nalézt na webových stránkách IEC.

Komise rozhodla, že obsah této publikace zůstane nezměněn až do data příští prověrky (stability date) uvedeného na webových stránkách IEC (<http://webstore.iec.ch>) v údajích o této publikaci. K tomuto datu bude publikace buď

- znovu potvrzena;
- zrušena;
- nahrazena revidovaným vydáním, nebo

- změněna.

Upozornění na národní poznámky

Do normy byla k článku 6.5.2.4 doplněna národní poznámka.

Vypracování normy

Zpracovatel: EGC – EnerGoConsult ČB, s. r. o., IČ 25166972, Ing. Václav Král

Technická normalizační komise: TNK 97 Elektroenergetika

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Urban

EVROPSKÁ NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 62351-11

Únor 2017

ICS 33.200

Řízení energetických soustav a přidružená výměna informací –
Bezpečnost dat a komunikací –
Část 11: Bezpečnost pro soubory XML
(IEC 62351-11:2016)

Power system managements and associated information exchange –
Data and communication security –
Part 11: Security for XML documents
(IEC 62351-11:2016)

Gestion des systemes 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)
--	---

Tato evropská norma byla schválena CENELEC dne 2016-11-02. Členové CENELEC jsou povinni splnit vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se této evropské normě bez jakýchkoliv modifikací uděluje status národní normy.

Aktualizované seznamy a bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídícím centru CEN-CENELEC nebo u kteréhokoliv člena CENELEC.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém jiném jazyce přeložená členem CENELEC do jeho vlastního jazyka, za kterou zodpovídá a kterou notifikuje Řídícímu centru CEN-CENELEC, má stejný status jako oficiální verze.

Členy CENELEC jsou národní elektrotechnické komitety Belgie, Bulharska, Bývalé jugoslávské republiky Makedonie, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Maltý, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Srbska,

Španělska, Švédsko, Švýcarsko a Turecko.



Evropský výbor pro normalizaci v elektrotechnice
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung
Řídící centrum CEN-CENELEC: Avenue Marnix 17, B-1000 Brusel

© 2017 CENELEC Veškerá práva pro využití v jakékoli formě a jakýmkoli prostředky
jsou celosvětově vyhrazena členům CENELEC.

Ref. č. EN

62351-11:2017 E

Evropská předmluva

Text dokumentu 57/1753/FDIS, budoucího prvního vydání IEC 62351-11, který vypracovala technická komise IEC/TC 57 *Řízení elektrizačních soustav výměna přidružených informací*, byl předložen k paralelnímu hlasování IEC-CENELEC a byl schválen CENELEC jako EN 62351-11:2017.

Jsou stanovena tato data:

- nejzazší datum zavedení dokumentu na národní úrovni
vydáním identické národní normy nebo vydáním
oznámení o schválení k přímému používání
jako normy národní (dop) 2017-08-10
- nejzazší datum zrušení národních norem,
které jsou s dokumentem v rozporu (dow) 2020-02-10

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CENELEC [a/nebo CEN] nelze činit odpovědným za identifikaci jakéhokoliv nebo všech patentových práv.

Oznámení o schválení

Text mezinárodní normy IEC 62351-11:2016 byl schválen CENELEC jako evropská norma bez jakýchkoliv modifikací.

Evropská předmluva.....	6
1..... Rozsah platnosti.....	9
2..... Citované dokumenty.....	9
3..... Termíny a definice.....	10
4..... Otázky zabezpečení řešené tímto dokumentem.....	10
4.1..... Obecně.....	10
4.2..... Řešené bezpečností hrozby.....	11
4.3..... Řešené metody útoků.....	11
5..... Dokumenty XML.....	11
6..... Zapouzdření dokumentu XML.....	12
6.1..... Obecně.....	12
6.2..... TypHlavičky (HeaderType).....	13
6.3..... Informace (Information).....	14

6.3.1...	
Obecně.....	
.....	14
6.3.2...	
Nonce.....	
.....	15
6.3.3... ŘízeníPřístupu	
(AccessControl).....	
.....	15
6.3.4... Tělo	
(Body).....	
.....	20
6.4..... Prvek Zašifrováno	
(Encrypted).....	
....	21
6.4.1...	
Obecně.....	
.....	21
6.4.2... ŠifrovacíMetoda	
(EncryptionMethod).....	
.....	21
6.4.3... DataŠifrování	
(CipherData).....	
.....	22
6.4.4... InfoOKlíči	
(KeyInfo).....	
.....	22
6.5..... TypPodpisu	
(SignatureType).....	
.....	22
6.5.1...	
Obecně.....	
.....	22
6.5.2... TypPodepsanýchInfo	
(SignedInfoType).....	
23	
6.6..... Podpora typů	
XSD.....	
.....	26
6.6.1...	

