



BSI Standards Publication

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)

National foreword

This British Standard is the UK implementation of EN 62351-9:2017. It is identical to IEC 62351-9:2017.

The UK participation in its preparation was entrusted to Technical Committee PEL/57, Power systems management and associated information exchange.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2017
Published by BSI Standards Limited 2017

ISBN 978 0 580 94718 6

ICS 33.200

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2017.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

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

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 (dop) 2018-03-22
implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2020-06-22
standards conflicting with the
document have to be withdrawn

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

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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	Information technology - Open Systems Interconnection - The Directory -	-	-
Rec. ITU-T X.509	2016	Part 8: Public-key and attribute certificate frameworks	-	-
ISO/IEC 9834-1/	2012	Information technology - Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree	-	-
Rec. ITU-T X.660	2011		-	-
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

This page deliberately left blank

CONTENTS

FOREWORD.....	6
1 Scope.....	8
2 Normative references	8
3 Terms and definitions	9
4 Abbreviations and acronyms.....	14
5 Cryptographic applications for power system implementations.....	15
5.1 Cryptography, cryptographic keys, and security objectives.....	15
5.2 Types of cryptography	16
5.3 Uses of cryptography	16
5.3.1 Goals of cyber security	16
5.3.2 Confidentiality.....	17
5.3.3 Data integrity	17
5.3.4 Authentication.....	18
5.3.5 Non-repudiation	18
5.3.6 Trust.....	18
6 Key management concepts and methods in power system operations	19
6.1 Key management system security policy	19
6.2 Key management design principles for power system operations	19
6.3 Use of Transport Layer Security (TLS)	19
6.4 Cryptographic key usages.....	19
6.5 Trust using a public-key infrastructure (PKI).....	20
6.5.1 Registration authorities (RA).....	20
6.5.2 Certification authority (CA)	20
6.5.3 Public-key certificates	20
6.5.4 Attribute certificates.....	21
6.5.5 Public-key certificate and attribute certificate extensions	21
6.6 Trust via non-PKI self-signed certificates	22
6.7 Authorization and validation lists.....	22
6.7.1 General	22
6.7.2 AVLs in non-constrained environments	23
6.7.3 AVLs in constrained environments	23
6.7.4 Use of self-signed public-key certificates in AVLs	23
6.8 Trust via pre-shared keys.....	23
6.9 Session keys	24
6.10 Protocols used in trust establishment.....	24
6.10.1 Certification request	24
6.10.2 Trust Anchor Management Protocol (TAMP)	24
6.10.3 Simple Certificate Enrolment Protocol (SCEP)	24
6.10.4 Internet X.509 PKI Certificate Management Protocol (CMP).....	24
6.10.5 Certificate Management over CMS (CMC)	25
6.10.6 Enrolment over Secure Transport (EST)	25
6.10.7 Summary view on the different protocols	25
6.11 Group keys	26
6.11.1 Purpose of group keys.....	26
6.11.2 Group Domain of Interpretation (GDOI)	26
6.12 Key management lifecycle	31

6.12.1	Key management in the life cycle of an entity	31
6.12.2	Cryptographic key lifecycle	32
6.13	Certificate management processes	34
6.13.1	Certificate management process	34
6.13.2	Initial certificate creation	34
6.13.3	Enrolment of an entity	34
6.13.4	Certificate signing request (CSR) process	36
6.13.5	Certificate revocation lists (CRLs)	37
6.13.6	Online certificate status protocol (OCSP)	38
6.13.7	Server-based certificate validation protocol (SCVP)	41
6.13.8	Short-lived certificates	41
6.13.9	Certificate renewal	42
6.14	Alternative process for asymmetric keys generated outside the entity	43
6.15	Key distribution for symmetric keys with different time frames	44
7	General key management requirements	44
7.1	Asymmetric and symmetric key management requirements	44
7.2	Required cryptographic materials	44
7.3	Public-Key certificates requirements	45
7.4	Cryptographic key protection	45
7.5	Use of existing security key management infrastructure	45
7.6	Use of object identifiers	45
8	Asymmetric key management	45
8.1	Certificate generation and installation	45
8.1.1	Private and public key generation and installation	45
8.1.2	Private and public key renewal	46
8.1.3	Random Number Generation	46
8.1.4	Certificate policy	46
8.1.5	Entity registration for identity establishment	46
8.1.6	Entity configuration	47
8.1.7	Entity enrolment	47
8.1.8	Trust anchor information update	48
8.2	Public-key certificate revocation	49
8.3	Certificate validity	49
8.3.1	Validity of certificates	49
8.3.2	Certificate revocation	50
8.3.3	Certificate revocation status checking	50
8.3.4	Handling of authorization and validation lists (AVLs)	50
8.4	Certificate expiration and renewal	55
8.5	Secured Time Synchronization	55
9	Symmetric key management	56
9.1	Group based key management (GDOI)	56
9.1.1	GDOI requirements	56
9.1.2	Internet Key Exchange Version 1 (IKEv1)	56
9.1.3	Phase 1 IKEv1 main mode exchange type 2	57
9.1.4	Phase 1/2 ISAKMP informational exchange type 5	60
9.1.5	Phase 2 GDOI GROUPKEY-PULL exchange type 32	62
9.1.6	GROUPKEY-PULL group key download exchange	70
10	Connections to the IEC 62351 parts and other IEC documents	71

