PD CEN/TS 419261:2015

BSI Standards Publication

Security requirements for trustworthy systems managing certificates and time-stamps

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TS 419261:2015.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and personal identification.

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.

Published by BSI Standards Limited 2015

ISBN 978 0 580 86425 4
ICS 03.120.20; 35.040; 35.240.30

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2015.

Amendments/corrigenda issued since publication

Date	Text affected

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 419261

March 2015

ICS 03.120.20; 35.040; 35.240.30

English Version

Security requirements for trustworthy systems managing certificates and time-stamps

Exigences de sécurité pour systèmes de confiance gérant des certificats et des horodatages

Sicherheitsanforderungen für vertrauenswürdige Systeme zur Verwaltung von Zertifikaten für elektronische Signaturen und Zeitstempel

This Technical Specification (CEN/TS) was approved by CEN on 18 November 2014 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

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

Ref. No. CEN/TS 419261:2015 E

Contents

Page

Foreword

This document (CEN/TS 419261:2015) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by AFNOR.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

Successful implementation of European Directive 1999/93/EC on a Community framework for electronic signatures [Dir.1999/93/EC] and of REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [Reg.910/2014/EU] requires standards for services, processes, systems and products related to electronic signatures as well as guidance for conformity assessment of such services, processes, systems and products.

NOTE According to Article 50 of Reg.910/2014/EU Directive 1999/93/EC is repealed with effect from 1 July 2016 and references to the repealed Directive shall be construed as references to the Regulation.

In 1999 the European Information and Communications Technologies Standards Board, with the support of the European Commission, undertook an initiative bringing together industry and public authorities, experts and other market players, to create the European Electronic Signature Standardization Initiative (EESSI).

Within this framework the Comité Européen de Normalization / Information Society Standardization System (CEN/ISSS) and the European Telecommunications Standards Institute / Electronic Signatures and Infrastructures (ETSI/ESI) were entrusted with the execution of a work programme to develop generally recognized standards to support the implementation of [Dir.1999/93/EC] and development of a European electronic signature infrastructure.

The CEN/ISSS Workshop on electronic signatures (WS/E-SIGN) resulted in a set of deliverables, CEN Workshop Agreements (CWA), which contributed towards those generally recognized standards.

In 2011 the European Commission (EC) with the support of the European Free Trade Association has signed a specific grant agreement with the European Committee for Standardization (CEN) regarding the update of the existing European e-Signature CEN Workshop Agreements (CWAs) in the framework of Phase 1 of the mandate M/460. The present document is such a CEN Workshop Agreement that was first created as a CWA and then updated into a Technical Specification (TS).

The purpose of this TS is to describe the security requirements for trustworthy systems managing certificates for electronic signatures and to define overall system security requirements, whereas EN 419221 specifies security requirements for cryptographic devices. The requirements were partly inspired by Common Criteria [CC] Part 2, but the TS is not compliant to [CC], as e.g. EN 419221. In consequence, this TS cannot be used to perform Common Criteria certifications of products.

The TS is intended for use by designers and developers of systems managing certificates and time-stamps, as well as customers of such systems.

Executive Summary

This Technical Specification specifies security requirements on products and technology components, used by Trust Service Providers (TSPs) for issuing and managing certificates as well as electronic time-stamps in the sense of the REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [Reg.910/2014/EU].

The term TSP includes certification service providers (CSPs) issuing qualified certificates as defined in the Directive *"Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures"* [Dir.1999/93/EC]. These certificates are used in conjunction with electronic signatures and advanced electronic signatures in accordance with Directive 1999/93/EC [Dir.1999/93/EC]. Additionally, electronic time-stamps issued by a TSP provide evidence that the stamped data existed at a given time.

This Technical Specification contains the same requirements for TWS used by CSPs according to [Dir.1999/93/EC] and for TWS used by TSPs according to [Reg.910/2014/EU]. However, [Reg.910/2014/EU] allows TSPs to manage electronic time-stamps without managing certificates. This is not allowed for CSPs according to [Dir.1999/93/EC]. Therefore, this Technical Specification distinguishes between CSPs and TSPs with respect to the provided services where necessary.

TSPs need to use Trustworthy Systems (TWSs) for securely providing the following services, which are defined in this TS:

a) Registration Service - to verify the identity and, if applicable, any specific attributes of a subject;

b) Certificate Generation Service - to create certificates;

c) Dissemination Service - to provide certificates and policy information to subjects and relying parties;

d) Revocation Management Service - to allow the processing of revocation requests;

e) Revocation Status Service - to provide certificate revocation status information to relying parties;

f) Subject Device Provision Service – to prepare and provide a Signature Creation Device (SCDev) to subjects. This includes Qualifed electronic Signature and Seal Creation Device (QSCD) provision;

g) Time-stamping Service – provides a Time-stamping Service which may be needed for signature verification purposes.

TSP shall follow:

h) "General Security Requirements" specified in 5.2 that are applicable to all previously mentioned services;

i) Security requirements specified in 5.3, 5.4 and 5.5 that are specific to some of the previously mentioned services.

In accordance with Directive1999/93/EC, CSPs need to establish and maintain the first five core services relevant for the issuance and management of qualified certificates (Registration Service, Certificate Generation Service, Dissemination Service, Revocation Management Service, and Revocation Status Service). The other two services (Subject Device Provision Service and Time-stamping Service) are optional ones and are not required to be established and maintained by CSPs, because of having not being specifically addressed in Directive1999/93/EC.

TSPs managing certificates and operating in accordance with Regulation (EU) No 910/2014 [Reg.910/2014/EU] will need to establish and maintain the first five core services relevant for the issuance and management of qualified certificates (Registration Service, Certificate Generation Service, Dissemination Service, Revocation Management Service, and Revocation Status Service). The Subject Device Provision Service is an optional service for such a TSP. TSP managing electronic time-stamps need to establish and maintain the Time-stamping Service relevant for the issuance and management of electronic time-stamps.

TSPs issuing:

j) Certificates according to ETSI/TS 119 411-1 or TS 119 411-2 (or equivalent ENs to be subsequently published) and/or

k) Time-stamps according to ETSI/TS 119 421 (or equivalent EN to be subsequently published)

may use TWSs that have been independently assessed against the relevant security requirements defined in this Technical Specification and declared as being compliant to these requirements. In this case, TSP may reduce their burden to establish conformance of their policy to the relevant standards and in meeting the requirements of Dir.1999/93/EC and/or [Reg.910/2014/EU].

Guidance for conformity assessment to the security requirements defined in this TS can be found in CWA 14172-3.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

The European Directive 1999/93/EC and the Regulation (EU) No 910/2014 [Reg.910/2014/EU] establish a framework of requirements for the use of electronic signatures which are legally equivalent to hand-written signatures. This is the case for “advanced electronic signatures” which are based on a “qualified certificate” and which are created by a “secure-signature-creation device” according to Article 5.1 of 1999/93/EC and qualified signatures according to Article 25.2 of [Reg.910/2014/EU].

In particular, Annex II of Dir. 1999/93/EC and Article 24.2 (e) of [Reg.910/2014/EU] provide the requirements to be followed by TSP when issuing qualified certificates (QCs) and qualified TSP providing qualified trust services. More specifically, they shall

- use trustworthy systems and products which are protected against modification and ensure the technical security of the processes supported by them.

This Technical Specification defines security requirements for TWSs within the scope of the services a TSP needs to provide. It is assumed that TWSs being compliant to relevant security requirements of this TS may be adopted by TSPs to reduce their effort in deploying systems meeting Dir.1999/93/EC and/or [Reg.910/2014/EU]. This approach should support industry in developing systems which meet the requirements laid down in Annex II (f) of Dir.1999/93/EC and in Article 24.2 (e) of [Reg.910/2014/EU].

ETSI TS 119 411-1, 119 411-2, and 119 421 have been taken into account as reference. As a consequence, TWSs already compliant to relevant security requirements of this TS will require minimal configuration by TSPs using them, to meet the security requirements for TWS defined in ETSI TS 119 411-1, 119 411-2, and 119 421 (or equivalent ENs to be subsequently published). In addition, compliant TWS may be used by different TSPs without the need to repeat the conformity assessment.

TWSs for TSPs managing certificates shall comply with the security requirements defined in 5.2 and 5.3 to support TSPs in providing the following core services:

a) Registration of subject information (Registration Service);

b) Certificate generation (Certificate Generation Service);

c) Certificate dissemination (Dissemination Service);

d) Certificate revocation management (Revocation Management Service);

e) Certificate revocation status provision (Revocation Status Service).

TWS for TSPs managing certificates may comply with the other security requirements defined in 5.4 and 5.5 to support TSPs in providing the following supplementary services:

f) SCDev / QSCD production (Subject Device Provision Service);

g) Time-stamping functions (Time-Stamping Service).

TWS for TSPs managing electronic time-stamps shall comply with requirements defined in 5.5 to provide the Time-Stamping Service and may provide the other services, either a) – e) or a) – f) and comply with the corresponding requirements, defined in 5.2 and 5.3 or 5.2, 5.3, and 5.4, respectively.

All security requirements defined in this TS are either:

h) mandatory (indicated by SHALL (NOT) or SHALL (NOT));

i) recommended (indicated by SHOULD (NOT) or (NOT) RECOMMENDED); or

j) optional (MAY or MAY (NOT)).

