IEC 62351-3

Edition 2.0 2023-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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 62351-3:2023-06(en-fr)

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 300 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 19 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

IEC 62351-3

Edition 2.0 2023-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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 978-2-8322-6935-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 3: Communication network and system security – Profiles including TCP/IP

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 62351-3 has been prepared by IEC technical committee 57: Power systems management and associated information exchange. It is an International Standard.

This second edition cancels and replaces the first edition published in 2014, Amendment 1:2018 and Amendment 2:2020. This edition constitutes a technical revision.

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

a) Inclusion of the TLSv1.2 related parameter required in IEC 62351-3 Ed.1.2 to be specified by the referencing standard. This comprises the following parameter:
   - Mandatory TLSv1.2 cipher suites to be supported.
   - Specification of session resumption parameters.
   - Specification of session renegotiation parameters.

- Revocation handling using CRL and OCSP.
- Handling of security events.

b) Inclusion of a TLSv1.3 profile to be applicable for the power system domain in a similar way as for TLSv1.2 session.

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

Draft	Report on voting
57/2578/FDIS	57/2593/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) are presented in `courier new` and **`bold courier new`**

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 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.

INTRODUCTION

This edition of IEC 62351-3 is a self-contained document profiling the usage of TLS for to secure power system communication. It is recommended to refer to this edition of this document rather than any previous edition, because this edition updates the utilized cryptographic algorithms (ciphersuites), provides enhanced functionality, and covers different TLS versions. In contrast to previous editions, this document specifies all necessary TLS specific settings and does not require the referencing standard to define specific settings for TLS.

Note that the recommendation to use this edition, potentially also with older referencing standards, requires technical support by implementations of the TLS settings specified in this edition of the document.

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

Part 3: Communication network and system security – Profiles including TCP/IP

1 Scope

1.1 Scope

This part of IEC 62351 specifies how to provide confidentiality, integrity protection, and message level authentication for protocols that make use of TCP/IP as a message transport layer and utilize Transport Layer Security when cyber-security is required. This may relate to SCADA/telecontrol, protection, automation and control protocols.

IEC 62351-3 specifies how to secure TCP/IP-based protocols through constraints on the specification of the messages, procedures, and algorithms of Transport Layer Security (TLS) (TLSv1.2 defined in RFC 5246, TLSv1.3 defined in RFC 8446). In the specific clauses, there will be subclauses to note the differences and commonalities in the application depending on the target TLS version. The use and specification of intervening external security devices (e.g., "bump-in-the-wire") are considered out-of-scope.

In contrast to previous editions of this document, this edition is self-contained in terms of completely defining a profile of TLS. Hence, it can be applied directly, without the need to specify further TLS parameters, except the port number, over which the communication will be performed. Therefore, this part can be directly utilized from a referencing standard and can be combined with further security measures on other layers. Providing the profiling of TLS without the need for further specifying TLS parameters allows declaring conformity to the described functionality without the need to involve further IEC 62351 documents.

This document is intended to be referenced as a normative part of other IEC standards that have the need for providing security for their TCP/IP-based protocol exchanges under similar boundary conditions. However, it is up to the individual protocol security initiatives to decide if this document is to be referenced.

The document also defines security events for specific conditions, which support error handling, security audit trails, intrusion detection, and conformance testing. Any action of an organization in response to events to an error condition described in this document are beyond the scope of this document and are expected to be defined by the organization's security policy.

This document reflects the security requirements of the IEC power systems management protocols. Should other standards bring forward new requirements, this document may need to be revised.

1.2 Intended audience

The initial audience for this document is intended to be experts developing or making use of protocols in the field of power systems management and associated information exchange. For the measures described in this document to take effect, they must be accepted and referenced by the specifications of protocols making use of TCP/IP security by applying TLS. This document is written to enable that process.

The subsequent audience for this document is intended to be the developers of products that implement these protocols.

Portions of this document may also be of use to managers and executives in order to understand the purpose and requirements of the work.

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 62351-1:2007, *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*

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

RFC 5246:2008, *The TLS Protocol Version 1.2*[1]

RFC 5280:2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 5288:2008, *AES Galois Counter Mode (GCM) Cipher Suites for TLS*

RFC 5289:2008, *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*

RFC 5746:2010, *Transport Layer Security (TLS) Renegotiation Indication Extension*

RFC 6066:2011, *Transport Layer Security Extensions*

RFC 6176:2011, *Prohibiting Secure Sockets Layer (SSL) Version 2.0*

RFC 8422:2018, *ECC Cipher Suites for TLSv1.2 and earlier*

RFC 8446:2018, *The TLS Protocol Version 1.3*

RFC 9150:2021, *TLS 1.3 Authentication and Integrity only Cipher Suites*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 62351-2 and the following apply.