Annex A (normative) Protocol Implementation Conformance Statement (PICS).....	73
Annex B (informative) Random Number Generation (RNG)	74
B.1 Random number generation types.....	74
B.2 Deterministic random bit generators.....	74
B.3 Non-deterministic random number generation	75
B.4 Entropy sources	75
Annex C (informative) Certificate enrolment and renewal flowcharts	76
C.1 Certificate enrolment.....	76
C.2 Certificate renewal	76
Annex D (informative) Examples of certificate profiles.....	78
Bibliography.....	82
Figure 1 – Relationship between public-key certificates and attribute certificates	21
Figure 2 – Group key management distribution	26
Figure 3 – GDOI IKE Phase 1 – Authentication and securing communication channel	27
Figure 4 – GDOI Pull Phase 2.....	28
Figure 5 – Key renewal triggered by the entities.....	30
Figure 6 – Key management in product life cycle	31
Figure 7 – Simplified certificate life cycle	32
Figure 8 – Cryptographic key life cycle	33
Figure 9 – Example of the SCEP entity enrolment and CSR process.....	35
Figure 10 – Example of the EST entity enrolment and CSR process	36
Figure 11 – CSR processing	37
Figure 12 – Certificate revocation list.....	38
Figure 13 – Overview of the online certificate status protocol (OCSP).....	39
Figure 14 – Diagram using a combination of CRL and OCSP processes	40
Figure 15 – Call Flows for the Online Certificate Status Protocol (OCSP).....	41
Figure 16 – Overview Server-Based Certificate Validation Protocol using OCSP Backend	41
Figure 17 – SCEP certificate renewal.....	42
Figure 18 – EST certificate renewal/rekeying	43
Figure 19 – Central certificate generation	44
Figure 20 – IKEv1 (RFC 2409) main mode exchange with RSA digital signatures	57
Figure 21 – IKEv1 main mode exchange and security association messages	58
Figure 22 – IKEv1 main mode exchange: key exchange messages	59
Figure 23 – IKEv1 Main Mode Exchange: ID authentication messages.....	59
Figure 24 – IKEv1 HASH_I calculation	60
Figure 25 – Phase 1 Informational Exchange	61
Figure 26 – GD004FI GROUPKEY-PULL as define in RFC 6407	62
Figure 27 – GROUPKEY-PULL hash computations	63
Figure 28 – GROUPKEY-PULL initial SA request exchange	64
Figure 29 – RFC 6407 Identification Payload	64
Figure 30 – ID_OID Identification Data.....	65
Figure 31 – 61850_UDP_ADDR_GOOSE/SV ASN.1 BNF	66

Figure 32 – IPADDRESS ASN.1 BNF	66
Figure 33 – Example IecUdpAddrPayload ASN.1 Data with DER Encoding	67
Figure 34 – 61850_UDP_TUNNEL Payload ASN.1 BNF	67
Figure 35 – 61850_ETHERNET_GOOSE/SV Payload ASN.1 BNF	67
Figure 36 – RFC 6407 SA TEK Payload	68
Figure 37 – IEC-61850 SA TEK Payload	69
Figure 38 – GROUPKEY-PULL Key Download Exchange	70
Figure 39 – IEC 62351 Part 9 relationship to other IEC 62351 parts	71
Figure C.1 – Certificate enrolment	76
Figure C.2 – Certificate renewal state machine	77
Table 1 – KDC IKEv1 Requirements	56
Table 2 – IEC 61850 Object IDs: Mandatory (m) and Optional (o)	65
Table D.1 – Examples of operator public-key certificates	79
Table D.2 – Examples of OEM certificates	80
Table D.3 – Example of OCSP certificate	81

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.

International Standard IEC 62351-9 has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

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

FDIS	Report on voting
57/1838/FDIS	57/1853/RVD

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

This document 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 standard, the following print types are used:

- ASN.1 notions is 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.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "<http://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.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication 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, 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*

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

RFC 7030, *Enrolment over Secure Transport*

3 Terms and definitions

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

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>

3.1

asymmetric keys

two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification

3.2

authorization and validation list

AVL

signed list containing information to an AVL entity about potential communications entities and possible restrictions on the communications with such entities

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.9]

3.3

authorization and validation list entity

AVL entity

entity, when acting as a relying party, which is dependent on an AVL issued by a designated authorizer

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.10]

3.4

authorizer

entity trusted by one or more entities operating as AVL entities to create, maintain and sign authorization and validation lists

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.11]

3.5

certification path

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

Note 1 to entry: 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, 3.5.18 | Rec. ITU-T X.509 (2016), 3.5.21]

3.6 **certificate signing request** **CSR**

request issued when a new certificate or renewal of a certificate is required

Note 1 to entry: When the generated CSR is submitted to a CA, the CA signs the CSR using its private key and the CSR becomes the certificate.

[SOURCE: RFC 2986]

3.7 **controllership**

intersection of legal ownership, physical control, and logical control over a device or system, in which the nature of any contractual agreements between ownership and control of the device or system is not important in the context

3.8 **cryptographic binding**

use of one or more cryptographic techniques by a CKMS to establish a trusted association between a key and selected metadata elements

[SOURCE: NIST SP 800-130]

3.9 **cryptographic key management system** **CKMS**

system for the management (e.g., generation, distribution, storage, backup, archive, recovery, use, revocation, and destruction) of cryptographic keys and their metadata

[SOURCE: NIST SP 800-130]

3.10 **dataset**

collection of data

3.11 **digital signature**

result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity, and signatory non-repudiation

[SOURCE: FIPS 186]

3.12 **entity**

generic term that covers human users, automation systems, software applications, communication nodes, field devices, and other types of assets

3.13 **group controller/key server** **GCKS**

device that defines group policy and distributes keys for that policy

[SOURCE: RFC 3740]

3.14**group domain of interpretation****GDOI**

domain that manages group security associations, which are used by IPsec and potentially other data security protocols

Note 1 to entry: These security associations protect one or more key-encrypting keys (KEK), traffic-encrypting keys (TEK), or data shared by group members. GDOI uses the notion of a group controller, which is used to support the establishment of security associations between members of a group.

