IEC 62351-9

Edition 2.0 2023-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-6950-3

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 9: Cyber security key management for power system equipment

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
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.

IEC 62351-9 has been prepared by WG15: Data and Communication Security, of IEC technical committee TC57: Power systems management and associated information exchange. It is an International Standard.

This second edition cancels and replaces the first edition published in 2017. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) Certificate components and verification of the certificate components have been added;
b) GDOI has been updated to include findings from interop tests;
c) GDOI operation considerations have been added;
d) GDOI support for PTP (IEEE 1588) support has been added as specified by IEC/IEEE 61850-9-3 Power Profile;
e) Cyber security event logging has been added as well as the mapping to IEC 62351-14;

f) Annex B with background on utilized cryptographic algorithms and mechanisms has been added.

The text of this International Standard is based on the following documents:

Draft	Report on voting
57/2579/FDIS	57/2594/RVD

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

NOTE The following print types are used:

Abstract Syntax Notation One (ASN.1): `in courier new` and **`bold courier new`** `type`.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

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, primarily focused on the management of long-term keys, which are most often asymmetric key pairs, such as public-key certificates and corresponding private keys. As certificates build the base this document builds a foundation for many IEC 62351 services (see also Annex A). Symmetric key management is also considered but only with respect to session keys for group-based communication as applied in IEC 62351-6. The objective of this document is to define requirements and technologies to achieve interoperability of key management by specifying or limiting key management options to be used.

This document assumes that an organization (or group of organizations) has defined a security policy to select the type of keys and cryptographic algorithms that will be utilized, which may have to align with other standards or regulatory requirements. This document therefore specifies only the management techniques for these selected key and cryptography infrastructures. This document assumes that the reader has a basic understanding of cryptography and key management principles.

The requirements for the management of pairwise symmetric (session) keys in the context of communication protocols is specified in the parts of IEC 62351 utilizing or specifying pairwise communication such as:

- IEC 62351-3 for TLS by profiling the TLS options
- IEC 62351-4 for the application layer end-to-end security
- IEC TS 62351-5 for the application layer security mechanism for IEC 60870-5-101/104 and IEEE 1815 (DNP3)

The requirements for the management of symmetric group keys in the context of power system communication protocols is specified in IEC 62351-6 for utilizing group security to protect GOOSE and SV communication. IEC 62351-9 utilizes GDOI as already IETF specified group-based key management protocol to manage the group security parameter and enhances this protocol to carry the security parameter for GOOSE, SV, and PTP.

This document also defines security events for specific conditions which could identify issues which might require error handling. However, the actions of the organisation in response to these error conditions are beyond the scope of this document and are expected to be defined by the organizations security policy.

In the future, as public-key cryptography becomes endangered by the evolution of quantum computers, this document will also consider post-quantum cryptography to a certain extent. Note that at this time being no specific measures are provided.

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*

IEC 62351-3:—[1], *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

IEC 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives*

IEC 62351-5, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

IEC 62351-6, *Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850*

IEC 62351-14:—[2], *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging*

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

ISO/IEC 9594-11:2020, Rec. ITU-T X.510 (2020), *Information technology – Open systems interconnection – The Directory: Protocol specifications for secure operations*

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*

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

IETF RFC 5755, *An Internet Attribute Certificate Profile for Authorization*

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

IETF RFC 6407, *The Group Domain of Interpretation*

IETF RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*

IETF RFC 7030, *Enrolment over Secure Transport*

IETF RFC 8052, *Group Domain of Interpretation (GDOI) Protocol Support for IEC 62351 Security*

_____

[1] Under preparation. Stage at the time of publication: IEC/RFDIS 62351-3:2023.

[2] Under preparation. Stage at the time of publication: IEC/ACDV 62351-14:2023.

IETF RFC 8263, *Group Domain of Interpretation (GDOI) GROUPKEY-PUSH Acknowledgement Message*

IETF RFC 8894, *Simple Certificate Enrolment Protocol*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments du présent document de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 62351-9 a été établie par le WG 15, Sécurité des communications et des données, du comité d'études 57 de l'IEC, Gestion des systèmes de puissance et échanges d'informations associés. Il s'agit d'une Norme internationale.

Cette deuxième édition annule et remplace la première édition parue en 2017. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) des composants de certificats et leur vérification ont été ajoutés;
b) le GDOI a été mis à jour pour inclure les résultats des essais d'interopérabilité;
c) des aspects liés au fonctionnement du GDOI ont été ajoutés;
d) la prise en charge du GDOI pour PTP (IEEE 1588) a été ajoutée comme spécifié par le profil de puissance de l'IEC/IEEE 61850-9-3;
e) l'enregistrement des événements de cybersécurité a été ajouté, ainsi que la mise en correspondance avec l'IEC 62351-14;
f) l'Annex B qui fournit des informations sur les algorithmes et mécanismes cryptographiques utilisés a été ajoutée.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
57/2579/FDIS	57/2594/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/publications.