1 Scope

1.1 General

This Technical Specification establishes security requirements for TWSs that can be used by a TSP in order to issue QCs and Non-Qualified Certificates (NQCs) as well as electronic time-stamps in accordance with Dir.1999/93/EC and with [Reg.910/2014/EU].

Security requirements for the Subject Device Provision Service, which includes SCDev/QSCD provision to subjects, are defined in this TS. However, requirements specific to SCDev/QSCD devices, as used by subjects of the TSP, are outside the scope of this TS. These requirements are defined as Common Criteria [CC] Protection Profiles (PP) in the EN 419211 series.

Recommendations for the cryptographic algorithms to be supported by TWSs are provided in ETSI/TS 119 312.

Although this TS is based on the use of public key cryptography, it does not require or define any particular communication protocol or format for electronic signatures, certificates, certificate revocation lists, certificate status information and time-stamp tokens. It only assumes certain types of information to be present in the certificates in accordance with Annex I of Dir.1999/93/EC and of [Reg.910/2014/EU]. Interoperability between TSP systems and subject systems is outside the scope of this document.

The use of TWSs that are already compliant to relevant security requirements of this TS should support TSPs in reducing their burden to establish conformance of their policy to ETSI TS 119 411-1, 119 411-2, and 119 421 (or equivalent ENs to be subsequently published) and in meeting the Annex I and Annex II requirements of Dir.1999/93/EC as well as the requirements from Annex I and Article 24.2 (e) of [Reg.910/2014/EU].

1.2 European Regulation-specific

The main focus of this document is on the requirements in Article 24.2 (e) of [Reg.910/2014/EU] whilst still facilitating the meeting of requirements in Dir.1999/93/EC, Annex II (f). In considering [Reg.910/2014/EU] it is important to take into account the following requirements of particular relevance to TSP trustworthy systems:

a) Article 24.2 (f) – “use trustworthy systems to store data provided to it, in a verifiable form so that:

   (i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,

   (ii) only authorised persons can make entries and changes to the stored data,

   (iii) the data can be checked for authenticity”;

b) Article 24.2 (g) – “take appropriate measures against forgery and theft of data”;

c) Article 24.2 (h) – “record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically”;

d) Article 24.2 (j) – “ensure lawful processing of personal data in accordance with Directive 95/46/EC”;

e) Article 24.2 (k) – “in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database”;

f) Article 24.3 – “If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication”;

g) Article 24.4 – "With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient”;

h) Article 42.1 – “A qualified electronic time stamp shall meet the following requirements:

   (i) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;

   (b) it is based on an accurate time source linked to Coordinated Universal Time; and

   (c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method”;

i) Annexes I, III, IV – requirements on data in qualified certificates

2 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.

EN 419211 (all parts), *Protection profiles for secure signature creation device*

ETSI TS 119 411-1, *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements*

ETSI TS 119 411-2, *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy Requirements for trust service providers issuing EU qualified certificates*

ETSI TS 119 421, *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing Electronic Time-Stamps*

NOTE Equivalent ENs will be published in 2015.

3 Terms, definitions, symbols and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1
activation data
data values, other than keys, that are required to operate cryptographic devices and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share)

[SOURCE: RFC 3647:2014, Clause 2]

3.1.2
advanced electronic signature
electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory;

c) it is created using means that the signatory can, with a high level of confidence, use under his sole control; and

d) it is linked to the data signed therewith in such a way subsequent change in the data is detectable

[SOURCE: Reg.910/2014/EU]

3.1.3
authentication data
data used to verify the claimed identity of a user requesting services from TWS

3.1.4
certificate
electronic attestation which links signature-validation-data to a person and confirms the name or the pseudonym of that person

[SOURCE: Reg.910/2014/EU]

3.1.5
certificate generation service
service that creates and signs certificates based on the identity and other attributes verified by the registration service

3.1.6
certificate policy
named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

[SOURCE: ISO/IEC 9594-8:2014, 3.5.10 ITU-T X.509; modified — An example in the original definition has not been included here.]

3.1.7
certification authority
CA
authority trusted by one or more users to create and assign certificates and which optionally may create the users' keys

[SOURCE: ISO/IEC 9594-8:2014, 3.5.16; ITU-T X.509, modified — The definition has been altered.]

3.1.8
certification-service-provider
entity or a legal or natural person who issues certificates or provides other services related to electronic signatures

[SOURCE: Dir.1999/93/EC]

3.1.9
cryptographic device
hardware-based cryptographic device that generates stores and protects cryptographic keys and provides a secure environment for the execution of cryptographic functions

3.1.10
digital signature
data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

[SOURCE: ISO 7498-2:1989, 3.3.26]

3.1.11
dissemination service
service that disseminates certificates to subjects, and if the subject consents, to relying parties and that also disseminates the CA's policy & practice information to subjects and relying parties

3.1.12
electronic seal
data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity

[SOURCE: Reg.910/2014/EU]

3.1.13
electronic signature
data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign

[SOURCE: Reg.910/2014/EU]

3.1.14
electronic signature / seal creation device
configured software or hardware used to create an electronic signature / seal

[SOURCE: Reg.910/2014/EU]

3.1.15
end-entity
certificate subject which uses its private key for purposes other than signing certificates

[SOURCE: ISO/IEC 9594-8:2014, 3.5.26; ITU-T X.509, modified — One out two possible definitions in the original text has been retained here.]

3.1.16
hash function
function which maps string of bits to fixed-length strings of bits, satisfying the following two properties:

a) it is computationally infeasible to find for a given output an input which maps to this output;

b) it is computationally infeasible to find for a given input a second input which maps to the same output.

[SOURCE: ISO/IEC 10118-1:2000, 3.5; modified — A note that was part of the original definition is not kept here.]

3.1.1715
nonce
randomly-generated value used in a communication protocol to ensure old messages cannot be reused in replay attacks

3.1.18
private key
key of an entity's asymmetric key pair which should only be used by that entity

[SOURCE: ISO/IEC 9798-1:2010, 3.22; modified — A small part of the original definition has been cut.]

3.1.19
public key
key of an entity's asymmetric key pair which can be made public

[SOURCE: ISO/IEC 9798-1:2010, 3.25]

3.1.20
qualified certificate
certificate that is issued by a qualified trust service provider and which meets the requirements laid down in Annex I of Reg.910/2014/EU

[SOURCE: Reg.910/2014/EU]

3.1.21
qualified electronic signature
advanced electronic signature that is created by a qualified signature / seal creation device and which is based on a qualified certificate

[SOURCE: Reg.910/2014/EU]

3.1.22
qualified electronic signature / seal creation device
electronic signature creation device that meets the requirements laid down in Annex II of Reg.910/2014/EU

[SOURCE: Reg.910/2014/EU]

3.1.23
registration service
service that verifies the identity and, if applicable, any specific attributes of a subject, and the results of which are passed to the Certificate Generation Service

3.1.24
relying party
user or agent that relies on the data in a certificate in making decisions

[SOURCE: RFC 5280:2008]

3.1.25
revocation management service
service that processes requests and reports relating to revocation to determine the necessary action to be taken, and the results of which are distributed through the Revocation Status Service

3.1.26
revocation status service
service that provides certificate revocation status information to relying parties and that may be a real-time service or may be based on revocation status information which is updated at regular intervals

3.1.27
secure-signature-creation device
signature-creation device which meets the requirements laid down in Annex III of Dir.1999/93/EC

[SOURCE: Dir.1999/93/EC]

3.1.28
security perimeter
one or more areas that are not necessarily co-located, where TWS are sited with relevant ancillary equipment (power supply, air conditioning, access control system, intrusion alarm system, fire protection and prevention system)

3.1.29
security policy
set of rules laid down by the security authority governing the use and provision of security services and facilities

[SOURCE: ISO/IEC 9594-8:2014, 3.5.60; ITU-T X.509]

3.1.30
self-signed certificate
certificate for one CA signed by that CA

[SOURCE: RFC 5280:2008]

3.1.31
signatory
person who creates an electronic signature

Note 1 to entry: The term signer is sometimes used as a synonym.

[SOURCE: Reg.910/2014/EU]

3.1.32
signature-creation data
unique data which is used by the signatory to create an electronic signature

[SOURCE: Dir.1999/93/EC and Reg.910/2014/EU]

3.1.33
signature-creation device
configured software or hardware used to create an electronic signature

[SOURCE: Reg.910/2014/EU]

3.1.34
subject
entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

3.1.35
subject device provision service
service that prepares and provides a Signature Creation Device to subjects

3.1.36
trustworthy system
information system or product implemented as either hardware and/or software that produces reliable and authentic records which are protected against modification and additionally ensures the technical and cryptographic security of the processes supported by it

3.1.37
time-stamp token
data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time

3.1.38
time-stamping service
service that generates and provides time-stamp tokens

3.1.39
TSP IT network systems
IT network systems consisting of network components such as firewalls, routers, switches and cabling

3.1.40
validation data
data, that is used to validate an electronic signature or an electronic seal

[SOURCE: Reg.910/2014/EU]

3.2 Symbols and abbreviations

For the purposes of this document, the following symbols and abbreviations apply.