[SOURCE: RFC 6407]

3.15**group member****GM**

authorized member of a secure group, sending and/or receiving IP packets related to the group

3.16**hash function**

(mathematical) function which maps data of arbitrary size into data of a fixed size called a digest

Note 1 to entry: Approved hash functions satisfy the following properties:

- 1) One-Way. It is computationally infeasible to find any input that maps to any pre-specified output.
- 2) Collision Resistant. It is computationally infeasible to find any two distinct inputs that map to the same output.

[SOURCE: ISO/IEC 9598-8:2017 | Rec. ITU-T X.509 (2016), 3.5.36]

3.17**hash message authentication code****HMAC**

cryptographic code used for authentication with symmetric keys and for data integrity

[SOURCE: RFC 2104]

3.18**key distribution centre****KDC**

centre which, in an IEC 62351-9 context, provides a network service that supplies temporary (symmetrical) session keys to predefined set of peers after successful authentication

Note 1 to entry: This is also known as Group Controller/Key Server (GCKS) (See GDOI).

3.19**message authentication code****MAC**

cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modification of the data

[SOURCE: SP 800-63; FIPS 201]

3.20**object identifier**

ordered list of primary integer values from the root of the international object identifier tree to a node, which unambiguously identifies that node

[SOURCE: ISO/IEC 9834-1:2012 | Rec. ITU-T X.660 (2011), 3.5.11]

3.21

online certificate status protocol

OCSP

protocol that enables applications to determine the (revocation) state of an identified certificate

Note 1 to entry: OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response.

[SOURCE: RFC 6960]

3.22

pre-shared key

PSK

secret which is shared in advanced between the two entities, such as software applications or devices, to be able to authenticate themselves after establishing a secure connection

3.23

private key

(in a public-key cryptosystem) that key of an entity's key pair which is known only by that entity

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.49]

3.24

public-key certificate

public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the CA which issued it

Note 1 to entry: A public-key certificate is often called an X.509 certificate or a digital certificate. However, such terms are ambiguous, as they could also mean attribute certificates, which are also defined by ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016).

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.57]

3.25

public-key cryptography standards

PKCS

specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography

[SOURCE: www.rsa.com]

3.26

random number generation

RNG

process used to generate an unpredictable series of numbers

Note 1 to entry: Each individual value is called random if each of the values in the total population of values has an equal probability of being selected.

[SOURCE: NIST SP 800-57]

3.27

registration authority

those aspects of the responsibilities of a certification authority that are related to identification and authentication of the subject of a public-key certificate to be issued by that certification authority

Note 1 to entry: A registration authority may either be a separate entity or be an integrated part of the certification authority.

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T Rec. X.509 (2016), 3.5.60]

3.28

relying party

entity that relies on the data in a public-key certificate in making decisions

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.61]

3.29

secret key

cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public

[SOURCE: FIPS 140-2]

3.30

security association

SA

relationship established between two or more entities to enable them to protect data they exchange

[SOURCE: NIST IR 7298 Rev.1]

3.31

security strength

ability of the security technologies to make it infeasible for a would-be attacker to bypass or subvert

Note 1 to entry: This is often measured in bits of security.

[SOURCE: NIST SP 800-130]

3.32

session key

in the context of symmetric encryption, key that is temporary or is used for a relatively short period of time

[SOURCE: RFC 2828]

3.33

simple certificate enrolment protocol

SCEP

protocol supporting the secure issuance of certificates to network devices in a scalable manner, using existing technologies whenever possible

Note 1 to entry: The protocol supports the following operations:

CA and RA public key distribution

Certificate enrolment

Certificate revocation

Certificate query

CRL query

[SOURCE: IETF Draft SCEP]

3.34

symmetric key

cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or to create a message authentication code and to verify the code

[SOURCE: NIST SP 800-63]

3.35

trust

firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.2.1]

3.36

trust anchor

entity that is trusted by a relying party and used for validating public-key certificates in certification paths

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.71]

3.37

trust anchor information

at least the: distinguished name of the trust anchor, associated public key, algorithm identifier, public key parameters (if applicable), and any constraints on its use including a validity period

Note 1 to entry: The trust anchor information may be provided as a self-signed CA-certificate or as a normal CA-certificate (i.e., cross-certificate).

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.72]

3.38

trust anchor management protocol

TAMP

protocol used to manage a trust anchor store

[SOURCE: RFC 5934]

3.39

trust anchor store

trust anchor information collection at a relying party for one or more trust anchors

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.73]

4 Abbreviations and acronyms

Additional abbreviations and acronyms are listed in IEC TS 62351-2.

