SLOVENSKI STANDARD
oSIST prEN 62351-4:2017

01-september-2017

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

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

Ta slovenski standard je istoveten z: prEN 62351-4:2017

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

oSIST prEN 62351-4:2017 en

57/1860/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: **IEC 62351-4 ED1**	
DATE OF CIRCULATION: **2017-05-19**	CLOSING DATE FOR VOTING: **2017-08-11**
SUPERSEDES DOCUMENTS: **57/1476/RR**	

IEC TC 57 : POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE			
SECRETARIAT: Germany		SECRETARY: Mr Heiko Englert	
OF INTEREST TO THE FOLLOWING COMMITTEES:		PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.	
FUNCTIONS CONCERNED:			
☐ EMC	☐ ENVIRONMENT	☐ QUALITY ASSURANCE	☐ SAFETY
☒ SUBMITTED FOR CENELEC PARALLEL VOTING **Attention IEC-CENELEC parallel voting** The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.		☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING	

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

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

NOTE FROM TC/SC OFFICERS:

This project was originally intended to be circulated as a CD (see 57/1476/RR) . After further considerations between the WG, the project leader and the TC 57 secretariat it has been agreed to rather issue a CDV. The existing publication IEC TS 62351-4 Edition 1 will be cancelled and replaced once the present document is published as an international standard.

1

Document history

Any person intervening in the present document is invited to complete the table below before sending the document elsewhere. The purpose is to allow all actors to see all changes introduced and the intervening persons.

Any important message to IEC editors should also be included in the table below.

Name of intervening person	Document received		Brief description of the changes introduced	Document sent	
	From	Date		To	Date
Erik Andersen			Base document	Steffen Fries	8 July 2016
Steffen Fries	Erik Andersen	8 July 2016	Updates and comments, including TLS	Erik Andersen	12 July 2016
Erik Andersen	Steffen Fries	12 July 2016	Further editing and proof reading	Steffen Fries	16 Oct. 2016
Steffen Fries	Erik Andersen	16 Oct. 2016	Clean-up the TLS	Erik Andersen	1 November
Erik Andersen	Steffen Fries	1 November, 2016	Complete rework of text	Steffen Fries	1 March 2017
Steffen Fries	Erik Andersen	1 March, 2017	Solutions for open questions in TLS section, general review comments and enhancements	Erik Andersen	3 March 2017
M. Noeth	E. Anderson	2017-03-14	CD document	CO	2017-03-15

Table of Content

FOREWORD 1
SECTION 1 – GENERAL 3
1 Scope and object 3
1.1 Scope 3
1.2 Object 3
2 Normative references 3
3 Terms, definitions and abbreviations 5
3.1 Defined terms and definitions 5
3.2 Additional definitions 5
3.3 Defined abbreviations 7
3.4 Additional abbreviations 7
4 Security issues addressed by this part of IEC 62315 8
4.1 Security for application and transport profiles 8
4.2 Security threats countered 8
4.3 Attack methods countered 8
4.4 Logging 9
5 Bilateral Agreements 9
SECTION 2 – T-PROFILE 11
6 T-profile security 11
6.1 General 11
6.2 Use of Transport Layer Security (TLS) 11
6.2.1 Disabling of TLS 12
6.2.2 TLS cipher suites support 12
6.2.3 TLS session resumption 13
6.2.4 Individual public-key certificate components 13
6.2.5 Supported number of Certification Authorities 13
6.2.6 TCP ports 13
6.2.7 Public-key certificate size 13
6.2.8 Evaluation period for revocation state of public-key certificates 14
6.2.9 Public-key certificate validation 14
6.2.10 Security events handling 14
SECTION 3 – APPLICATION SECURITY PROFILES OVERVIEW 15
7 Application security profile overview (informative) 15
8 Use of cryptographic algorithms (informative) 15
8.1 Basic cryptographic definitions 15
8.2 Public-key algorithms 16
8.3 Signature algorithms 16
8.4 Symmetric encryption algorithms used for encryption only 17
8.5 Authenticating encryption algorithms 17
8.6 Integrity check value algorithms 18
9 Object identifier allocation (normative) 18
10 General OSI upper layer requirements (normative) 19
10.1 Overview 19
10.2 General on OSI upper layer requirements 19
10.3 Session protocol requirements 20
10.4 Presentation protocol requirements 20
10.4.1 Context list 20