ARL	Authority Revocation List
CA	Certification Authority
CC	Common Criteria
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CEN/ISSS	CEN Information Society Standardization System
CP	Certificate Policy
CRL	Certificate Revocation List
CSP	Certification Service Provider
EC	European Commission
EN	European Norm
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunications Standards Institute
ISSS	Information Society Standardization System
NQC	Non-Qualified Certificate
OCSP	Online Certificate Status Protocol
OS	Operating System
PKI	Public Key Infrastructure
PP	Protection Profile
QC	Qualified Certificate
QSCD	Qualified electronic Signature / Seal Creation Device
SCDev	Signature-Creation Device
TS	Technical Specification
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TSS	Time-Stamping Service
TST	Time-Stamp Token

TWS	Trustworthy System
UPS	Uninterruptable Power Supply
UTC	Coordinated Universal Time
WORM	Write Once Read Many
WS/E-SIGN	CEN/ISSS Electronic Signatures workshop

4 Description of a Trust Service Provider System

4.1 General

A Trust Service Provider (TSP), within this specification, provides and manages certificates used for the support of electronic signatures, prepares signature creation devices and/or issues time-stamp tokens. It is a primary assumption that a TSP will use a Public Key Infrastructure (PKI) for the management of certificates. The approach adopted in this specification is for a TSP to offer a number of services, each service having defined functions to facilitate service delivery. Each defined function is required to meet minimum security standards thus achieving trustworthy status.

The TSP's TWSs may consist of a number of subsystems each providing specific TSP services. Although this specification considers security requirements for the subsystems involved in the TSP's service, the aim is to provide the subject (signatory) and relying party a single view of the TSP and hence a single view of the TWSs employed by it. To ensure this, the customer interface, in this specification, is to the 'TSP Service' and not directly to the individual services offered by the TSP. As subsystems are further decomposed any functionality defined by other acceptable standards has been referenced.

In the context of the present document, a TSP SHALL provide its services by deploying TWSs that SHOULD be assessed beforehand to be compliant to this TS. TSPs SHALL implement relevant core services as described in section 4.2 when managing certificates and core services as described in section 4.4 when managing electronic time-stamps. A TSP may choose to implement any supplementary or additional service as deemed necessary by national, business and market requirements. However, if a TSP managing certificates implements the optional Subject Device Provision Service the TSP SHALL implement the General Security Requirements in 5.2 plus all security requirements for that service as specified in 5.4.

TWSs used for issuing and managing certificates are required to fulfil the General Security Requirements in 5.2 as well as specific Core Services Security Requirements in 5.3, and if applicable Supplementary Services Security Requirements in 5.4. TWSs used for issuing and managing electronic time-stamps are required to fulfil the General Security Requirements in 5.2 as well as specific Core Services Security Requirements in 5.3. In summary, a TSP SHALL deploy TWSs meeting all General and Core Security Requirements. It is important to note that this technical/security integration does not necessarily impede on the freedom of the TSP to run the different components of the service using different business entities.

4.2 TSP Core Services for certificate management

The core services for certificate management a TSP MAY provide and that CSPs in accordance to Dir.1999/93/EC and TSPs managing certificates in accordance to Reg.910/2014/EU SHALL implement are:

— **Registration Service:** verifies the identity and, if applicable, any specific attributes of a subject. The results of this service are passed to the Certificate Generation Service.

— **Certificate Generation Service:** creates and signs certificates based on the identity and other attributes of a subject as verified by the Registration Service.

— **Dissemination Service:** disseminates certificates to the CA, certificates to subjects, and if the subject consents, to relying parties. This service also disseminates the CA's policy and practice information to subjects and relying parties.

— **Revocation Management Service:** processes requests and reports relating to revocation and suspension (if used) to determine the necessary action to be taken. The results of this service are distributed through the Revocation Status Service.

— **Revocation Status Service:** provides certificate revocation status information to relying parties. This service may be a real-time service or may be based on revocation status information which is updated at regular intervals.

The figure below shows the relationship between the Revocation Management Service and the Revocation Status Service. In the figure, message A updates the TSP Certificate Status Database whereas Message B is either data 'pushed' to the Revocation Status Service or is a query/response message.

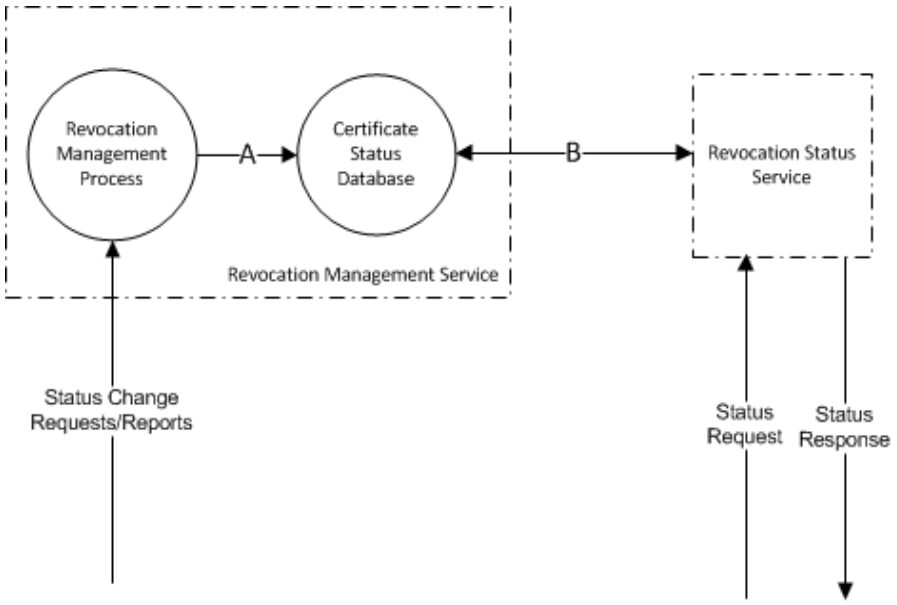

Figure 1 — Messaging between Revocation Management Service and Revocation Status Service

4.3 TSP Supplementary Services for certificate management

The supplementary service a TSP managing certificates in accordance to Reg.910/2014/EU may provide is:

Subject Device Provision Service: Prepares and provides a Signature Creation Device (SCDev) to subjects.

NOTE Examples of this service are:

a) a service which generates the subject's key pair and distributes the private key to the subject;

b) a service which prepares the subject's QSCD and device enabling codes and distributes the QSCD to the registered subject.

It is important to note that this service may provide a SCDev and/or a QSCD. Within this document the security requirements applicable to SCDevs are equally applicable to QSCDs, where QSCDs meet the additional requirements stated in Annex III of Dir.1999/93/EC and in Annex II of Reg.910/2014/EU. No distinction is made whether the SCDev/QSCD is implemented in hardware or software.

4.4 TSP Core Services for electronic time-stamp management

The core service for electronic time-stamp management a TSP MAY provide and that TSP managing electronic time-stamps in accordance to Reg.910/2014/EU SHALL implement are:

Time-Stamping Service: a third party, trusted to generate and provide time-stamp tokens. A time-stamp token provides evidence that a data item existed before a certain point of time.

Within this document, security requirements are only provided for the time-stamping service, which cryptographically binds time values to data values. The figure below shows a conceptual TSA providing the time-stamping service.

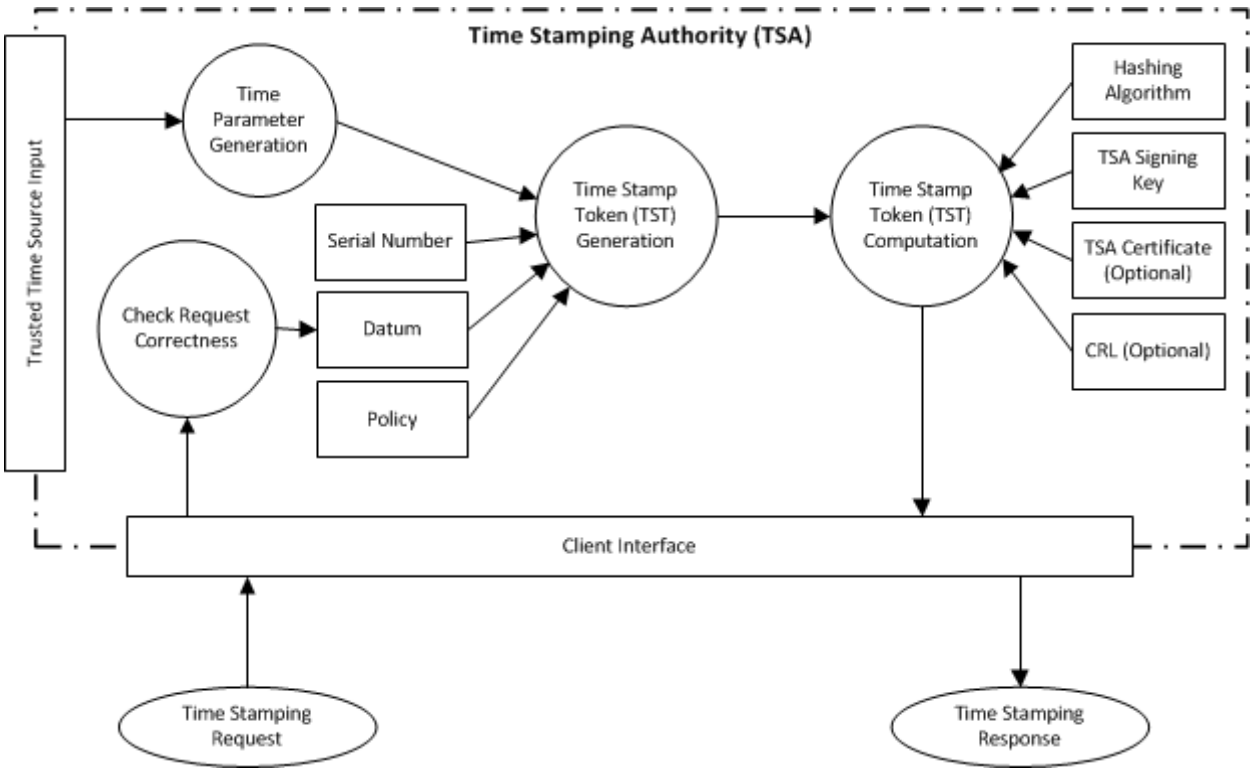

Figure 2 — Time-Stamping Service

4.5 Overall Architecture

A TSP's logical architecture is shown in the figure below, and can be seen to facilitate the production and use of a signed transaction from the subject to a relying party. This figure illustrates both mandatory and optional services along with the TSP's interfaces to its subjects, relying parties and to any external Trust Services.