ASN.1	Abstract Syntax Notation One
AVL	Authorization and Validation List
AVMP	Authorization and Validation Management Protocol
CA	Certification Authority
CASP	Certification Authority Subscription Protocol
CKMS	Cryptographic Key Management System

CIA	Confidentiality, Integrity, and Availability
CMC	Certificate Management over CMS
CMS	Cryptographic Message Syntax
CSR	Certificate Signing Request
DER	Distinguished Encoding Rules
DOI	Domain of Interest
DSA	Digital Signature Algorithm
EST	Enrolment over Secure Transport
GCKS	Group Controller/Key Server
GDOI	Group Domain of Interpretation
GKDC	Group KDC
GM	Group Member
GMAC	Galois Message Authentication Code
GOOSE	Generic Object Oriented Substation Event
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
ID	Identity
IKE	Internet Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
KD	Key Download
KDC	Key Distribution Centre, a.k.a GKDC
KEK	Key Encryption Key
OCSP	Online Certificate Status Protocol
PDU	Protocol Data Unit
PEM	Privacy-enhanced Electronic Mail
PKCS	Public-Key Cryptography Standard
PKI	Public-Key Infrastructure
RA	Registration Authority
RNG	Random Number Generation
RSA	Rivest Shamir Adleman, public-key crypto system
SA	Security Association
SCEP	Simple Certificate Enrolment Protocol
SV	Sample Values
TAMP	Trust Anchor Management Protocol
TEK	Traffic Encryption Key

5 Cryptographic applications for power system implementations

5.1 Cryptography, cryptographic keys, and security objectives

The term cryptography refers to the use of a family of data transformation algorithms for the purposes of achieving specific security-oriented goals such as obscuring the contents of a message from unintended recipients (confidentiality), ensuring no one has tampered with message contents during transit (integrity), and verifying the claimed identity of the sender (authenticity). In order to provide confidentiality, integrity, and authenticity, modern implementations of ciphers use a cryptographic key as the changeable part of the data.

transformation, shifting the sensitivity of the data to the key rather than the data payload. This part of IEC 62351 is about management of these cryptographic keys to ensure security objectives are met in the context of power system implementations.

5.2 Types of cryptography

This part of IEC 62351 focuses on the management of keys for two basic types of cryptography: asymmetric and symmetric. Both of these types of cryptography rely on cipher suites and numerous well-accepted cryptographic algorithms. This document does not address the specification of cipher algorithms and configurations for particular implementations, but does address the unique requirements associated with management of both types of cryptographic keys for power system implementations.

For symmetric cryptography, the same key is used to encrypt and decrypt data, so this key must be known and be kept secret by both parties who are exchanging a symmetrically encrypted message. The different symmetric key algorithms are each identified by an object identifier (see 7.6).

Asymmetric cryptography uses a pair of mathematically related keys. One of the keys is the private key to be kept secret by the owner and the other one is the public key that may be publicly known. The public key is typically provided in a public-key certificate that binds the public key with the identity of the owner of the public-key certificate and thereby the corresponding private key. Such a public-key certificate is verified and digitally signed by a certification authority.

Asymmetric cryptography is primarily used for digital signature generation, in which the private key is used in combination with a hash algorithm to create a digital signature. The corresponding public key in combination with the same hash algorithm is used for validating the digital signature. Digital signatures provide data integrity (see 5.3.3), authentication (see 5.3.4), and non-repudiation (see 5.3.5). Asymmetric cryptography may also be used for key agreement whereby two or more entities can agree on a key in such a way that both influence the outcome, possibly using the Diffie Hellman technique ([1]). These different public-key algorithms are identified by an object identifier.

Certain public-key algorithms based on the RSA technology (see e.g., [25]), may be used for encryption and decryption. Data encrypted using the private key may be decrypted using the public key and vice versa.

While there are fundamental functional differences between RSA asymmetric cryptography and symmetric cryptography, neither type of cryptography is inherently stronger than the other. Their different characteristics cause them to be used for different purposes, and they may often complement each other. However, each has a distinct set of characteristics involving computational complexity and key length that create performance considerations for specific applications. Asymmetric cryptography used in power system implementations tends to be more computationally intense than comparably strong symmetric cryptography. These different performance characteristics thus guide choices for usage, although the specific algorithm, configuration, and platform choices may also greatly affect overall performance. For this reason, computational intensive RSA asymmetric key cryptography is often used just to exchange symmetric secret “session” keys, which can then be used to rapidly encrypt and decrypt all the messages during a “session”.

The robustness of a cryptographic algorithm is expressed as security strength measured in a number of bits that reflects the expected effort it takes to break the algorithm.

5.3 Uses of cryptography

5.3.1 Goals of cyber security

Cyber security is focused on countering key threats that includes the following functionality:

- Ensuring the source of commands and data is authenticated.
- Ensuring access to resources and data is authorized.
- Ensuring the integrity of data.
- Ensuring that system control and changes are authenticated and authorized.
- Preventing the disclosure of confidential data.
- Preventing non-repudiation (loss of accountability).
- Preventing denial of service (availability).

Traditionally, cyber security addresses confidentiality, integrity, and availability (CIA). However, for power system operations, the continued safe and reliable operation of the power system is the highest priority. This places the highest priority on the first three: data source authentication, access authorization, and integrity protection, while confidentiality and non-repudiation can be important for certain interactions.

Cryptography can help to address most of these threats, but primarily the first five threats – prevention of denial of service usually involves engineering designs and strategies. Therefore, for power system implementations, five primary goals are considered for the use of cryptography:

- Verifying the claimed identity of a message sender (authentication).
- Verifying that the sender has the right to access the requested data (authorization).
- Ensuring no one has tampered with a message during transit (integrity).
- Obscuring the contents of a message from unintended recipients (confidentiality).
- Associating specific actions with the entity that performed them (non-repudiation).

