
**Upravljanje elektroenergetskega sistema in pripadajoča izmenjava informacij -
Varnost podatkov in komunikacij - 4. del: Profili, vključno z MMS in izpeljankami -
Dopolnilo A1**

Power systems management and associated information exchange - Data and
communications security - Part 4: Profiles including MMS and derivatives

Energiemanagementsysteme und zugehöriger Datenaustausch - IT-Sicherheit für Daten
und Kommunikation - Teil 4: Profile einschließlich MMS und Ableitungen

Gestion des systèmes de puissance et échanges d'informations associés - Sécurité des
communications et des données - Partie 4: Profils comprenant MMS

Ta slovenski standard je istoveten z: EN IEC 62351-4:2018/A1:2020

ICS:

29.240.30	Krmilna oprema za elektroenergetske sisteme	Control equipment for electric power systems
35.240.50	Uporabniške rešitve IT v industriji	IT applications in industry

SIST EN IEC 62351-4:2019/A1:2020 en

iTeh STANDARD PREVIEW
(standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/sist/ch6e076e-4834-4a41-abe6-13e4549ac84c/sist-en-iec-62351-4-2019-a1-2020>

EUROPEAN STANDARD

EN IEC 62351-4:2018/A1

NORME EUROPÉENNE

EUROPÄISCHE NORM

September 2020

ICS 33.200

English Version

Power systems management and associated information
exchange - Data and communications security - Part 4: Profiles
including MMS and derivatives
(IEC 62351-4:2018/A1:2020)

Gestion des systèmes de puissance et échanges
d'informations associés - Sécurité des communications et
des données - Partie 4: Profils comprenant le MMS et ses
dérivés
(IEC 62351-4:2018/A1:2020)

Energiemanagementsysteme und zugehöriger
Datenaustausch - IT-Sicherheit für Daten und
Kommunikation - Teil 4: Profile einschließlich MMS und
Ableitungen
(IEC 62351-4:2018/A1:2020)

This amendment A1 modifies the European Standard EN IEC 62351-4:2018; it was approved by CENELEC on 2020-08-21. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this amendment 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 amendment 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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, 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: Rue de la Science 23, B-1040 Brussels

EN IEC 62351-4:2018/A1:2020 (E)**European foreword**

The text of document 57/2217/FDIS, future IEC 62351-4/A1, 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 IEC 62351-4:2018/A1:2020.

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) 2021-05-21
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2023-08-21

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

Endorsement notice

The text of the International Standard IEC 62351-4:2018/A1:2020 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 61850-8-1:2011 | NOTE | Harmonized as EN 61850-8-1:2011 (not modified) |
| IEC 61850-8-2:2018 | NOTE | Harmonized as EN IEC 61850-8-2:2019 (not modified) |

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where 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.

Replace the existing reference to ISO/IEC 9594-8 with the following reference:

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
ITU-T X.509	-	Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks	-	-

ITeH STANDARD PREVIEW
 (standards.iteh.ai)
 SIST EN IEC 62351-4:2019/A1:2020
<https://standards.iteh.ai/catalog/standards/sist/en-iec-62351-4-2019/a1-2020>
<https://standards.iteh.ai/catalog/standards/sist/en-iec-62351-4-2019/a1-2020>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/sist/ch6e076e-4834-4a41-abe6-13e4549ac84c/sist-en-iec-62351-4-2019-a1-2020>



INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 1
AMENDEMENT 1

**Power systems management and associated information exchange – Data and communications security –
Part 4: Profiles including MMS and derivatives**

**Gestion des systèmes de puissance et échanges d'informations associés –
Sécurité des communications et des données –
Partie 4: Profils comprenant le MMS et ses dérivés**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-8520-6

**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.**

FOREWORD

This amendment has been prepared by working group 15: Data and communication security, of IEC technical committee 57: Power systems management and associated information exchange.

The text of this amendment is based on the following documents:

FDIS	Report on voting
57/2217/FDIS	57/2233/RVD

Full information on the voting for the approval of this amendment can be found in the report on voting indicated in the above table.