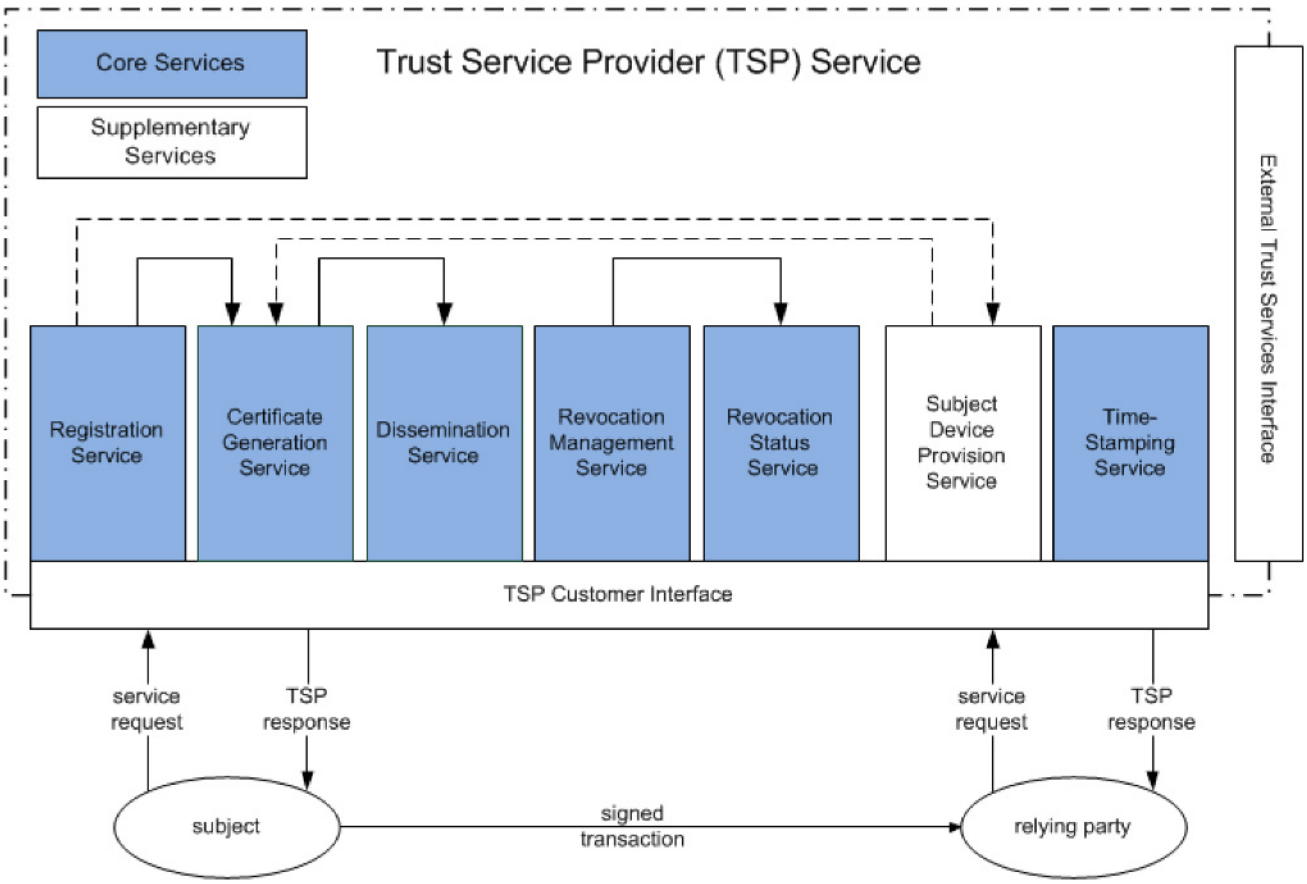

Figure 3 — TSP Logical Architecture

As shown, the TSP managing certificates provides initial registration and certificate generation as well as subsequent dissemination. Primary certificate lifecycle management (where no revoked or suspended states exist) is provided by way of the Registration, Certificate Generation and Dissemination Services. Secondary certificate lifecycle management, where exceptional certificate states exist (e.g. revoked or suspended states), is provided by the Revocation Management and Revocation Status Services. The Subject Device Provision Services is a possible supplemental service for such a TSP.

Time-Stamping Service is either an optional additional service for a TSP managing certificates or a single core service a TSP managing electronic time-stamps may provide in accordance with Reg.910/2014/EU.

The TSP Customer Interface provides access to the TSP's services for subjects and relying parties. The optional External Trust Services Interface provides access to external services e.g. Cross-certification with other TSPs, trusted archiving services, etc. A TSP may utilize multiple TWSs to provide core and, if applicable, supplementary services.

5 Security Requirements

5.1 Relationship between Security Requirements and Recommendations

The figure below shows the relationship between security requirements and recommendations defined in 5.2, 5.3, 5.4 and 5.5, and in Annexes A and B below.

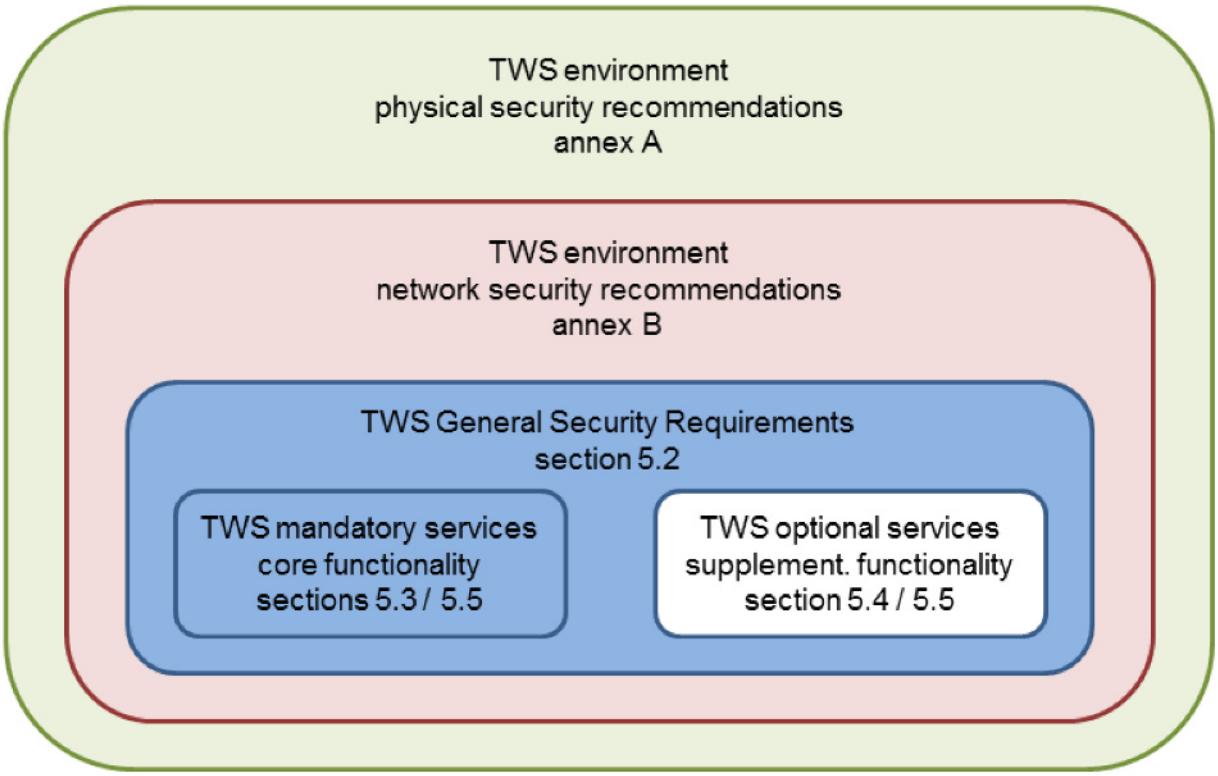

Figure 4 — Security Requirements and Recommendations Relationship

Subclause 5.2 defines “General Security Requirements” applicable to **core** (see 4.2, 4.4) and **supplementary** (see 4.3) TSP services.

Subclause 5.3 defines additional security requirements specific to TSP managing certificates **core** services.