These cryptographic measures are discussed in 5.3.2 through 5.3.6. The ordering of these clauses does not imply priority for power system applications: in such environments, confidentiality usually has one of the lower priorities among these cryptographic goals. However, some of the cryptographic mechanisms to achieve these goals build upon each other, and so the goals are presented in the following order for ease of conceptual explanation.

5.3.2 Confidentiality

The cryptographic goal of data confidentiality in power system implementations is typically accomplished by encrypting the message using symmetric key cryptography. The message may be encrypted individually at the application level, at the underlying communications channel, or possibly both. As stated previously, the confidentiality of this message is dependent upon the sender and receiver maintaining the secrecy of the encryption key. Additionally, asymmetric cryptography is often used to negotiate and exchange symmetric session keys that are valid for a specified length of time, thus reducing the risk associated with keeping a specific session key secret.

5.3.3 Data integrity

Data integrity includes the detection of unauthorized changes to data. Any changes to the data as it transits the communication networks should be detected by the recipient. Cryptographic hash functions (e.g. SHA256) are used to detect any integrity violations of the received data.

The cryptographic goal of message integrity in power system implementations is typically accomplished by using another form of cryptographic algorithm called HMAC (keyed-hash message authentication code), a cryptographic hash function used in combination with a secret symmetrical cryptographic key. The result is a key hashing function, such as HMAC, that provides not only data integrity, but also validates the source of the data.

Alternatively, instead of symmetrical cryptographic, the sender may attach a digital signature to the message, providing additional cryptographic binding information on the data source (see 5.3.5).

5.3.4 Authentication

When entities, namely field devices, software applications, automation systems, and the users who interact with them, need to exchange data, it is critical that the source of this data is authenticated. To accomplish reliable authentication, data sources are provided with cryptographic keys that allow them to prove their identity to the recipients of the data. Public-key certificates and asymmetric cryptographic methods can be used to authenticate these entities as the sources of data.

5.3.5 Non-repudiation

Non-repudiation refers to the ability to bind an action (e.g., a command or a message) irrefutably to an issuing entity. It may bind a sender to the action of sending a specific message or a receiver to the action of receiving a specific message. This is accomplished using public-key certificates and asymmetric cryptography. A public-key certificate is a digitally signed statement that claims a public-private key pair is associated with a unique entity. Receivers of a signed message can prove that a message was sent by its originator since only the originator is presumably in possession of the private key needed to create the signature. If non-repudiation of receipt were required, the receiver would need to sign a copy of the received message and send it back to those requiring proof. Typically, a time-stamp is included in such signed messages since otherwise a signor could refute the message simply by declaring that their secret key is no longer secret.

5.3.6 Trust

One important part of securing digital communication is the need for trust. Entities (systems or devices) should only accept data (communicate) with entities that they can authenticate and trust (see 5.3.4). Public-key certificates provide the basis to establish such trust by asserting the association of a public-key certificate with a unique entity. Trust for a particular public-key certificate is established by validating a so-called certification path that has its root in a trust anchor that is trusted by the entity doing the validation, also called the relying party. A certification path is a chain of public-key certificates starting with the public-key certificate signed by the trust anchor ending with the public-key certificate to be validated. The concepts of relying party, trust anchor and certification paths are further described in Clause 6, 7.5 and 7.7 of ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016).

In some cases, trust may be established directly between a trust anchor and the relying party. However, a chain of trust can be established. If a relying party receives a public-key certificate from an entity with which it has a trust relationship, this public-key certificate may be validated without going through the complete certification path, instead relying on the chain of trust. In this case, the public-key certificate may not need to be issued and signed by the trust anchor, but may be signed by a certification authority that has established a chain of trust back to the trust anchor.

For power system implementations, certification authorities might be the relevant organizational unit within a company, the company itself, a governmental entity, or accepted third party.

Public-key digital certificates have a finite period of validity, after which they expire. Trust can also be revoked in the event of compromise. Management of public-key certificates is closely related to cryptographic key management, and is therefore covered in this standard. See 6.5.

6 Key management concepts and methods in power system operations

6.1 Key management system security policy

Cryptographic keys need to be protected. Therefore, every organization should develop a security policy for its key management system that establishes and specifies all of the requirements for protecting the confidentiality, integrity, availability, and source authentication of all cryptographic keys and metadata used by the organization. These protection requirements should cover the entire key life cycle, including when they are operational, stored, and transported. A key management security policy should also include the selection of all cryptographic mechanisms and protocols to be used throughout the organization's systems.

Key management systems also need security administrative support to ensure the security policies are followed and the procedures are maintained. The specification of this support is out-of-scope for this document, but can be found in other documents such as ISO/IEC 11770 ([8]) or in NIST SP 800-130 ([13]).

6.2 Key management design principles for power system operations

Cryptographic keys used with selected cryptographic functions can be used to secure the messages being sent between different entities, such as users, systems, software applications, communication nodes, and the potentially large numbers of equipment and devices that are often located at remote and often untrusted sites.

These cryptographic keys should be managed so that they can effectively and securely be provided to the entities that require secure exchanges of data. This key management must take into account many issues, ranging from the capabilities of entities, to the varied types of locations of these entities, to the timing for providing and revoking keys, and to protecting the key management processes themselves from attacks.