The committee has decided that the contents of this amendment and the base 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.

2 Normative references

Replace the existing reference to ISO/IEC 9594-8 with the following new reference:

ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

3 Terms and definitions

3.2.2

Replace the existing text:

[SOURCE: ISO/IEC 7498-1:1994 | Rec. ITU-T X.200:1994, 7.1.1.2]

with the following new text:

[SOURCE: ISO/IEC 7498-1:1994 | Rec. ITU-T X.200 (1994), 7.1.1.2]

Add, after 3.2.2, the following new definition and renumber subsequent subclauses accordingly:

3.2.3

alarm

security event that might be caused by an adversary

3.2.7

Replace the existing text:

[SOURCE: Rec. ITU-T X.217:1995, 3.5.1]

with the following new text:

[SOURCE: Rec. ITU-T X.217 (1995), 3.5.1]

3.2.11

Replace the existing text:

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.14]

with the following new text:

[SOURCE: ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019), 3.5.14]

3.2.12

Replace the existing text:

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509:2016, 3.5.21]

with the following new text:

[SOURCE: ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019), 3.5.21]

3.2.18

Replace the existing text:

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509:2016, 3.5.31]

with the following new text:

[SOURCE: ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019), 3.5.31]

Add, after 3.2.20, the following new definition and renumber subsequent subclauses accordingly:

3.2.21**error**

security event that is caused by bad implementation behaviour resulting in disruption of communication

Add, after 3.2.27, the following new definition and renumber subsequent subclauses accordingly:

3.2.28**protocol control information**

information exchanged between entities of a given layer, via the service provided by the next lower layer, to coordinate their joint operation

3.2.29

Replace the existing text:

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509:2016, 3.5.57]

with the following new text:

[SOURCE: ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019), 3.5.58]

3.2.34

Replace the existing text:

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509:2016, 3.5.71]

with the following new text:

[SOURCE: ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019), 3.5.72]

3.3 Abbreviated terms

Add the following new abbreviation:

PCI Protocol Control Information

4.2 Security for application and transport profiles**Table 1 – Relationship between security and security measure combinations**

Remove the end parenthesis in the first column, first row of Table 1.

4.5.3 Attacks countered in native mode

In the second set of bullet items, replace the existing text:

- Man-in-the-middle: This threat is countered through the use of authentication during end-to-end association by use of digital signature and during data transfer by use of ICV.

with the following new text:

- Man-in-the-middle: This threat is countered through the use of authentication during end-to-end association establishment by use of digital signature and during data transfer by use of ICV.

6.2.6 Public-key certificate size

Replace the existing text of the first paragraph of 6.2.6 with the following new text:

An implementation that claims conformance to this document shall support a public-key certificate size of minimum and maximum 8192 octets. It is a local issue if larger public-key certificates are supported.

Add, after the first paragraph of 6.2.6, the following new paragraph:

In order to achieve interoperability of public-key certificates, it is necessary to set a maximum allowed size for the public-key certificates exchanged by ACSE. This size shall be limited to a maximum encoding size of 8192 octets.

6.3.4.1 General

Replace the existing text of the second paragraph of 6.3.4.1 with the following new text:

TLS prioritizes the proposed cipher suites in the TLS handshake according to the order in the proposed cipher suite list in the ClientHello message. To accommodate a security policy it is strongly recommended to have the order of proposed cipher suites according to the local security policy. Cipher suites marked as mandatory shall be stated in the proposal list of the ClientHello message.

6.3.4.2 Mandatory and recommended cipher suites for compatibility mode

Replace the existing text of the first paragraph of 6.3.4.2 with the following new text:

All implementations that claim conformance to IEC TS 62351-4:2007 shall support TLS_DH_DSS_WITH_AES_256_CBC_SHA at a minimum.