Subclause 5.4 defines additional security requirements specific to TSP **supplementary** services.

Subclause 5.5 defines additional security requirements specific to TSP managing electronic time-stamps **core** services. This service may be a supplementary service to TSPs managing certificates.

Physical and network security recommendations for the TWS operational environment are provided in Annexes A and B, respectively. They should be applied for the secure operation / protection of the TWS at the TSP location.

5.2 General Security Requirements

5.2.1 Management

5.2.1.1 M1 Systems and Security Management

A TSP needs to manage its security in order to operate TWSs.

[M1.1]

TWSs SHALL support roles with different privileges.

[M1.2]

As a minimum, TWSs for all services SHALL maintain the following privileged roles a), d) - f):

a) **Security Officers:** Having overall responsibility for administering the implementation of the security policies and practices;

b) **Registration Officers**: Responsible for verifying information that is necessary for certificate issuance and approval of certification requests;

c) **Revocation Officers:** Responsible for operating certificate status changes;

d) **System Administrators:** Are authorized to install, configure and maintain TWSs for service management;

e) **System Operators:** Are responsible for operating TWSs on a day-to-day basis. Authorized to perform system backup and recovery;

f) **System Auditors:** Authorized to view archives and audit logs of TWSs for the purposes of auditing the operations of the system in line with the security policy.

TWSs providing the Registration / Revocation Service SHALL additionally maintain the role b) / c), respectively.

[M1.3]

TWSs SHALL be able to associate users with these roles.

[M1.4]

TWSs SHALL be capable of ensuring:

a) a user that is authenticated in the role Security Officer or Registration Officer or Revocation Officer shall not have the privileges of a System Auditor role;

b) a user that is authenticated in the role System Administrator and/or System Operator shall not have the privileges of a Security Officer or a System Auditor role.

NOTE Requirement [M1.4] does not restrict access to the audit records, which is subject of requirement [AA5].

5.2.2 Systems and Operations

5.2.2.1 SO1 Operations Management

A TSP operating TWSs needs to ensure that its operations management functions are adequately secure and the underlying operating systems are adequately hardened.

[SO1.1]

A TWS manufacturer SHALL provide sufficient installation, administration and user guidance to allow the TWS to be:

a) deployed in a manner where the risk of systems failure is minimal;

b) correctly and securely operated;

c) protected against viruses and malicious code to ensure the integrity of the systems and the information they process is upheld;

d) patched on a regular and timely manner to fix known security vulnerabilities.

[SO1.2]

Operating systems SHALL be configured in such a way that functionality not needed for operation is deactivated.

[SO1.3]

All operating systems and other software needed for TWS operation SHALL be patched on a regular and timely manner to fix known security vulnerabilities and to protect TWS against viruses and malicious code. Patches SHALL be tested before being deployed to ensure that they do not disturb normal operation in terms of TSP services integrity and availability.

Risks related to the deployment and non-deployment of patches SHOULD be identified and assessed by the TSP. Risk treatment options SHOULD be defined if needed with the support of the TWS manufacturer.

[SO1.4]

Operating system accounts SHALL be configured in such a way that users are equipped with least privileges access rights only.

[SO1.5]

Operating system accounts SHALL be related to single individuals. (no group accounts) Granted access rights SHALL be withdrawn after a given time without user activity.

NOTE In general, accounts provided by TWS underlying operating system(s) are different to accounts provided by the TWS itself. Therefore, requirements [SO1.4] and [SO1.5] supplements access control requirements applicable for TWS contained in 5.2.4.2.

5.2.2.2 SO2 Business Continuity

Business Continuity ensures that the TSP's services are quickly and securely restored within a defined recovery time objective (RTO) in case of failure in a TWS.

[SO2.1]

TWSs providing the following services SHALL withstand a single failure, and continue uninterrupted operations:

a) Dissemination Service;

b) Revocation Management Service;

c) Revocation Status Service.

It is RECOMMENDED that these services provide at least 99,8 % availability on a monthly basis.

NOTE The requirement of a continued uninterrupted dissemination service (point a) does not put any requirements on the certificate generation or subject device provision service in terms of continued uninterrupted operation.

[SO2.2]

In the event of a disaster, TWSs SHALL provide functions to enable the TSP to continue operations using alternative (e.g. backup) components of TWSs.

NOTE Disaster situations include failure of several critical components of a TSP system, including hardware and software. Availability requirements are not applicable in a disaster situation. The maximum acceptable delay for service resumption is usually specified in the applicable TSP's policy document.

[SO2.3]

Failover from primary to disaster recovery systems SHALL NOT put unacceptable risk on the trustworthy nature of the systems.

5.2.2.3 SO3 Time Synchronization

The issuing of certificates and their subsequent management is time related, therefore a need exists to ensure TWSs are suitably synchronized to a standard time source. This requirement is separate from any time-stamping requirements that may be in place by the TSP.

[SO3.1]

All clocks of TWSs used for delivering TSP services that are time dependant SHALL be regularly synchronized, such as on a daily basis, to a trusted source of Coordinated Universal Time (UTC) within one second.

It is RECOMMENDED to use two independent trusted sources of UTC to maintain a resilient time source.

5.2.3 Identification and Authentication

5.2.3.1 Functionalities

The Identification and Authentication functions restrict access and use of TWSs to authorized persons only. Identification and Authentication may be provided either by the underlying operating software or directly by the TWS itself.

5.2.3.2 Security Requirements

5.2.3.2.1 IA1 User Authentication

[IA1.1]

TWSs SHALL require each user to identify him/herself and be successfully authenticated before allowing any action on behalf of that user or role assumed by the user.

[IA1.2]

Mechanisms SHALL be implemented to reduce the risk of an authenticated user session being taken over if the user's input device is left unattended, for example by terminating a user session after a given idle period.

[IA1.3]

Re-authentication SHALL be mandatory after log-out.

5.2.3.2.2 IA2 Authentication Failure

[IA2.1]

If the number of unsuccessful authentication attempts equals or surpasses the maximum number of allowed attempts, the TWS SHALL prevent further authentication attempts for a defined period of time, e.g. 5 min.

[IA2.2]

If the number of unsuccessful authentication attempts equals or surpasses the maximum number of allowed attempts, and the role is that of an administrator, then a notification event (alarm, message, etc.) SHOULD be created.

NOTE This is not applicable to TWSs that use *in situ* token authentication mechanisms, e.g. a smartcard reader with a built-in PIN pad.

5.2.3.2.3 IA3 Verification of Secrets

[IA3.1]

TWSs SHALL provide a mechanism(s) to prevent the use of weak secrets for authentication.

NOTE Examples for week secrets are passwords with insufficient length or complexity and cryptographic keys with insufficient entropy.

5.2.3.2.4 IA4 Two-Factor Authentication Mechanism

[IA4.1]

TWSs SHALL provide at least a two factor authentication mechanism to authenticate users.

5.2.4 System Access Control

5.2.4.1 Functionalities

System Access Control functions control use of objects of TWSs to authenticated users only. This is applicable to all sensitive objects of the TWS. System Access Control may be provided either, by the underlying operating software, or directly by the actual component itself. Access rights to specific TWS objects are determined by the owner of the object based on the identity of the user attempting the access and:

a) the access rights to the object granted to the user or;

b) the privileges held by the user.

5.2.4.2 Security Requirements — System Access Control

[SA1.1]

TWSs SHALL provide the capability of controlling and limiting access by identified users to the system/user objects they are responsible for.

[SA1.2]

TWSs SHALL provide access protection to sensitive residual information.

5.2.5 Key Management

5.2.5.1 Functionalities

A TWS will typically use cryptographic keys to provide integrity, confidentiality and authentication functions within its own subsystems and in between subsystems. Unauthorized use, disclosure, modification, or substitution of keys that have an impact on the TWS security shall be prevented and/or detected in a timely manner. It is essential that (lifecycle) management of these keys is carried out securely.

Due to the different threats on the keys of TWSs, depending upon where and how they are used, it is important to categorize keys according to their risk profile. For this specification, keys are separated into the following categories:

a) TSP Signing Keys - Certificate Generation Service's private keys for producing qualified certificates or non-qualified certificates and Revocation Status Service's keys for signing certificate status information and Time-Stamping Service's keys for signing / producing qualified or non-qualified electronic time-stamps;

b) Infrastructure Keys – these are keys used by the TWSs for processes such as key agreement, subsystem authentication, audit log signing, encrypting transmitted or stored data, etc. Short term session keys are not categorized as Infrastructure keys;

c) Control Keys – these are keys used by (identified) users managing or using the TWS and may provide authentication, signing or confidentiality services for those users interacting with the system.

d) Session keys – these keys are short term ones used for single/short transactions.

NOTE Keys used for SCDev Preparation (see 5.4.2.2.1) do not fall into one of these categories.

In terms of security requirements, TSP Signing Keys are long-term keys whose impact from exposure is high. Consequently, countermeasures for managing this risk are also high, both in number and in effect. Infrastructure keys are also considered high risk but due to their distributed functionality and shorter lifespan they are a lower risk in comparison to signing keys. The lowest risk keys, used by TSP, are considered to be those used by personnel for controlling TWSs, as these are used by trusted users and have an even shorter lifespan. Session keys are treated as sensitive information but with lower security requirements to the above stated categories.

Infrastructure, Control and Session Keys may be either asymmetric or symmetric keys.