For instance, many smaller devices are limited in computational power and memory capacity, while the communication networks may also be limited in available bandwidth. Therefore, some of the key management techniques used in traditional enterprise information technology system environments with powerful systems and high bandwidth communications are not well suited to power system automation and communication environments.

To address these constraints, this document specifies different key management techniques that could be used for different requirements and constraints. Specifically it specifies how to manage keys for each of the cryptographic functions specified in the other IEC 62351 parts. Sources of guidance on key management design principles include:

- Reference [8] ISO/IEC 11770-1:2010 Information technology – Security techniques – Key management – Part 1: Framework, 6.1.2, D-3.4.
- Reference [10] ISO/IEC 11770-3:2008 Information technology – Security techniques – Key management – Part 3: Mechanisms Using Asymmetric Techniques.
- Reference [15] NIST 800-57, Part 1, 8.1.4 and 8.1.5.

6.3 Use of Transport Layer Security (TLS)

This part of IEC 62351 refers to Transport Layer Security as defined by RFC 5246. The details on how to use TLS in power systems are specified in IEC 62351-3.

6.4 Cryptographic key usages

Cryptographic keys are used for different purposes and in different phases of the product lifecycle and are applied as:

- Digital certificates and corresponding private keys: Used to authenticate entities when in a public-key infrastructure (PKI) environment.
- Pre-shared keys (e.g., for real-time communication): Used as a shared secret between entities to build up mutual authentication between them. This may be useful in non-PKI environments. Additionally, this scheme may be used during PKI enrolment, allowing an entity to authenticate itself against the certification authority (CA), for example when performing a certificate signing request (CSR). *Engineering tools could automate the generation of the entity registration password. Password complexity options are given by the organization security policies and CA supported possibilities.*
- Session secret keys (pair wise or group-based): Used for efficient encryption or integrity checks on communication messages.
- Session parameters (dedicated cryptographic algorithms): Used to support sessions (keys, lifetime, etc.).
- Cryptographic access tokens: Mostly used to transfer/provide authorization/access of resources to entities for a limited time.
- Other relevant entities or organizational credentials.

6.5 Trust using a public-key infrastructure (PKI)

6.5.1 Registration authorities (RA)

In PKI-based systems, entities are required first to prove their identity through a Registration Authority (RA). For humans, RAs may determine an individual identity through birth certificates, passports, or other official documents. For systems and devices, RAs may determine an entity's identity through a manufacturer-issued digital certificates or a unique one-time-password (OTP).

6.5.2 Certification authority (CA)

After its identity is established, a system or device needs to be bound to a certificate by a certification authority (CA). The manufacturer creates and digitally signs a certificate signing request (CSR) for the entity. The CA verifies the CSR and issues a digital certificate based on the data included in the CSR. CAs establish a trusted association between the entity's public key and the public-key certificate metadata by cryptographically binding the entity's public key and the metadata (i.e. the CA's digital signature computed on the combination of the public key and metadata). This digital certificate thus binds the entity's identity with its public key, so that there is now a trusted public/private key combination that can be used by the entity to exchange information with other entities. The trust in the entity's key thus relies on one's trust in the validity of the CA's key (see 6.5.3).

CAs may be operated either by an organization itself, allowing for a closed, organization-controlled communication group, or by a third party (service provider, system operator or grid manager) that is publicly accepted and hence has a wider scope of trust. Third-party CAs require a secure method for ensuring the valid identity of any new entity, which can range from in-person validation for humans to business-entity validation and to security chains of digital certificates linking previously validated digital certificates to new digital certificates.

6.5.3 Public-key certificates

A public-key certificate (a.k.a. digital certificate) is a digital document that binds the identity of entity to the public key private key pair of that entity. As noted in 6.5.2, this binding is verified by a digital signature by the issuing CA. In addition to the public-key and identity of the owner of public-key certificate, the public-key certificates holds verified information about validity period and the identity of the issuer. A public-key certificate may include extensions providing additional information. An extension is identified by an object identifier allocated by the organisation defining the extension. A public-key certificate may be issued to a CA and is then called a CA certificate or to an end entity and is then called an end-entity public-key certificate.

In a PKI environment, public-key certificates may be digitally signed by the CA of the organization to which the entity belongs. In some cases, multiple public-key certificates are created as an entity goes through a supply chain from manufacturer, to distributor, to purchaser, to installer, etc. Root certificates of the issuing CA become the trust anchors, if used. Typically, organizations should install only root certificates from CAs they trust, including public-key certificates issued by their own CA.