NOTE Les caractères d'imprimerie suivants sont employés:

Notation de syntaxe abstraite numéro un (ASN.1): en type `courier new` et **`bold courier new`**.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera:

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de ce document indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

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

1 Domaine d'application

La présente partie de l'IEC 62351 spécifie la gestion des clés cryptographiques, principalement axée sur la gestion des clés à long terme, qui sont le plus souvent des paires de clés asymétriques, telles que des certificats de clés publiques et les clés privées correspondantes. Comme les certificats constituent la base, le présent document établit une fondation pour de nombreux services de l'IEC 62351 (voir également Annex A). La gestion des clés symétriques est également prise en compte, mais uniquement en ce qui concerne les clés de session pour les communications de groupe, telles qu'elles sont appliquées dans l'IEC 62351-6. L'objectif du présent document est de définir les exigences et les technologies permettant d'assurer l'interopérabilité de la gestion des clés en spécifiant ou en limitant les options de gestion de clés à utiliser.

Le présent document présume qu'une organisation (ou un groupe d'organisations) a défini une politique de sécurité pour sélectionner le type de clés et d'algorithmes cryptographiques qui seront utilisés, qui peuvent être à aligner sur d'autres normes ou exigences réglementaires. Le présent document spécifie donc uniquement les techniques de gestion de ces infrastructures de clé et de cryptographie sélectionnées. Le présent document présume que le lecteur a des notions de base en cryptographie et sur les principes de gestion des clés.

Les exigences relatives à la gestion des paires de clés (de session) symétriques dans le contexte des protocoles de communication sont spécifiées dans les parties de l'IEC 62351 qui utilisent ou spécifient une communication par paire, telles que:

- l'IEC 62351-3 pour TLS en profilant les options TLS;
- l'IEC 62351-4 pour la sécurité de bout en bout de la couche application;
- l'IEC 62351-5 pour le mécanisme de sécurité de la couche application pour l'IEC 60870-5-101/104 et l'IEEE 1815 (DNP3).

Les exigences relatives à la gestion des clés de groupe symétriques dans le contexte des protocoles de communication des systèmes de puissance sont spécifiées dans l'IEC 62351-6 pour l'utilisation de sécurité de groupe pour protéger les communications GOOSE et SV. L'IEC 62351-9 utilise GDOI comme protocole de gestion de clés par groupe déjà spécifié par l'IETF (Internet Engineering Task Force) pour gérer le paramètre de sécurité de groupe et améliore ce protocole pour transporter le paramètre de sécurité pour les communications GOOSE, SV et PTP.

Le présent document définit également les événements de sécurité pour des conditions spécifiques susceptibles d'identifier des problèmes pouvant exiger un traitement des erreurs. Cependant, les actions de l'organisation en réponse à ces conditions d'erreur ne relèvent pas du domaine d'application du présent document et sont censées être définies par la politique de sécurité des organisations.

À l'avenir, lorsque la cryptographie à clé publique sera mise en danger par l'évolution des ordinateurs quantiques, le présent document examinera également la cryptographie post-quantique dans une certaine mesure. Il est à noter qu'à l'heure actuelle, aucune mesure spécifique n'est prévue.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms* (disponible en anglais seulement)

IEC 62351-3:— [1], *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 62351-4, *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 62351-5, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 5: Aspects de sécurité pour l'IEC 60870- 5 et ses dérivés*

IEC 62351-6, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 6: Sécurité pour l'IEC 61850*

IEC 62351-14:— [2], *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging* (disponible en anglais seulement)

ISO/IEC 9594-8:2020, Rec. UIT-T X.509 (2019), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire – Partie 8: Cadre général des certificats de clé publique et d'attribut*

ISO/IEC 9594-11:2020, Rec. UIT-T X.510 (2020), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire – Partie 11: Spécifications de protocole pour un fonctionnement sécurisé*

ISO/IEC 9834-1:2012, Rec. UIT-T X.660 (2011), *Technologies de l'information – Procédures opérationnelles des autorités d'enregistrement des identificateurs d'objet – Partie 1: Procédures générales et arcs sommitaux de l'arborescence des identificateurs d'objet internationale*

IETF RFC 5272, *Certificate Management over CMS (CMC)* (disponible en anglais seulement)

IETF RFC 5755, *An Internet Attribute Certificate Profile for Authorization* (disponible en anglais seulement)

IETF RFC 5934, *Trust Anchor Management Protocol (TAMP)* (disponible en anglais seulement)

IETF RFC 6407, *The Group Domain of Interpretation* (disponible en anglais seulement)

_____

[1] En cours d'élaboration. Stade au moment de la publication: IEC/RFDIS 62351-3:2023.

[2] En cours d'élaboration. Stade au moment de la publication: IEC/ACDV 62351-14:2023.

IETF RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP* (disponible en anglais seulement)

IETF RFC 7030, *Enrolment over Secure Transport* (disponible en anglais seulement)

IETF RFC 8052, *Group Domain of Interpretation (GDOI) Protocol Support for IEC 62351 Security* (disponible en anglais seulement)

IETF RFC 8263, *Group Domain of Interpretation (GDOI) GROUPKEY-PUSH Acknowledgement Message* (disponible en anglais seulement)

IETF RFC 8894, *Simple Certificate Enrolment Protocol* (disponible en anglais seulement)