[1] This is typically referred to as SSL/TLS.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.2 Abbreviated terms

ACSE	Association Control Service Element
AEAD	Authenticated Encryption with Associated Data
BCP	Best Current Practice
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DH(E)	Diffie Hellman (Ephemeral) Key Agreement (see also IEC 62351-9)
ECDH(E)	Elliptic Curve based Diffie Hellman (Ephemeral) Key Agreement (see also IEC 62351-9)
ECDSA	Elliptic Curve Digital Signature Algorithm
IV	Initialization Vector
MAC	Message Authentication Code
MitM	Man-in-the-Middle (type of attack)
OCSP	Online Certificate Status Protocol (see RFC 6960)
PICS	Protocol Implementation Conformance Statement
PIXIT	Protocol Implementation eXtra Information for Testing
PSK	Pre-shared key
TLS	Transport Layer Security

4 Security issues addressed by this document

4.1 General

The IEC power system environment has different operational requirements from many Information Technology (IT) applications that make use of TLS to protect the transport of information over a TCP/IP connection. This requires on one hand the management of certificates used to authenticate entities, which is handled in IEC 62351-9. On the other hand, specific TLS related security parameters such as selected cipher suites, session management parameter and utilized extensions need to be defined, which is the focus of this document. One main difference in the application of TLS in the power system domain is the duration of the TCP/IP connection for which security needs to be maintained. Besides this it also has to be considered that the equipment in power system automation is long lasting. This may also require supporting older versions of TLS or cipher suites to retain backward compatibility.

Many IT protocols have short duration connections, which allow the encryption algorithms to be renegotiated at connection re-establishment. However, the connections within a telecontrol environment tend to have longer durations, often "permanent". It is the longevity of connections in the field of power systems management and associated information exchange that give rise to the need for specific consideration. In this regard, in order to provide protection for the "permanent" connections, a mechanism for updating the session key is selected within this document, based upon existing TLS features. Note that TLSv1.2 and TLSv1.3 support different approaches for rekeying.

TLS allows for a wide variety of settings such as selected cipher suites to protect the handshake and the record layer protocol, which are negotiated during connection establishment. It also supports session management mechanisms to setup new sessions or renew existing sessions. To ensure interoperability between different implementations, this document specifies a common set of TLS features to be supported by conforming implementations.

TLS has evolved and is available in version 1.3. In version 1.3 several parts of the protocol have been reworked, resulting in a protocol, which is functionally not backward compatible to TLSv1.2. As the first message exchange is defined in a backward compatible way, the TLS server may be able to switch to either version, depending on the security policy.

Additionally, this document specifies the use of particular TLS capabilities that allow for specific security threats to be countered (see also 4.2). Specifically, TLS allows the definition of extensions to the protocol to mitigate potential protocol vulnerabilities or to enhance protocol functionality. This specification makes use of already-defined extensions.

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

NOTE It is assumed that the certificate management necessary to operate TLS is addressed in accordance with IEC 62351-9.

4.2 Security threats countered

See IEC TS 62351-1 for a discussion of security threats and attack methods.

TCP/IP and the security specifications in this document cover only the communication transport layers (OSI layers 4 and lower). Specifically, TLS protects the transported messages from OSI layer 5 and above in a transparent way. This document does not cover security functionality specific for the communication application layers (OSI layers 5 and above) or application-to-application security. This is defined in other parts of IEC 62351, e.g., IEC 62351-4 for MMS, IEC 62351-5 for serial communication and telecontrol, and IEC 62351-6 for (R)GOOSE and (R)SV.

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

The specific threats countered in this document for the transport layer include:

– Tampering (unauthorized modification or insertion of messages) is addressed by mutual, certificate-based authentication of the communication participants, and TLS packet-level integrity protection.

Additionally, when the information has been identified as requiring confidentiality protection:

– Unauthorized access to information through TLS packet-level encryption of the messages.

4.3 Attack methods countered

The following security attack methods are countered through the appropriate implementation of the specifications and recommendations in this document.

– Impersonation: This threat is countered through the use of mutual authentication based on X.509 certificates during the TLS handshake and digitally signed information as revocation information.
– Man-in-the-middle (MitM): This threat is countered for the TLS record layer through the use of cryptographic checksums (MAC) based on mutually authenticated negotiation of session keys. These keys are set up during the TLS handshake. Protection against MitM attacks during the TLS handshake phase itself is provided by the `Finish` message, ending the handshake phase. This message is encrypted and contains a hash value over all messages

exchanged in the handshake. In addition, TLSv1.3 already provides cryptographic protection of the handshake messages directly (except the `ClientHello`)..

– Replay: This threat is countered by the application of a MAC for integrity protection on a per packet bases including a sequence number to detect an actual replay.