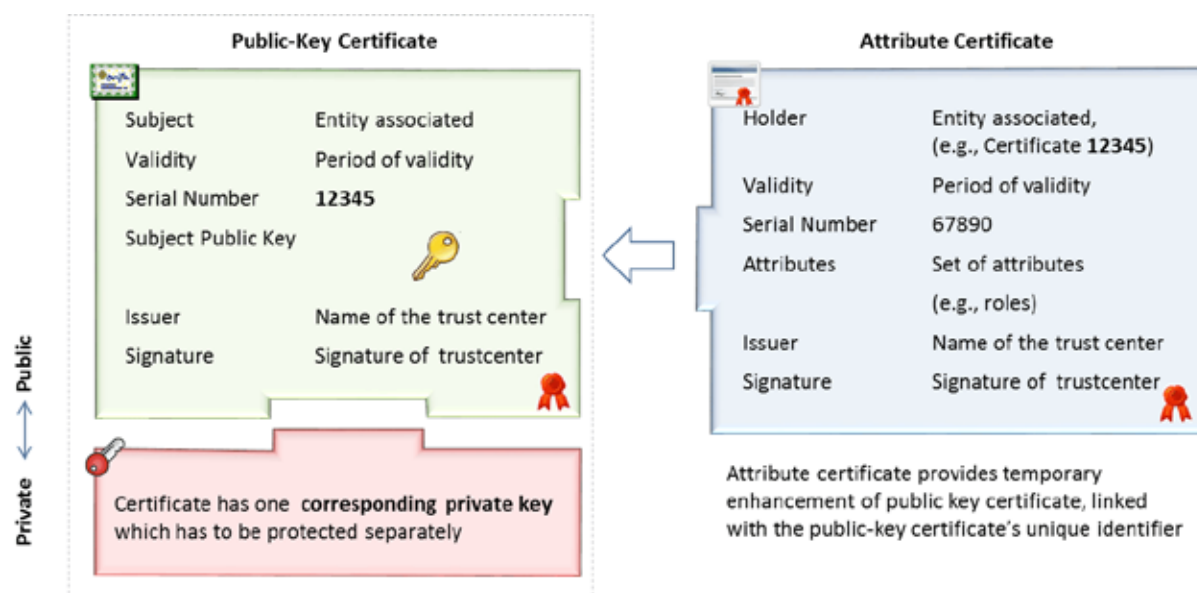
Public-key certificates and attribute certificates are defined by a base set plus extensions to the base set. Extensions are identified by an international register of object identifiers (OIDs). See 6.5.4.

OIDs are allocated by various international standards, including ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), and may be registered for private use. The OID namespace (root) value for IEC 62351 is 1.0.62351 and 1.2.840.10070. IEC TS 62351-8 utilizes the latter approach to define access tokens (authorizations). This part of IEC 62351 and every new upcoming part of IEC 62351 should use the first OID (1.0.62351).

6.5.4 Attribute certificates

Attribute certificates provide an effective way to separate the management of identity from the management of authorizations associated with an identity. Full separation can be achieved by managing public-key certificates with a PKI and attribute certificates with a “privilege management infrastructure” (which uses the same CA technology as a PKI).

As shown in Figure 1, attribute certificates can be used to extend the information in a public key certificate. They allow for instance for temporary enhancement of the permissions of the public key certificate holder by specific role-based access information. This approach has been leveraged in IEC TS 62351-8.



IEC

Figure 1 – Relationship between public-key certificates and attribute certificates

6.5.5 Public-key certificate and attribute certificate extensions

Both public-key certificates and attribute certificates allow extensions to be optionally included. Each such extension provides additional information.

An extension type consists of an object identifier (see 7.6) that identifies the type of extension and specifies the syntax for the associated information. In addition, it includes a Boolean that specifies whether a particular extension is flagged as critical or as non-critical. If an extension

is flagged as critical, it cannot be ignored and the public-key or attribute certificate should be considered invalid if the relying party does not support the type of extension. If the extension is flagged as non-critical, the relying party may ignore the extension if the extension type is not supported. For more details, see 7.3 of ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016).

ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016) specifies a number of general useable extensions. IEC TS 62351-8 specifies the **IECUserRoles** extension, which has been defined for power systems to provide means for role-based access control.

6.6 Trust via non-PKI self-signed certificates

Self-signed certificates play an important role in a PKI. Trust hierarchies or trust chains in PKIs are rooted by “root certificates” (see 6.5.3). PKI root certificates may be self-signed certificates known as trust anchors, created by trusted CAs that allow this trust to be distributed.

Under certain circumstances, non-PKI self-signed certificates may be more easily implemented than the more complex PKI signed certificates in order to establish trust. This may especially be the case in smaller deployments with only a limited number of entities. Self-signed certificates are public/private key pairs internally generated by an entity, where the private key is used to sign the entity’s own public key together with additional information, such as the subject name, validity time, etc. So that they can be used in the same way as PKI based certificates, e.g., to authenticate interactions in TLS connections, self-signed public-key certificates are required to comply with the public-key certificate structure as described in ISO/IEC 9594-8.

Self-signed certificates cannot be generally accepted as trustworthy. Hence, to enable the acceptance of self-signed certificates by a limited group of entities for authentication, they should only be used in conjunction with authorization and validation lists (see 6.7).

The level of complexity of using entity specific self-signed certificates and authorization and validation lists can be compared with the use of pre-shared keys. Self-signed certificates are issued per entity while pre-shared keys are issued per paired connection. Thus while the number of self-signed certificates will depend upon the number of end points, the number of pre-shared keys will depend upon the number of connections between the end points.

As self-signed certificates need to be public-key certificates, their application could open the migration path to PKI-based public-key certificate implementations, so that self-signed certificates may easily be replaced with PKI-based certificates once those are available.

6.7 Authorization and validation lists

6.7.1 General

Authorization and validation lists (AVLs), also known as White Lists, provide information about potential communications entities and possible restrictions on the communications with such entities in a particular environment. They are specified in Clause 11 of ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016).

An AVL is used by an entity when that entity is acting as a relying party. Such an entity is called an AVL entity. An AVL is placed in an entity called authorizer that is responsible for the content of the AVL, i.e., the authorizer is trusted by the AVL entity to provide valid information. An AVL is signed by the issuing authorizer.

The communication between the authorizer and the AVL entity has to be protected as any other communication with respect to integrity, authenticity and possible confidentiality. To simplify validation of the AVLs, it is recommended that an authorizer be closely related to the AVL entities it serves, e.g. being within the same organization so that a trust relationship may be established between the authorizer and the AVL entities it serves (see 5.3.6).