Obecně.....	26
6.6.2... TypSeqNázvu (NameSeqType).....	26
6.7..... Volba algoritmu zabezpečení.....	26
7..... Příklady souborů (informativní).....	27
7.1..... Nešifrovaný příklad.....	27
7.2..... Šifrovaný příklad.....	29
8..... Seznam IANA pro metody podpisu, výtahu a šifrování (informativní).....	31
Bibliografie.....	35
Příloha ZA (normativní) Normativní odkazy na mezinárodní publikace a jim odpovídající evropské publikace.....	37
Obrázek 1 - Přehled Struktury IEC 62351-11.....	9
Obrázek 2 - Příklad předávaných dat.....	11
Obrázek 3 - Bezpečnostní zapouzdření pro dokumenty XML.....	12
Obrázek 4 - Obecné schéma XSD IEC 62351-11.....	13
Obrázek 5 - Definice KomplexníTyp XSD TypuHlavičky.....	13
Obrázek 6 - Definice komplexního typu XSD informace.....	14

Obrázek 7 - Definice komplexního typu XSD ŘízeníPřístupu.....	15
Obrázek 8 - Definice komplexního typu XSD TypŘízeníPřístupu.....	15
Obrázek 9 - Definice komplexního typu XSD TypOmezeníPřístupu.....	16
Obrázek 10 - Definice komplexního typu XSD TypEntity.....	17
Obrázek 11 - Příklad ŘízeníPřístupu a XPATH.....	19
Obrázek 12 - Příklad Těla IEC 62351-11 s dokumentem CIM.....	20
Obrázek 13 - Struktura šifrovaného prvku IEC 62351-11.....	21
Obrázek 14 - Struktura TypuMetodyŠifrování.....	21
Obrázek 15 - Struktura TypuŠifrovacíchDat.....	22
Obrázek 16 - Definice prvku ŠifrovanáData.....	22
Obrázek 17 - Definice W3C TypuPodpisu.....	23
Obrázek 18 - Struktura XML TypuPodepsanýchInfo.....	23
Obrázek 19 - Struktura TypuMetodyPodpisu.....	24
Obrázek 20 - Struktura TypuOdkazu.....	24
Obrázek 21 - Struktura TypuInfoOKlíči.....	

..... 25

Obrázek 22 - Definice

TypuSekNázvu.....
..... 26

Tabulka 1 - Definice obecné struktury dokumentu IEC

62351-11..... 13

Tabulka 2 - Definice prvku

TypHlavičky.....
. 14

Tabulka 3 - Definice prvků

informace.....
. 14

Tabulka 4 - Definice prvku „Smluvní“

a ACL..... 16

Tabulka 5 - Definice prvku

TypOmezeníACL.....
16

Tabulka 6 - Definice výčtových hodnot pro

TypACL..... 17

Tabulka 7 - Definice výčtových hodnot pro

Omezení..... 17

Tabulka 8 - Definice prvku

TypEntity.....
... 18

1 Rozsah platnosti

Tato část IEC 62351 specifikuje schéma, postupy a algoritmy pro zabezpečení souborů XML, které jsou využívány v rámci rozsahu platnosti IEC a zároveň souborů v jiných doménách (například IEEE, soukromých atd.). Smyslem je, aby se na tuto část odkazovaly normy, které vyžadují bezpečnou výměnu, pokud se strany vzájemně nedohodnou na využití jiných uznávaných mechanismů zabezpečení výměny.

Tato část IEC 62351 využívá dobře známé normy W3C pro bezpečnost XML souboru a poskytuje profilování těchto norem a další rozšíření. Rozšíření IEC 62351-11 zajišťují následující možnosti:

- Header (Hlavička): hlavička obsahuje důležité informace týkající se vytvoření zabezpečeného dokumentu, jako jsou datum a čas kdy byl IEC 62351-11 vytvořen.
- Možnost zapouzdřit původní XML soubor do šifrovaného (Encrypted) nebo nešifrovaného (nonEncrypted) formátu. Pokud je zvoleno šifrování, je poskytován mechanismus popisující skutečnou metodu šifrování interoperabilním způsobem (EncryptionInfo).
- AccesControl (ŘízeníPřístupu): mechanismus popisující řízení přístupu, týkající se informací obsažených v původním souboru XML.
- Body (Tělo): obsahuje původní XML soubor, který je zapouzdřený.
- Signature (Podpis): podpis, který lze využít pro autentizaci a detekce falšování (sabotáže).

Obecná struktura je zobrazena na obrázku 1.



Obrázek 1 - Přehled Struktury IEC 62351-11

Aby opatření popisovaná v tomto dokumentu byla účinná, musí být přijata a odkazována samotnými specifikacemi. Tento dokument je napsán tak, aby tento proces umožnil.

Tato část IEC 62351 je určena pracovníkům vyvíjejícím produkty, které implementují tyto specifikace.

Určité pasáže této části IEC 62351 mohou sloužit také manažerům a exekutivě k pochopení smyslu a požadavkům práce.

Konec náhledu - text dále pokračuje v placené verzi ČSN.