10.4.2 Abstract syntaxes 20
10.4.3 Presentation user data 21
10.4.4 ASN.1 encoding requirements 21
10.5 Association control service element (ACSE) protocol requirements 21
10.5.1 Protocol version 21
10.5.2 Titles 21
10.5.3 Use of ASN.1 EXTERNAL data type 22
SECTION 4 – MMS A-SECURITY-PROFILE 22
11 OSI requirements specific to A-security profile (normative) 22
11.1 Introduction 22
11.2 Presentation protocol requirement 23
11.3 ACSE requirements 23
11.3.1 Functional unit selection 23
11.3.2 Application context 23
11.3.3 Authentication mechanism 23
11.3.4 Authentication value 23
12 MMS Authentication value (normative) 24
12.1 MMS-Authentication value data type 24
12.2 Handling of the association request (AARQ-apdu) 24
12.2.1 AARQ-apdu handling by the client 24
12.2.2 AARQ-apdu handling by the server 25
12.3 Handling of the association result (AARE-apdu) 25
12.3.1 AARE-apdu handling by the server 25
12.3.2 AARE-apdu handling by the client 25
SECTION 5 – END-TO-END APPLICATION SECURITY PROFILES 26
13 Overview and overall principles 26
13.1 Basic concepts 26
13.2 Relationship between E2E-security and the protected application protocol 26
13.3 E2E-security interface to protected application protocol 27
13.3.1 General 27
13.3.2 ASN.1 as schema definition 27
13.3.3 XML Schema Definition (XSD) 28
14 Specific requirements for an OSI environment 28
14.1 Introduction 28
14.2 Additional presentation layer requirements 29
14.3 Additional ACSE requirements 29
14.4 Specific OSI related protocol elements 29
14.4.1 OSI wrapping for E2E-security handshake 29
14.4.2 OSI wrapping for E2E-security data transfer 30
15 Association management 30
15.1 General concept 30
15.2 General syntax 30
15.3 Handshake request and accept 30
15.3.1 General 30
15.3.2 OSI specific considerations 31
15.3.3 NON-OSI specific considerations 31
15.4 Association reject by the protected application protocol 31
15.4.1 General 31
15.4.2 OSI specific considerations 32

15.4.3 NON-OSI specific considerations 32
15.5 Association reject due to security issues 32
15.5.1 General 32
15.5.2 OSI specific considerations 32
15.5.3 Non-OSI specific considerations 33
15.6 Data transfer security abort 33
15.6.1 General syntax 33
15.6.2 OSI specific considerations 33
15.6.3 Non-OSI specific considerations 33
16 Data transfer phase 33
16.1 Normal data transfer 33
16.1.1 General syntax 33
16.1.2 OSI specific considerations 34
16.1.3 Non-OSI specific considerations 34
16.2 Abort by protected application protocol 34
16.2.1 General 34
16.2.2 OSI specific considerations 34
16.2.3 Non-OSI specific considerations 34
17 ClearToken data types 34
17.1 The ClearToken1 data type 34
17.1.1 General syntax 34
17.1.2 Supported signature algorithms 35
17.1.3 Diffie-Hellman set 36
17.1.4 Shared keys derivation 36
17.1.5 Confidentiality parameters 37
17.1.6 Certification path 37
17.1.7 Supported integrity algorithms 38
17.2 The ClearToken2 data type 38
17.3 The ClearToken3 data type 39
18 Authentication and integrity specifications 39
18.1 The Signature data type 39
18.2 The authenticator data type 39
19 E2E-security error handling 40
19.1 Handshake diagnostics 40
19.2 The data transfer diagnostics 41
20 Procedure for checking association request (normative) 42
20.1 E2E-security carrier checking 42
20.1.1 E2E-security carrier checking within an OSI environment 42
20.1.2 E2E-security carrier checking within a non-OSI environment 42
20.2 Checking of E2E-security handshake request 42
20.2.1 E2E-security handshake request in an OSI environment 42
20.2.2 General checking of E2E-security Handshake request 43
21 Procedure for checking association result (normative) 43
21.1 E2E-security carrier checking 44
21.1.1 E2E-security carrier checking within an OSI environment 44
21.1.2 E2E-security carrier checking within a non-OSI environment 44
21.2 Specific checking of E2E-security handshake result 44
21.2.1 E2E-security handshake in an OSI environment 44
22 Checking of security parameters during data transfer 44