AVLs may be used either in non-constrained environments or in constrained environments as detailed in 6.7.2 and 6.7.3.

6.7.2 AVLs in non-constrained environments

A non-constrained environment is an environment where AVL entities are capable of performing traditional validation of received public-certificates.

AVLs are used to restrict communication within a specified set of other entities, and may impose restrictions on such entities beyond path length, policy and name restriction as detailed in ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016). 8.3.4 specifies such additional restrictions imposed by AVLs.

The entities with which communication is possible are identified in the AVL either by reference to their public-key certificates or by the name structure of the organization to which the entity belong.

6.7.3 AVLs in constrained environments

An entity may be constrained in many ways:

- a) It is battery driven and needs to limit processing to save on the battery.
- b) It has little processing capabilities.
- c) Its communication channel has limited bandwidth.
- d) It has limited storage.
- e) It may have stringent time constraints having to respond to incident very quickly not allowing time for external communication to validate received public-key certificates.

In addition to what is described in 6.7.2, the authorizer is responsible for validating that all public-key certificates represented in the AVL are valid and may be trusted at all times. It is also the responsibility of the authorizer to be updated on the validity of the public-key certificates in their AVLs. The authorizer also makes the judgement as to when an expired or revoked public-key certificate should or should not be used in cases where its withdrawal might affect a critical entity. An AVL entity assumes that a listed public-key certificate is valid to use.

This mode of operation requires communication between the authorizer and the CAs that issued the public-key certificates listed in the AVL.

6.7.4 Use of self-signed public-key certificates in AVLs

Use of self-signed public-key certificates is not recognized by ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), but is provided here as an added capability.

By placing the self-signed public-key certificates in an AVL, the authorizer takes the responsibility to ensure that these self-signed public-key certificates may be safely used by digitally signing the AVL. How the authorizer maintains information about the validity of the self-signed public-key certificates is outside the scope of this part of IEC 62351.

6.8 Trust via pre-shared keys

Under special conditions, pre-shared keys may be manually installed in entities. These pre-shared keys, which are symmetric keys shared in advance among communicating entities, may be used to establish trust for peer-to-peer interactions and may also be used to secure further key management steps. The pre-shared keys, which need to be kept secret, need to be installed by a trusted entity using trusted installation methods. Guidance on the installation of pre-shared keys is provided in NIST SP 800-133 ([14]).

6.9 Session keys

Session keys are used for a relatively short time, ostensibly for a “session” between two entities, but in reality to ensure that cryptographic keys are replaced in a timely manner. That update time period is generally related to the cryptographic strength of the keys and the time it might take an attacker to break the key.

For instance, session keys are often used in conjunction with secret keys with entities that are compute-constrained and/or communications-constrained. Asymmetric cryptography, which can be computationally intensive, may be used periodically to update the session keys in the entities. These session keys can then be used by these entities for a few hours or even a few days. Usually a short overlap time is allowed between the expiration of a previous session key and the provision of the new session key, in order to ensure that communications can be maintained continuously (without doubling computational load).

6.10 Protocols used in trust establishment

6.10.1 Certification request

The certification request is specified as PKCS#10 in RFC 2986 ([20]). A certification request is sent from an entity to the registration authority (RA), which may be co-located with the CA or be physically separated.

A certification request contains the information to be included in the `subject` and `subjectPublicKeyInfo` components of the public-key certificate to be generated. In addition, some directory attributes may be included.

RFC 2985 defines two attribute types, one providing a challenge password and another one providing a list of extensions to be included in the generated public-key certificate.

6.10.2 Trust Anchor Management Protocol (TAMP)

The Trust Anchor Management Protocol (TAMP), as defined in RFC 5934, specifies a protocol for the management of trust anchors stores (TAs) and community identifiers stored in a trust anchor store. The protocol makes use of the Cryptographic Message Syntax (CMS), which provides integrity protection and data origin authentication. The protocol can be used to manage trust anchor information within trust anchors stores. Trust anchor information may be represented as a CA-certificate, as an unsigned CA certificate or as a `TrustAnchorInfo` object as defined by RFC 5914.

6.10.3 Simple Certificate Enrolment Protocol (SCEP)

The Simple Certificate Enrolment Protocol (SCEP) was developed to simplify the enrolment of large numbers of devices and to make the issuing and revocation of digital certificates as scalable as possible. Entities can use SCEP to request their digital certificate electronically using the PKI certificate forms PKCS#7 and PKCS#10 over HTTP. The key material is generated only on the client side. SCEP is defined by the IETF in draft-nourse-scep-23. Based on the dependency on PKCS#7, SCEP targets the enrolment in RSA based infrastructures. SCEP may be terminated at the RA or at the CA directly.

NOTE 1 Draft-nourse-scep-23 is a historic draft, which itself recommends using either CMP (RFC 4210, see 6.10.4) or CMC (RFC 5272, see 6.10.5) if SCEP support is not required by the infrastructure.

NOTE 2 Meanwhile there exists an attempt to bring SCEP to RFC status. The draft-gutmann-scep-04 targets the improvement of SCEP by addressing recently discovered issues. Nevertheless, it will continue to be bound to the RSA environment.

6.10.4 Internet X.509 PKI Certificate Management Protocol (CMP)

The Certificate Management Protocol (CMP) is an Internet protocol used for obtaining public-key certificates in a PKI. It defines a protocol for the interaction between a client and the PKI