Key Generation

Key Generation refers to the creation of keys.

Key Distribution

Key Distribution is the function of distributing the public TSP Signing Key, Infrastructure or Control keys.

Key Usage

This is the controlling of usage of generated keys within cryptographic algorithms to provide cryptographic services.

Key Change

Key change may be:

1) Programmed – where a key is replaced by a newly generated key once it reaches the end of its operational life (as determined by policy);

2) Non-Programmed – where a key is replaced by a newly generated key, e. g. if it has been compromised.

Key Destruction

When a key is compromised or when it reaches the end of its operational life it may be destroyed to prevent any further use of the key.

Key Storage, Backup and Recovery

After Key Generation, the keys may be stored in secure environments and may be copied and backed up to meet operational requirements. These backed up keys may need to be recovered when for example the existing key is inadvertently destroyed.

Key Archival

At the end of a key's operational life it may be archived to allow use of the key at some later (undefined) time. This is specifically in reference to public keys used to verify digital signatures but does not preclude archiving of other types of keys where justified.

5.2.5.2 Security Requirements

5.2.5.2.1 KM1 Key Generation

[KM1.1]

Certificate Signing, Infrastructure and Control Keys SHALL be generated, used and stored inside a cryptographic device.

[KM1.2]

The cryptographic device used for TSP Signing Keys SHALL be evaluated and certified to fulfil the requirements of the relevant part of ETSI TS 119 411-1, 119 411-2, and 119 421 (or equivalent ENs to be subsequently published).

[KM1.3]

The cryptographic device used for TSP Signing Keys SHALL ONLY generate TSP Signing Keys under at least dual person control.

Dual person control of the required function MAY be achieved either directly by the cryptographic device or by the TWS implementing suitable dual person controls.

[KM1.4]

Infrastructure and Control Keys SHALL be generated, used and stored inside a cryptographic device that fulfils the requirements of the relevant part of ETSI TS 119 411-1, 119 411-2, and 119 421 (or equivalent ENs to be subsequently published), or of another suitable specification with at least equivalent requirements.

NOTE Suitable specifications could be other Common Criteria [CC] Protection Profiles for cryptographic modules or the standard [ISO/IEC 19790].

[KM1.5]

The key generation algorithm and selected key length for TSP Signing Keys shall be one which is recognized as being fit for the purposes of certificates as issued by the CA.

NOTE See ETSI/TS 119 312 for guidance on algorithms and their parameters.

[KM1.6]

TWS used to generate Root CA keys, SHALL be operated on an isolated stand-alone system that has no physical connection to other systems. The system SHOULD be switched off when not needed.

5.2.5.2.2 KM2 Key Distribution

[KM2.1]

Private and secret keys SHALL NOT be distributed in plain text.

[KM2.2]

The TWSs of a TSP SHALL distribute cryptographic keys in accordance with a specified cryptographic key distribution method that is recognized being secure for the purpose.

[KM2.3]

The public key associated with the TSP Signing Keys and/or Infrastructure Keys (e.g. Revocation Status Service, Time-Stamping Service) MAY need to be made available to subjects and relying parties. The integrity and authenticity of this public key and any associated parameters SHALL be maintained during initial and subsequent distribution.

The public key associated with the TSP Signing Keys may be made available in a certificate signed by itself or issued by another Certification Authority (CA). By itself, a self-signed certificate cannot be proven to have come from the CA.

[KM2.4]

A self-signed certificate for TSP Signing Keys SHALL have the following properties:

a) the certificate signature SHALL be verifiable using data provided within the certificate;

b) the certificate subject and issuer fields SHALL be identical.

NOTE Additional measures, such as checking the fingerprint of the certificate (hash value calculated over the self-signed certificate) against information provided by a trusted route, are RECOMMENDED to give assurance of the correctness of this certificate.

[KM2.5]

The TWS SHALL be capable of producing a fingerprint of a self-signed certificate using a hashing algorithm which is recognized as being fit for the purposes of certificates as issued by the CA.

NOTE See ETSI/TS 119 312 for guidance on algorithms and their parameters.

5.2.5.2.3 KM3 Key Usage

[KM3.1]

Access controls SHALL be in place for all cryptographic devices used for Certificate Signing, Infrastructure and Control Keys.

[KM3.2]

The Certificate Generation Service SHALL provide support for dual person control when enabling use of TSP Signing Keys.

NOTE Typically, this would provide administration functionality of the Certificate Generation Service.

[KM3.3]

It is RECOMMENDED that separate infrastructure keys are generated for separate functions. This reduces the impact of a single key compromise. Infrastructure keys associated with the Registration Service, Certificate Generation Service and the Revocation Management Service SHOULD NOT be shared.

[KM3.4]

TWSs providing the Subject Device Provision Service SHALL ensure that subject keys for creating electronic signatures are separate from those used for other functions e.g. encryption or authentication.

[KM3.5]

Authorized key usage SHALL ONLY occur within the operational life of the key (as determined by certificate policy).

[KM3.6]

Before TWSs rely on certificates for asymmetric Infrastructure or Controls Keys they SHALL ensure that the certificates related to these keys are still valid. This MAY require the checking of suitable ARLs (Authority Revocation Lists)/CRLs (Certificate Revocation Lists) and/or the query of suitable on-line servers (e. g. OCSP servers).

5.2.5.2.4 KM4 Key Change

[KM4.1]

Infrastructure and Control Keys SHOULD be changed on a regular basis, e.g. annually.

[KM4.2]

Key changeover SHALL be carried out securely and MAY be an online or an out-of-band change.

[KM4.3]

Keys SHOULD be changed immediately when the keys are compromised or suspected to be compromised or the underlying algorithms or key length are considered to have become unsuitable.

5.2.5.2.5 KM5 Key Destruction

[KM5.1]

When TSP Signing Keys reach the end of their life they SHALL be destroyed or put beyond use such that the signing keys cannot be retrieved.

[KM5.2]

When systems have been used to generate, use or store secret/private keys and are to be withdrawn from service or transferred their associated keys SHALL be destroyed or put beyond use.

[KM5.3]

TWSs SHALL provide the capability to securely destroy plaintext secret and private keys stored in both hardware and software.

[KM5.4]

Key destruction SHALL be carried out using secure destruction methods. Examples of such methods (dependent upon the level of risk exposure) are: overwriting (multiple times)/degaussing magnetic storage media multiple times, or shredding the media.

5.2.5.2.6 KM6 Key Storage, Backup and Recovery

[KM6.1]

All private/secret keys SHALL be securely stored.

[KM6.2]

TSP Signing Keys SHALL be stored in a cryptographic device which meets the evaluation and certification requirements outlined in requirement [KM1.2] (Key Generation).

[KM6.3]

Private/secret Infrastructure and Control Keys SHALL be stored in a cryptographic device.

[KM6.4]

If any private/secret Certificate Signing, Infrastructure or Control key is exported from the cryptographic device, it SHALL be protected to ensure its confidentiality and integrity to the same or higher security level as within the device.

Wherever the private/secret key is protected for its export by encryption, only cryptographic algorithms and algorithm parameters of equivalent or higher strength SHALL be used.

[KM6.5]

TWSs SHALL ensure that backup, storage and recovery of private/secret Certificate Signing, Infrastructure and Control Keys are only performed by authorized users (e.g. Security Officer role).

[KM6.6]

TWSs SHALL ensure that backup, storage and recovery of private TSP Signing Keys are only performed by authorized users under at least dual person control.

[KM6.7]

TWSs SHALL NOT contain functions that allow for backup or escrow of private subject signature keys.

5.2.5.2.7 KM7 Key Archival

[KM7.1]

TWSs SHALL NOT contain functions that allow archiving of subject signature keys (private keys).

5.2.6 Accounting and Auditing

5.2.6.1 AA1 Audit Data Generation

[AA1.1]

As a minimum, TWS SHALL log the following events:

a) significant TWS environmental, key management and certificate management events;

b) as described in the service audits sections (R3, CG4, RM3, RS3, TS5, SP4);

c) start-up and shut-down of the audit data generation function;

d) changes to the audit parameters;

e) actions taken by TWS due to audit storage failure.

5.2.6.2 AA2 Guarantees of Audit Data Availability

[AA2.1]

The system SHALL maintain audit data and guarantee sufficient space is reserved for that data.

[AA2.2]

The audit log SHALL NOT be automatically overwritten.

[AA2.3]

The system SHALL generate an alarm when space left for audit data are below a defined threshold (e.g. 1/5 of the total space).

5.2.6.3 AA3 Audit Data Parameters

[AA3.1]

All audit records (including service specific audit logging) SHALL contain the following parameters:

a) date and time of event;

b) type of event;

c) identity of the entity responsible for the action;

d) success or failure of the audited event.

5.2.6.4 AA4 Selectable Audit Review

[AA4.1]

All TSP TWSs SHALL provide the capability to search for events in the audit log based on the date and time of event, type of event and/or identity of the user.

[AA4.2]

The audit records SHALL be presented in a suitable data format for the user to be able to interpret the information.

5.2.6.5 AA5 Restricted Audit Review

[AA5.1]

TWSs SHALL prohibit all users read access to the audit records, except those users that have been granted explicit read access, e.g. those with System Auditor role. Additional users, e.g. System Operators or System Administrators, MAY have read access to audit records if needed for the operation.

[AA5.2]

Modifications of the audit records SHALL be prevented.