22.1 Checking within an OSI environment ... 44
22.2 Checking within a non-OSI environment ... 44
22.3 Common checking ... 45
22.3.1 Overall checking ... 45
22.3.2 Authenticator checking ... 45
22.3.3 Checks of the ClearToken2 value ... 45
23 Application layer routing ... 45
23.1 General on application layer routing ... 45
23.2 Application layer routing in an OSI environment ... 46
23.3 Application layer routing in a non-OSI environment ... 46
24 Conformance to this part of IEC 62351 ... 47
24.1 General ... 47
24.2 T-Profile Conformance ... 47
24.3 A-Profile Conformance ... 47
24.4 Conformance of IEC 60870-6 TASE.2 Security ... 47
Annex A (normative) Formal ASN.1 specification for the A-security profile ... 48
Annex B (normative) Formal ASN.1 specification for the End-to-End security ... 49
Annex C (normative) Formal XSD specification for the End-to-End security ... 55
Annex D (normative) End-entity public-key certificate specification ... 60
D.1 Scope of annex ... 60
D.2 General requirement ... 60
D.3 Specific OSI application considerations ... 60
D.4 Basic Structure requirement and recommendations ... 60
D.4.1 Version component ... 60
D.4.2 Serial number component ... 60
D.4.3 Issuer signature algorithm component ... 60
D.4.4 Issuer component ... 61
D.4.5 Validity component ... 61
D.4.6 Subject component ... 61
D.4.7 Subject public key Information component ... 61
D.4.8 Issuer unique ID and subject unique ID components ... 61
D.5 Extensions ... 61
D.5.1 Key usage extension ... 62
D.5.2 Subject alternative name extension ... 62
D.5.3 Revocation checking ... 62
D.5.4 IEC user role information extension ... 62
Annex E (normative) Lower layer requirements ... 63
E.1 Scope of annex ... 63
E.2 Transport protocol class 0 ... 63
E.2.1 Enforcement of maximum lengths ... 63
E.2.2 Response to Class 0 unsupported TPDUs ... 63
E.2.3 Transport selectors ... 63
E.3 IETF RFC 1006 ... 63
E.3.1 Version number ... 63
E.3.2 Length ... 64
E.3.3 Keep-alive ... 64
Annex F (informative) ASN.1 definition of ACSE ... 65
Bibliography ... 69

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

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

Part 4: Profiles including MMS and derivatives

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.

International Standard IEC 62351-4 has been prepared by IEC technical committee 57: Power systems management and associated exchange.

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

FDIS	Report on voting
XX/XX/FDIS	XX/XX/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

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.

In this part of IEC 62351, the following print types are used:

– Abstract Syntax Notation One (ASN.1) and XML Schema Definition (XSD) notions are presented in bold Courier New typeface;

– when ASN.1 types and values are referenced in normal text, they are differentiated from normal text by presenting them in bold Courier New typeface.

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 publication will remain unchanged until the stability date indicated on the IEC web site 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.

The National Committees are requested to note that for this publication the stability date is ....

THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED AT THE PUBLICATION STAGE.

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

Part 4: Profiles including MMS and derivatives

SECTION 1 – GENERAL

Scope and object

1.1 Scope

This second edition of this part of IEC 62351 substantially extents the scope of the first edition. While the first edition primarily provided some limited support for authentication during handshake for the Manufacturing Message Specification (MMS) based applications, this second edition provides support for extended integrity and authentication both for the handshake phase, and for the data transfer phase. In addition, it provides for shared key management and data transfer encryption and it provides security end-to-end (E2E) with zero or more intermediate entities. While the first edition only provides support for systems based on the MMS, i.e., systems using Open Systems Interworking (OSI) protocols, this second edition also provides support for application protocols using other protocol stacks, e.g., a TCP/IP protocol stack. This support is extended to protect application protocols using XML encoding and other protocols that have a handshake that can support the Diffie-Hellman key exchange. This extended security is referred to as E2E-security.