– Eavesdropping: This threat is countered through the use of encryption cipher suites, when negotiating TLS record layer security.

NOTE The actual performance characteristics of an implementation claiming conformance to this part of the IEC 62351 series are out-of-scope of this document.

4.4 Handling of security events

Throughout the document security events are defined. These security events are intended to support error handling and thus to increase system resilience. Implementations should provide a mechanism for announcing security events to an evaluation system. A recommended standard is IEC 62351-4.

The information about security events and potential detailed information can only be provided by the entity based on the availability of this information through the underlying platform or utilized components.

It is recommended that the security events defined throughout this document are made available to the operational infrastructure by cyber security events as specified in IEC 62351-14 or by monitoring objects as specified in IEC 62351-7. Annex A provides a mapping of the defined events in this document to the notion of IEC 62351-14.

Note that notice, warnings, errors, and alarms are used to indicate the severity of an event from a security point of view. The following notion from IEC 62351-14 is used:

– A notice refers to a cyber security related activity during the routine use or maintenance of an entity. It does not relate to a cyber security breach or attack or deviation from the normal operating condition of an entity.

– A warning is a deviation from the normal operating condition of an entity but not necessary a cyber-attack.

– An error describes an unforeseen condition, which may indicate unauthorized activity. It may not require immediate action.

– An alarm is an indication of a serious problem, which may indicate unauthorized activity. Action is recommended to be taken immediately.

In any case, it is expected that an organization’s security policy determines the final handling of events based on the operational environment. For instance, the assessment of one or more alarms could rise to the level of an incident.

5 Overview of differences in TLS versions

5.1 General

This clause provides a short overview about the main differences between the TLS version 1.2 and TLS version 1.3. Specifically addressed is the naming of cipher suites, backward compatibility, and extensions, which have been used in previous version of this standard.

5.2 Main differences between TLSv1.2 and TLSv1.3

In the following the main differences between TLSv1.2 and TLSv1.3 for the different subprotocols (TLS Handshake, TLS Record Layer) are listed (note that RFC 8446 provides a complete list of changes from TLSv1.2 to TLSv1.3), which have a relation to features used in TLSv1.2 in IEC 62351-3:

– Fewer handshake roundtrips in TLSv1.3 (one roundtrip for unilateral authenticated sessions, 1.5 for mutual authentication).
– TLSv1.3 handshake messages are encrypted, except the `ClientHello` and parts of the `ServerHello` are send in plain. Note that there is ongoing work in the IETF to define extensions to allow to encrypt part of the `ClientHello`, like the Server Name Indication (SNI) resulting in an encrypted SNI (ESNI) or encrypting the whole `ClientHello` as encrypted `ClientHello` (ECH).
– TLSv1.3 removes support for obsolete and vulnerable cryptographic algorithms: Export ciphers, DES, 3DES, AES-CBC, RC4, MD5, SHA-1 are no longer supported
– TLSv1.3 changes in key establishment
  • Removal of arbitrary Diffie-Hellman groups
  • Key establishment is based on ephemeral Diffie-Hellman
  • No support for RSA key encryption
– TLSv1.3 removes session renegotiation but provides post-handshake messages for key and IV update as well as client authentication.
– TLSv1.3 simplifies session resumption by using PSK and Session Tickets
– TLSv1.3 introduces post handshake messages for
  • Session Ticket
  • Client authentication
  • Key and IV Update
– TLSv1.3 removes the multistapling support of OCSP responses according to RFC 6961 (status_request_v2). It has been replaced with a direct variant allowing the stapling of OCSP response to certificates in a chain by an extension of a `CertificateEntry`.
– TLSv1.3 introduces OCSP stapling for client certificates, which may be important specifically for industrial use cases, in which the server often resides on the field device with potential limited capability of checking revocation state of received certificates
– TLSv1.3 removes non-AEAD cipher suites for TLS record layer protection. Note that integrity-only cipher suites have been defined in RFC 9051.
– TLSv1.3 provides the option to have already encrypted application data in the first roundtrip (0-RTT) with some reductions in the security (option for replay by an attacker). Note that this option is explicitly not used in this document.
– Note that `ChangeCipherSpec` is an independent TLSv1.2 protocol content type and is not a TLS handshake message. `ChangeCipherSpec` was removed in TLSv1.3.

5.3 Cipher suite naming

The changes in the TLS handshake and record layer handling in TLSv1.3 are also reflected in the cipher suite definition.

A cipher suite in TLSv1.2 and before combines algorithms for authentication and key agreement during the TLS handshake as well as algorithms for encryption and message authentication (integrity) for the record layer as shown in Figure 1. The cipher suite therefore considered both, the TLS handshake as well the record layer. Typically, each cipher suite has a name, which consists of a set of mnemonics separated by underscores and has the form shown in Figure 1.