5.2.6.6 AA6 Generation of Alarm

[AA6.1]

TWSs SHALL generate an alarm upon detection of a potential or actual security violation. A simple example is to email the Security Officer or use suitable monitoring agents capable of generating alarms.

5.2.6.7 AA7 Guarantees of Audit Data Integrity

[AA7.1]

TWSs SHALL ensure the integrity of the audit data.

To achieve this requirement, TWSs SHOULD provide a digital signature, keyed hash or an authentication code with each entry in the audit log, computed over the entire audit log or over the current entry and the cryptographic result of the previous one.

[AA7.2]

TWSs SHALL provide a function to verify the integrity of the audit data.

5.2.6.8 AA8 Guarantees of Audit Timing

[AA8.1]

A trusted time source (as outlined in SO3 - Time Synchronization) SHALL be used to mark the time of audited event.

5.2.7 Archiving

5.2.7.1 AR1 Archive Data Generation

[AR1.1]

TWSs SHALL be capable of generating an archive on media appropriate for storage and subsequent processing in providing necessary legal evidence in support of electronic signatures.

[AR1.2]

At a minimum, the following items SHALL be archived:

a) all certificates;

b) all CRLs/ARLs;

c) all Audit logs.

[AR1.3]

Each entry SHALL include the time at which the event occurred.

[AR1.4]

The archive SHALL NOT include critical security parameters or other confidential information in an unprotected form.

5.2.7.2 AR2 Selectable Search

[AR2.1]

The system SHALL provide the capability to search for events in the archive based on the type and time of events.

5.2.7.3 AR3 Integrity of Archived Data

[AR3.1]

Each entry in the archive SHALL be protected from modification in such a way that the integrity of entries is ensured and deletion is either not possible (e. g using WORM media) or only possible under at least dual person control.

5.2.8 Backup and Recovery

5.2.8.1 General

Backup and Recovery in this section only covers system information, subject information and all other data necessary to restore the system after a failure or disaster. It does NOT cover backup and recovery of keys, security requirements for which are found in 5.2.5.2.6 (KM6).

5.2.8.2 BK1 Backup Generation

[BK1.1]

TSP TWSs SHALL include a backup function.

[BK1.2]

The data stored in the backup SHALL be sufficient to recreate the state of the system.

[BK1.3]

A user linked to a role with sufficient privileges SHALL be capable of invoking the backup function on demand.

5.2.8.3 BK2 Integrity and Confidentiality of Backup Information

[BK2.1]

Backups SHALL be protected against modification in a way that allows verifying its integrity.

[BK2.2]

Critical security parameters and other confidential information SHALL be stored in a protected form in order to ensure confidentiality and integrity.

5.2.8.4 BK3 Recovery

[BK3.1]

The system SHALL include a recovery function that is able to restore the state of the system from a backup.

[BK3.2]

Recovery of backups SHALL ONLY be possible by authorized users under at least dual person control.

5.2.9 Network Security Requirements for the Operational Environment

Network security requirements for the operational environment of the TWS are necessary to protect TWS against unauthorized access and to provide the infrastructure for the availability of TSP services in terms of network connectivity. They are included in Annex B and do not constitute requirements on TWS providing the TSP services itself but on dedicated TSP IT network systems in the operational environment of the TWS that protect them at the location of the TSP.

NOTE In general, network security requirements cannot be checked at the TWS manufacturer without the TSP IT network systems in the operational environment but need to be checked at the site where the TWS are installed, i.e. at the location of the TSP.

5.2.10 Physical Security Requirements for the Operational Environment

Physical security requirements for the operational environment of the TWS are necessary to prevent unauthorized physical access to TWS and to provide the necessary infrastructure for the availability of services in terms of power, air conditioning, fire protection, and network connectivity. They are included in Annex A and do not constitute requirements on TWS itself but on its operational environment at the TSP site.

NOTE In general, physical and environmental security requirements cannot be checked at the TWS manufacturer without the physical operational environment but need to be checked at the site where the TWS are installed, i.e. at the location of the TSP.

5.3 Core Services Security Requirements for TWS managing certificates

5.3.1 General

[GE.1]

All external messages created and sent by TWS SHALL:

a) be protected (e.g. by using encryption, message authentication codes, digital signatures, etc.) by using the service's Infrastructure Keys;

b) contain a message time, to indicate the time at which the sender created the message;

c) include replay attack protection (e.g. by using nonces).

NOTE This requirement does not apply to TWS internal communications.

5.3.2 Registration Service

5.3.2.1 Functionalities

— Certificate Application

Certificate application is carried out by the Registration Service after identification of the subject has been carried out meeting the requirements specified in the associated certificate policy, e.g. EN 319411-2 or EN 319411-3.

— Subject Data Management

The Registration Service by its nature manages end entity subject data. The data may be affected by many different data protection requirements.

5.3.2.2 Security Requirements

5.3.2.2.1 R1 Certificate Application

A Registration Officer verifies by appropriate means, in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a certificate is issued.

[R1.1]

If the certificate application contains any subject sensitive information, the certificate request SHALL be protected before being forwarded from the Registration Service to the Certificate Generation Service thus ensuring message confidentiality. TWSs SHALL ensure this functionality is provided if required.

NOTE Subject sensitive information comprises any sensitive information such as medical records, criminal background history that identifies or can be used to identify, contact, or locate the person to whom such information pertains

[R1.2]

In case the TSP does not generate the key pair of the entity requesting certification, a suitable mechanism SHALL be implemented to ensure that the entity is the actual holder of the private key. (Proof of Possession)

[R1.3]

In case the TSP does not generate the key pair of the entity requesting certification, a suitable mechanism SHALL be implemented to verify that key algorithm and parameters are recognized by industry as being fit for the intended use.

NOTE See ETSI/TS 119 312 for guidance on algorithms and their parameters.

[R1.4]

The Registration Service SHALL be configured to allow collection of enough data needed for the issuance of the certificate.

NOTE Mandatory data for QCs are specified in Annex I of [Dir.1999/93/EC] and Annexes I, III, IV of [Reg.910/2014/EU].

[R1.5]

TWSs SHALL provide a mechanism to allow approval of certificate applications, by a Registration Officer, before sending a certificate request to the Certificate Generation Service".

[R1.6]

The following attribute SHALL accompany the application:

- Information about the subject's consent to disseminate the certificate to relying party via the Dissemination Service

Subject's consent for certificate to be published may be via a subscriber agreement (see the relevant parts of ETSI TS 119 411-1 and 119 411-2 or equivalent ENs to be subsequently published).

[R1.7]

Certificate requests from the Registration Service SHALL be protected for authenticity and data integrity. This MAY be achieved with a digital signature or the establishment of a trusted channel to the Certificate Generation Service using the Infrastructure or Control Keys.

5.3.2.2.2 R2 Subject Data Management

[R2.1]

TWSs SHALL ensure the confidentiality of subject sensitive information. (see also [R1.1])

5.3.2.2.3 R3 Registration Service Audit

[R3.1]

The following Registration Service specific events SHALL be logged:

- all events relating to registration including certificate re-key/renewal requests;
- all events relating to approved requests for Certification.

5.3.3 Certificate Generation Service

5.3.3.1 Functionalities

— Certificate Generation

After receiving a certificate application from the Registration Service, TWSs generate a certificate that contains the public key supplied. This ensures the TSP has 'locked' the binding of the subject's public key to a set of attributes which reflects its identity.

TWSs may also send their Infrastructure or Control Public Keys to be certified by the Certificate Generation Service. This produces Infrastructure or Control Certificates.

Following Certificate Generation, the certificate may be made available via the Dissemination Service, via the supplementary Subject Device Provision Service or to the subject directly.

Infrastructure and Control Certificates may be provided directly to the trustworthy component requiring its use.

— Certificate Renewal

During the period prior to the expiration of the certificate, such period being defined by applicable certificate policy, the certificate may be renewed. Certificate renewal may consist of the following scenarios:

- Re-Certification – a new certificate is produced using the existing public key;
- Re-Key – a new public key is certified using the registration information used to generate the previous certificate.

Certificate renewal covers Infrastructure, Control certificates and certificates issued to subjects.

— Cross Certification

This mechanism allows the establishing of a one-way or a mutual trust relationship between two (or more) TSPs. The responder TWS provides a cross certificate to the requester TWS who provides its public key for certification. The subjects of the responder TSP can now trust the requester TSP.

5.3.3.2 Security Requirements

5.3.3.2.1 CG1 Certificate Generation

[CG1.1]

The Certificate Generation Service SHALL verify the integrity, data origin authenticity, and ensure where necessary, the privacy and confidentiality of the certificate request message received from the Registration Service.

[CG1.2]

The certificate request SHALL be processed securely and checked for conformance with the applicable certificate policy.

[CG1.3]

In case the TSP does not generate the key of the entity requesting certification the TWS SHALL ensure that the Proof of Possession is validated.

[CG1.4]

The key used to sign a certificate SHALL ONLY be used for signing certificates and, optionally, the related Revocation Status Data (e. g. CRLs and OCSP responses).

[CG1.5]

This service SHALL ONLY generate certificates that are consistent with the allowed profiles.