It is intended that this part of IEC 62351 be referenced as normative part of IEC TC 57 standards that have a need for using application protocols, e.g., MMS, in a secure manner.

It is anticipated that there are implementation, in particular Inter-Control Centre Communications Protocol (ICCP) implementations that are dependent on the first edition of this part of IEC 52315. The first edition specification of the A-security-profile is therefore included as separate sections. Implementations supporting this A-security-profile will interwork with implementation supporting the first edition of this part of IEC 62351.

Special diagnostic information is provided for exception conditions for E2E-security.

This part of IEC 62351 represents a set of mandatory and optional security specifications to be implemented for protected application protocols.

1.2 Object

The initial audience for this part of IEC 62351 is the members of the working groups developing or making use of the protocols within IEC TC 57. For the measures described in this part of IEC 62351 to take effect, they shall be accepted and referenced by the specifications for the protocols themselves.

The subsequent audience for this part of IEC 62351 is the developers of products that implement these protocols.

Portions of this part of IEC 62351 may also be of use to managers and executives in order to understand the purpose and requirements of the work.

Normative references

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.

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 62351-3:2014, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*.

IEC 62351-8:2011, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control Role-based access control*.

IEC 62351-9:201x, *Power systems management and associated information exchange – Data and communications security – Part 9:* Key Management

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 9506-1:2003, *Industrial automation systems — Manufacturing Message Specification – Part 1: Service definition*.

ISO 9506-2:2003, *Industrial automation systems — Manufacturing Message Specification – Part 2: Protocol specification*.

ISO/IEC 8073:1997 | Rec. ITU-T X.224 (1995), *Information technology – open systems interconnection – Protocol for providing the connection-mode transport service*.

ISO/IEC 8823-1:1994 | Rec. ITU-T X.226 (1994), *Information technology – open systems interconnection – connection-oriented presentation protocol: Protocol specification*.

Rec. ITU-T X.127 (1995), *Information technology – open systems interconnection – service definition for the association control service element*.

NOTE 1 – The corresponding International Standard ISOIEC 8649:1996 has been withdrawn.

Rec. ITU-T X.227 (1995), *Information technology – open systems interconnection – connection-oriented protocol for the association control service element: Protocol specification*.

NOTE 2 – The corresponding International Standard ISOIEC 8650-1:1996 has been withdrawn.

Rec. ITU-T X.227 (1995)/Amd.1 (1996), *Information technology – open systems interconnection – connection-oriented protocol for the association control service element: Protocol specification – Amendment 1: Incorporation of extensibility markers.*

NOTE 3 – The corresponding International Standard amendment ISO/IEC 8650-1:1996/Amd.1:1997 has been withdrawn.

ISO/IEC 8824-1:2015 | Rec. ITU-T X.680 (2015), *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

ISO/IEC 8825-1:2015 | Rec. ITU-T X.690 (2015), *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.

ISO/IEC 8825-4:2015 | Rec. ITU-T X.693 (2015), *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)*.

IETF RFC 1006:1987, *ISO Transport Service on top of the TCP, Version: 3*.

IETF RFC 3447:2003, *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*.

IETF RFC 3526:2003, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*.

IETF RFC 5114:2008, *Additional Diffie-Hellman Groups for Use with IETF Standards*.

IETF RFC 5246:2008, *The Transport Layer Security (TLS) Protocol, Version 1.2*.

Terms, definitions and abbreviations

3.1 Defined terms and definitions

For the purpose of this part of IEC 62351, the terms and definitions given in IEC TS 62351-2 apply.

3.2 Additional definitions

3.2.1
abstract syntax
The specification of application-protocol-data-units by using notation rules that are independent of the encoding technique used to represent them.

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

3.2.2
application entity
An active element embodying a set of capabilities which is pertinent to communication systems and which is defined for the application layer.

3.2.3
application-context
A set of rules shared in common by two application-entity invocations in order to support an association.

