SIST

SLOVENSKI STANDARD
SIST EN 62351-3:2015/A1:2018

01-november-2018

Upravljanje elektroenergetskega sistema in pripadajoča izmenjava informacij - Varnost podatkov in komunikacij - 3. del: Varnost komunikacijskih omrežij in sistemov - Profili za TCP/IP - Dopolnilo A1

Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP

Datenmodelle, Schnittstellen und Informationsaustausch für Planung und Betrieb von Energieversorgungsunternehmen - Daten- und Kommunikationssicherheit - Teil 3: Sicherheit von Kommunikationsnetzen und Systemen - Profile einschließlich TCP/IP

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 62351-3:2015/A1:2018
https://standards.iteh.ai/catalog/standards/sist/f464323e-1c84-481f-a832-f4e2ef576cd2/sist-en-62351-3-2015-a1-2018

Gestion des systèmes de puissance et échanges d’informations associés - Sécurité des communications et des données - Partie 3: Sécurité des réseaux et des systèmes de communication - Profils comprenant TCP/IP

Ta slovenski standard je istoveten z: EN 62351-3:2014/A1:2018

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 62351-3:2015/A1:2018 en

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 62351-3:2015/A1:2018
https://standards.iteh.ai/catalog/standards/sist/f464323e-1c84-481f-a832-14e2ef576cd2/sist-en-62351-3-2015-a1-2018

SIST EN 62351-3:2015/A1:2018

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62351-3:2014/A1

September 2018

ICS 33.200

English Version

Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP (IEC 62351-3:2014/A1:2018)

Gestion des systèmes de puissance et échanges d'informations associés - Sécurité des communications et des données - Partie 3: Sécurité des réseaux et des systèmes de communication - Profils comprenant TCP/IP (IEC 62351-3:2014/A1:2018)

Management von Systemen der Energietechnik und zugehöriger Datenaustausch - Daten- und Kommunikationssicherheit - Teil 3: Sicherheit von Kommunikationsnetzen und Systemen - Profile einschließlich TCP/IP (IEC 62351-3:2014/A1:2018)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This amendment A1 modifies the European Standard EN 62351-3:2014; it was approved by CENELEC on 2018-06-29. 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.

SIST EN 62351-3:2015/A1:2018
https://standards.iteh.ai/catalog/standards/sist/f464323e-1c84-481f-a832-14e2ef576cd2/sist-en-62351-3-2015-a1-2018

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, 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.

CENELEC

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

© 2018 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

SIST EN 62351-3:2015/A1:2018

European foreword

The text of document 57/1976/FDIS, future edition 1 of IEC 62351-3/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 62351-3:2014/A1:2018.

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)	2019-03-29
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2021-06-29

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.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Endorsement notice

SIST EN 62351-3:2015/A1:2018
https://standards.iteh.ai/catalog/standards/sist/f464323e-1c84-481f-a832-14e2ef576cd2/sist-en-62351-3-2015-a1-2018

The text of the International Standard IEC 62351-3:2014/A1:2018 was approved by CENELEC as a European Standard without any modification.

SIST EN 62351-3:2015/A1:2018

Replace Annex ZA of 62351-3:2014 by the following one:

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 62351-3:2015/A1:2018
https://standards.iteh.ai/catalog/standards/sist/f164323e-1e84-481f-a832-14e2af576cd2/sist-en-62351-3-2015-a1-2018

Publication	Year	Title	EN/HD	Year
IEC/TS 62351-1	2007	Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues	-	-
IEC/TS 62351-2	2008	Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms	-	-
IEC 62351-9	-	Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment	EN 62351-9	-
ISO/IEC 9594-8	2017	Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks	-	-
RFC 4492	2006	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)	-	-
RFC 5246	2008	The Transport Layer Security (TLS) Protocol Version 1.2	-	-
RFC 5280	2008	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	-	-
RFC 5746	2010	Transport Layer Security (TLS) Renegotiation Indication Extension	-	-
RFC 6066	2006	Transport Layer Security (TLS) Extensions: Extension Definitions	-	-
RFC 6176	2011	Prohibiting Secure Sockets Layer (SSL) Version 2.0	-	-

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 62351-3:2015/A1:2018
https://standards.iteh.ai/catalog/standards/sist/f464323e-1c84-481f-a832-14e2ef576cd2/sist-en-62351-3-2015-a1-2018