Replace existing Table 2 with the following new table:

Table 2 – Commented recommended cipher suites from IEC TS 62351-4:2007

Key exchange		Encryption	Hash	IANA Value	Source	Support
Algorithm	Signature					
TLS_RSA_		WITH_RC4_128_	SHA	0x00,0x00	RFC 2246 (TLS 1.0)	Disallowed (RC 4 considered weak)
TLS_RSA_		WITH_3DES_ede_CBC_	SHA	0x00,0x0A	RFC 2246 (TLS 1.0)	o
TLS_DH_	DSS_	WITH_3DES_ede_CBC_	SHA	0x00,0x0D	RFC 2246 (TLS 1.0)	o
TLS_DH_	RSA_	WITH_3DES_ede_CBC_	SHA	0x00,0x10	RFC 2246 (TLS 1.0)	o
TLS_DHE_	DSS_	WITH_3DES_ede_CBC_	SHA	0x00,0x13	RFC 2246 (TLS 1.0)	o
TLS_DHE_	RSA_	WITH_3DES_ede_CBC_	SHA	0x00,0x16	RFC 2246 (TLS 1.0)	o
TLS_DH_	DSS_	WITH_AES_128_CBC_	SHA	0x00,0x30	RFC 4346 (TLS 1.1)	o
TLS_DH_	DSS_	WITH_AES_256_CBC_	SHA	0x00,0x36	RFC 4346 (TLS 1.1)	m
TLS_DH_		WITH_AES_128_CBC	SHA	0x00, 0x34	RFC 4346 (TLS 1.1)	Disallowed (anonymous)
TLS_DH_		WITH_AES_256_CBC	SHA	0x00, 0x3A	RFC 4346 (TLS 1.1)	Disallowed (anonymous)

6.3.4.3 Mandatory and recommended cipher suites for native mode

Replace the existing text of the first paragraph of 6.3.4.3 with the following new text:

All implementations that claim conformance to the native mode shall support the mandatory cipher suites listed in Table 3.

Replace existing Table 3 with the following new table:

Table 3 – Cipher suites combinations in the context of this document

Key exchange		Encryption	Hash	IANA Value	Source	Support
Algorithm	Signature					
TLS_RSA		WITH_AES_128_CBC_	SHA256	0x00,0x3C	RFC 5246	m
TLS_DH_	RSA_	WITH_AES_128_CBC_	SHA256	0x00,0x31	RFC 5246	o
TLS_DH_	RSA_	WITH_AES_128_GCM_	SHA256	0x00,0xA0	RFC 5288 [20]	m
TLS_DHE_	RSA_	WITH_AES_128_GCM_	SHA256	0xC0,0x9E	RFC 5288 [20]	m
TLS_DH_	RSA_	WITH_AES_256_GCM_	SHA384	0x00,0xA1	RFC 5288 [20]	o
TLS_ECDHE_	RSA_	WITH_AES_128_GCM_	SHA256	0xC0,0x2F	RFC 5289 [7]	o
TLS_ECDHE_	RSA_	WITH_AES_256_GCM_	SHA384	0xC0,0x30	RFC 5289 [7]	o
TLS_ECDHE_	ECDSA_	WITH_AES_128_GCM_	SHA256	0xC0,0x23	RFC 5289 [7]	m
TLS_ECDHE_	ECDSA_	WITH_AES_256_GCM_	SHA384	0xC0,0x24	RFC 5289 [7]	o

7.1 General

Replace the existing text of item b), first bullet, with the following new text:

- Clause 12 defines the overall model or architecture for E2E security, including how E2E security relates to an operational environment and a protected protocol.

7.2.2 ASN.1 as an XML schema definition

Replace the text EXTENDED-XER in item b) with EXTENDED-XER

Replace the existing text of the last sentence of item c) by the following new text:

DER is also specified by ISO/IEC 8857-1 | Rec. ITU-T X.690.

7.2.4 XML namespace

Replace the existing text:

(see 12.1)

with the following new text:

(see 16.5)

8.2 Basic cryptographic definitions

Replace the existing text of the last two paragraphs with the following new text:

A defined set represents a set of cryptographic algorithms relevant for a particular situation.

The extension mark (...) will cause an ASN.1 tool to accept any cryptographic object, whether it identifies a cryptographic algorithm for the specific purpose or not. A referencing specification or an implementers' agreement may remove the extension mark and/or add additional algorithms.