[SOURCE: ISO/IEC 9545:1994 | Rec. ITU-T X.207 (1993), 3.4.5 (slightly modified)]

3.2.4
application security profile
Those aspects of an application profile that relates to security.

3.2.5
application-service-element
A set of application functions that provides a capability for the interworking of application-entity invocations for a specific purpose.

[SOURCE: ISO/IEC 9545:1994 | Rec. ITU-T X.207 (1993), 3.4.8]

3.2.6
association
A cooperative relationship among application-entity invocations, which enables the communication of information and the coordination of their joint operation for an instance of communication. This relationship may be formed by the transfer of application-protocol-control-information using an underlying service.

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

3.2.7
association control service element
An application service element that provides the exclusive means for establishing and terminating application associations within an OSI environment.

[SOURCE: ISO/IEC 9545:1994 | Rec. ITU-T X.207 (1993), 3.2.4 (slightly modified)]

3.2.8
bilateral agreement
Agreement between two control centres which includes the data elements to be accessed and the means to access them.

[SOURCE: IEC 60870-6-503:2014, 3.3]

3.2.9
bilateral table
Computer representation of the bilateral agreement. The representation used is a local matter.

[SOURCE: IEC 60870-6-503:2014, 3.4]

3.2.10
certification path
An ordered list of one or more public-key certificates, starting with a public-key certificate signed by the trust anchor, and ending with the end-entity public-key certificate to be validated. All intermediate public-key certificates, if any, are CA certificates in which the subject of the preceding public-key certificate is the issuer of the following public-key certificate.

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

3.2.11
data transfer phase
The phase from the completion of the establishment of an association to the initiation of the association termination.

Note 1 to entry: In some specifications, this phase is termed a session. This term is avoided here, as it is used within the OSI architecture and within TLS.

3.2.12
E2E-security
A common term for the security facilities provided by the A-plus-security-profile and/or the AE-plus-security-profile.

3.2.13
end-to-end application profile
An application profile that specifies end-to-end security at the application layer between two application entities with possible intermediate relaying application entities.

3.2.14
first edition operation
A scenario where the partners in an association or an association establishment using the A-security-profile and thereby providing operability with an implementation conforming to the first edition of this part of IEC 62351.

3.2.15
key derivation function
A function that maps octet strings of any length to octet strings of an arbitrary, specified length, such that it computationally infeasible to find correlations between inputs and outputs, and such that given one part of the output, but not the input, it is computationally infusible to predict any bit of the remaining output. The precise security requirements depend on the application.

[SOURCE: ISO/IEC 18033-2:2007, 3.25]

3.2.16
nonce
Number used once.

[SOURCE: ISO/IEC 9797-3:2012, 3.3]

3.2.17
presentation data value
The unit of information specified in an abstract syntax, which is transferred by the underlying service.

[SOURCE: ISO/IEC 8822:1994 | Rec. ITU-T X.216 (1994), 3.4.6]

3.2.18
protected application protocol
An application protocol that is protected by the E2E-security.

3.2.19
second edition operation
A scenario where the partners in an association or an association establishment using E2E-security according to this part of IEC 62351.

3.3 Defined abbreviations

For the purpose of this part of IEC 62351, the abbreviations given in IEC TS 62351-2 apply.

3.4 Additional abbreviations

ACSE	Association Control Service Element
APDU	Application Protocol Data Unit
ASE	Application Service Element
CBC	Cipher Block Chaining
DHE	Ephemeral Diffie-Hellman
E2E	End-to-End
ECDHE	Elliptic Curve Ephemeral Diffie-Hellman
GCM	Galois/Counter Mode
GMAC	Galois Message Authentication Code
HMAC	Keyed-hash Message Authentication Code
ICCP	Inter-Control Centre Communications Protocol
ICV	Integrity Check Value
MAC	Message Authentication Code
OCSP	Online Certificate Status Protocol
PDU	Protocol Data Unit
PDV	Presentation Data Value
SDU	Service Data Unit
SPDU	Session Protocol Data Unit
TASE.2	Telecontrol Application Service Element 2
TPDU	Transport Protocol Data Unit
VPN	Virtual Private Network
XER	XML Encoding Rules
XML	eXtensible Markup Language
XSD	XML Schema Definition