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

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 62351-9:2017 sisaldab Euroopa standardi EN 62351-9:2017 ingliskeelset teksti.	This Estonian standard EVS-EN 62351-9:2017 consists of the English text of the European standard EN 62351-9:2017.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 07.07.2017.	Date of Availability of the European standard is 07.07.2017.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 33.200

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62351-9

July 2017

ICS 33.200

English Version

Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment (IEC 62351-9 :2017)

Gestion des systèmes de puissance et échanges d'informations associés - Sécurité des communications et des données - Partie 9: Gestion de clé de cybersécurité des équipements de système de puissance (IEC 62351-9 :2017)

Energiemanagementsysteme und zugehöriger Datenaustausch - IT-Sicherheit für Daten und Kommunikation - Teil 9: Cyber security Schlüssel-Management für Stromversorgungsanlagen (IEC 62351-9 :2017)

This European Standard was approved by CENELEC on 2017-06-22. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard 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 European Standard 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.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 62351-9:2017 E

European foreword

The text of document 57/1838/FDIS, future edition 1 of IEC 62351-9, 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 62351-9:2017.

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)	2018-03-22
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2020-06-22

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.

Endorsement notice

The text of the International Standard IEC 62351-9:2017 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 62351-3	NOTE	Harmonized as EN 62351-3.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 When 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

Publication	Year	Title	EN/HD	Year
IEC/TS 62351-2	-	Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms	-	-
ISO/IEC 9594-8/ Rec. ITU-T X.509	2017 2016	Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks	-	-
ISO/IEC 9834-1/ Rec. ITU-T X.660	2012 2011	Information technology - Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree	-	-
RFC 5246	-	The Transport Layer Security (TLS) Protocol Version 1.2	-	-
RFC 5272	-	Certificate Management over CMS (CMC)	-	-
RFC 5934	-	Trust Anchor Management Protocol (TAMP)	-	-
RFC 6407	-	The Group Domain of Interpretation	-	-
IETF RFC 6960	-	X.509 - Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	-	-
RFC 7030	-	Enrolment over Secure Transport	-	-

SCEP IETF Draft, Simple Certificate Enrolment Protocol, draft-gutmann-scep-04.txt

CONTENTS

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

Part 9: Cyber security key management for power system equipment

1 Scope

This part of IEC 62351 specifies cryptographic key management, namely how to generate, distribute, revoke, and handle public-key certificates and cryptographic keys to protect digital data and its communication. Included in the scope is the handling of asymmetric keys (e.g. private keys and public-key certificates), as well as symmetric keys for groups (GDOI).

This part of IEC 62351 assumes that other standards have already chosen the type of keys and cryptography that will be utilized, since the cryptography algorithms and key materials chosen will be typically mandated by an organization's own local security policies and by the need to be compliant with other international standards. This document therefore specifies only the management techniques for these selected key and cryptography infrastructures. The objective is to define requirements and technologies to achieve interoperability of key management.

The purpose of this part of IEC 62351 is to guarantee interoperability among different vendors by specifying or limiting key management options to be used. This document assumes that the reader understands cryptography and PKI principles.

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*

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

ISO/IEC 9834-1:2012 | Rec. ITU-T X.660 (2011), *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree*

SCEP IETF Draft, *Simple Certificate Enrolment Protocol, draft-gutmann-scep-04.txt*

RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*

RFC 5272, *Certificate Management over CMS (CMC)*

RFC 5934, *Trust Anchor Management Protocol (TAMP)*

RFC 6407, *The Group Domain of Interpretation*