SIST EN 62351-3:2015/A1:2018

IEC 62351-3

Edition 1.0 2018-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 1
AMENDEMENT 1

Power systems management and associated information exchange – Data and communications security –
Part 3: Communication network and system security – Profiles including TCP/IP

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 62351-3:2015/A1:2018
https://standards.iteh.ai/catalog/standards/sist/f4c4523e-1c84-481f-a832-14e2ef576e42/sist-en-62351-3-2015-a1-2018

Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données –
Partie 3: Sécurité des réseaux et des systèmes de communication – Profils comprenant TCP/IP

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 33.200 ISBN 978-2-8322-5720-3

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.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

SIST EN 62351-3:2015/A1:2018

FOREWORD

This amendment to the International Standard IEC 62351-3 has been prepared by 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
57/1976/FDIS	57/1990/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.

A list of all parts in 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 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 62351-3:2015/A1:2018
https://standards.iteh.ai/catalog/standards/sist/f464323e-1c84-481f-a832-14e2ef576cd2/sist-en-62351-3-2015-a1-2018

2 Normative references

Replace the existing reference IEC TS 62351-9 with the following new reference:

IEC 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

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

ISO/IEC 9594-8:2017, *Rec. ITU-T X.509 (2016), Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks*

4.1 Operational requirements affecting the use of TLS in the telecontrol environment

Replace the existing text of the fifth paragraph of 4.1 with the following new text:

Note that TLS utilizes X.509 certificates (see also ISO/IEC 9594-8 or RFC 5280) for authentication. In the context of this specification the term certificates always relates to public-key certificates (in contrast to attribute certificates).

SIST EN 62351-3:2015/A1:2018

4.2 Security threats countered

Replace the existing text of the second paragraph of 4.2 with the following new text:

TCP/IP and the security specifications in this part of IEC 62351 cover only to the communication transport layers (OSI layers 4 and lower). This part of IEC 62351 does not cover security functionality specific for the communication application layers (OSI layers 5 and above) or application-to-application security.

NOTE The application of TLS as profiled in this document supports the protection of information sent over the TLS protected connection.

4.3 Attack methods countered

Replace the existing text of the first bullet point of Subclause 4.3 by the following new text:

– Man-in-the-middle: This threat is countered through the use of a Message Authentication Code mechanism or digital signatures specified within this document.

5.1 Deprecation of cipher suites

Add the following new text before the fourth paragraph of 5.1:

The support of SHA-1 is intended for backward compatibility. SHA-256 shall be supported and is the preferred signature algorithm to be used.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SHA-1 is no longer recognized as secure with respect collision resistance and it is therefore strongly recommended to perform a risk assessment before using this algorithm. If SHA-256 cannot be used, it is also recommended that additional security measures be taken. The usage of SHA-1 will be disallowed in the next edition of this standard.

SIST EN 62351-3:2015/A1:2018
https://standards.iteh.ai/catalog/standards/sist/f464323e-1c84-481f-a832-14c2ef576cd2/sist-en-62351-3-2015-a1-2018

NOTE Recommendations regarding hash signature algorithms are reviewed constantly and can be found in NIST SP800-57, BNetzA (BSI), or the NSA Suite B.

Replace the existing text of the fourth paragraph of 5.1 by the following new text:

The list of disallowed suites includes, but is not limited to:

- TLS_NULL_WITH_NULL_NULL
- TLS_RSA_ WITH_NULL_MD5

5.2 Negotiation of Versions

Add the following new text at the end of Subclause 5.2:

The proposal of versions TLS 1.0 or TLS 1.1 should raise a security warning ("warning: insecure TLS version"). Implementations should provide a mechanism for announcing security warnings.

5.3 Session Resumption

Replace the existing text of Subclause 5.3 with the following new text:

Session resumption in TLS allows for the resumption of a session based on the session ID connected with a dedicated (existing) master secret, which will result in a new session key. This minimizes the performance impact of asymmetric handshakes, and can be done during a running session or after a session has ended within a defined time period (TLS suggests not more than 24 hours in RFC 5280). This specification follows this suggestion. Session resumption should be performed at least every 24 hours for active sessions or not later than 24 hours for sessions that have ended. The actual parameters should be defined based on