[CG1.6]

All certificates issued by a TWS SHALL have the following properties:

a) a unique distinguished name. Where a pseudonym is used this SHALL be clearly indicated;

b) the public key in the certificate is related to the subject's private key;

c) the advanced electronic signature of the TSP, created using the TSP Signing keys;

d) a serial number assigned by the TWS.;

e) the certificate SHALL specify a valid from time that does not precede the current time and a valid until time that does not precede the valid from time;

f) reference to the certificate policy under which the certificate is issued.

5.3.3.2.2 CG2 Certificate Renewal

[CG2.1]

For re-certification, the TWS SHALL ensure process security against certificate substitution attacks.

[CG2.2]

Re-certification of Control and Infrastructure certificates SHALL comply with KM4 – Key Change (5.2.5.2.4).

Control and Infrastructure certificates may be re-keyed or re-certified online or by out-of-band means.

[CG2.3]

TWSs SHALL ensure that TSP Signing keys are not used after expiry of the corresponding certificate.

[CG2.4]

If a TWS provides a mechanism for the re-certifying and/or re-keying of subject keys, it SHALL be as secure as the initial certificate generation.

[CG2.5]

It is RECOMMENDED that certificates issued to subjects be renewed prior to their expiry as the messaging between TSP and subject can be secured using the old keys/certificates. A TWS SHALL reject a renewal request signed with an expired or revoked key.

5.3.3.2.3 CG3 Cross-Certification

[CG3.1]

Where a TWS uses cross-certification for establishing one-way or mutual trust with other TWSs, the process SHALL ensure that:

a) generation of (cross-) certificates is performed at least under dual person control;

b) authentication and integrity of messages are maintained when transmitted between two TWSs.

5.3.3.2.4 CG4 Certificate Generation Service Audit

[CG4.1]

The following Certificate Generation Service specific events SHALL be logged:

a) all events relating to the life-cycle management of Certificate Signing, Infrastructure, and Control certificates;

b) all events relating to the life-cycle management of TSP Signing keys;

c) all events relating to the life-cycle management of certificates issued to subjects;

d) all events relating to cross-certification.

5.3.4 Dissemination Service

5.3.4.1 D1 Dissemination Management

[D1.1]

Certificate dissemination by TWSs SHALL be limited to the subject and to relying parties according to the limits expressed by the subject.

[D1.2]

The dissemination process SHALL manage the certificates according to [D1.1] requirements.

5.3.4.2 D2 Import/Export of Objects

[D2.1]

Whenever a repository is set up, an access control policy SHALL be defined to securely manage the access to stored data:

a) read access privileges SHALL be granted to subjects and to authorized entities according to the applicable security policy;

b) write access privileges SHALL be limited to authorized roles, according to the definition of roles proposed in 5.2.1.

5.3.5 Certificate Revocation Management Service

5.3.5.1 General

Figure 1 provides details of the Revocation Management Service, the Revocation Status Service and their relationship with other entities. This subclause (5.3.5) and the following subclause (5.3.6) make use of this figure for illustrating the requirements.

5.3.5.2 Functionalities

Certificate Status Change Requests

The subject and the TSP may request suspension (temporary revocation) of a certificate. A corresponding request to restore a certificate from suspension to operational use may be made by the subject if it determines that the key is actually not compromised.

Where the subject knows for certain that the private key is compromised, a request for revocation of their certificate is sent to their TSP's TWS.

The TSP may also request a certificate status change via this service. Status of Control and Infrastructure certificates may also be controlled through this service. Requests for certificate status change are authenticated messages and may be accepted or rejected by the TSP.

Certificate Suspension/Revocation

The TWS having obtained a suspension or revocation request via this service, changes the certificate status to either Suspended or Revoked (Figure 1: message A) in its Certificate Status Database, and this in turn is used by the TSP's Revocation Status Service.

5.3.5.3 Security Requirements

5.3.5.3.1 RM1 Certificate Status Change Requests

[RM1.1]

Requests and reports relating to revocation and/or suspension SHALL be processed in a timely manner. The maximum TWS internal processing time between receipt of a revocation and/or suspension request and the change to certificate status information (update of Certificate Status Database) SHALL NOT exceed 60 minutes.

NOTE TWS internal processing time does not comprise the time to (manually) enter a request into the TWS.

[RM1.2]

All requests for suspension, reinstating and revocation SHALL be suitably authenticated and validated.

[RM1.3]

Once a certificate is revoked the TWS SHALL ensure that it cannot be reinstated.

NOTE This does not apply to suspended certificates.

[RM1.4]

Revocation of certificates related to TSP Signing Keys SHALL ONLY be possible under at least dual person control.

[RM1.5]

Status changes SHALL ONLY be instigated by authenticated and authorised users, in particular:

a) TSP Security Officers for Infrastructure/Control certificates;

b) Registration/Security Officers for certificates issued to subjects;

c) subjects for their own certificates.

As determined by certificate policy, a subject's certificate may be revoked/suspended/unsuspended by a third party (e.g. employer of a subject) by sending a suitable request to the TSP, for instigation of a status change.

5.3.5.3.2 RM2 Certificate Suspension/Revocation

A TSP is responsible for updating/providing the status of certificates on the Revocation Status Service (Figure 1: message B). TWSs may implement this using:

a) Periodical messaging: where periodical update messages (e.g. CRLs/ARLs) are sent from the Revocation Management System to the Revocation Status Service or;

b) Real-time messaging: where a request/response mechanism is used and a status request via the Revocation Status Service queries the Certificate Status Database and a status response is generated and passed back via the Revocation Status Service.

[RM2.1]

A TWS SHALL be able to revoke any certificate it has issued, even after a disaster.

[RM2.2]

Where periodical messaging is used, a TWS SHALL support the following requirements:

a) the Revocation Status Service SHALL be updated at least on a daily basis;

b) each update message SHALL include the name and digital signature of the message issuer, the signing time and the time of status change;

c) the message SHALL contain a unique identifier of the certificate which status is changed;

d) it is RECOMMENDED that for each certificate in the list, its serial number and a reason for the status change is provided in the message.

[RM2.3]

Where real-time messaging is used, a TWS SHALL meet the following requirements:

a) where the Revocation Status Service queries a certificate status, the Certificate Status database SHALL reply by providing the current status of that certificate;

b) a trusted channel (Figure 1: message B) SHALL exist between the Revocation Management Service and the Revocation Status Service;

c) this trusted channel SHALL be configured to minimize denial of service attacks on the messaging;

d) request and response messages SHALL be protected from replay attacks (e.g. by using nonces).

[RM2.4]

Periodical messaging and real-time messaging SHALL meet the requirements as stated in the current applicable legislation.

NOTE This area is known to be subject to change in the applicable legislation. See also the latest version of the ETSI EN 319 411 series.

5.3.5.3.3 RM3 Revocation Management Audit

[RM3.1]

The following Revocation Management Service specific events SHALL be logged:

- All events related to certificate status change requests, whether approved or rejected.

5.3.6 Certificate Revocation Status Service

5.3.6.1 Functionalities

Revocation Status Data

The Revocation Status Service provides certificate revocation status information to relying parties. The Revocation Status Service reflects changes to certificate status, based on status change requests either from the subject, from the TSP, or from a third party, and processed by the Revocation Management Service. This data may also be made available to subjects if certificate policy requires subjects to have access to revocation status data.

Status Request/Response

A relying party having obtained the certificate(s) from the Dissemination Service (or otherwise), required for signature verification, needs to check the status of these certificates. The TSP provides a Revocation Status Service for this purpose. Depending on the applicable certificate policy, this Revocation Status Service may be an ‘online’ or an ‘offline’ service.

Where this is an ‘online’ service, a relying party communicates with this Revocation Status Service and provides details of the certificate(s) for which status is required. The ‘online’ Revocation Status Service, when using real-time messaging, either makes a query to the Certificate Status database to retrieve the current status of the requested certificate or if using periodical messaging queries its internal records, which have been updated by the last periodical message. A signed response is thus created and sent to the relying party indicating the status (e.g. not revoked, revoked at date/time, certificate unknown) of the requested certificate(s) and the response time. If retrieval of the certificate is allowed and requested, the certificate may optionally be provided too.

Where this is an ‘offline’ service, the Revocation Status Service holds the most recent Periodic Message. This may be obtained by the relying party for checking certificate status.

5.3.6.2 Security Requirements

5.3.6.2.1 RS1 Revocation Status Data

[RS1.1]

Real-time or Periodic Messages provided to this service SHALL ONLY be from trusted Revocation Management Services.

[RS1.2]

TWS SHALL support real-time certificate status information, e.g. in form of OCSP-responses and MAY support periodical messaging additionally.

[RS1.3]

TWSs providing an 'online' Revocation Status Service SHALL validate the integrity and authenticity of real-time or periodic messages received from the Revocation Management Service.

[RS1.4]

TWSs providing an 'online' Revocation Status Service using real-time messaging SHALL ensure that replies to responses from the certificate status database are for the requested certificates. The response SHALL contain a unique ID of the certificate. The TWS MAY provide the certificate together with the response if the subject allowed certificate retrieval. (See Requirement [D1.1].)

5.3.6.2.2 RS2 Status Request/Response

TWSs may request that relying parties digitally sign certificate status requests. TWSs may optionally provide session confidentiality and integrity. Status requests may be generated by TWSs themselves to obtain the status of Certificate Signing, Infrastructure and Control Certificates.

[RS2.1]

All certificate status responses from an 'online' Revocation Status Service SHALL be digitally signed by the Revocation Status Service using its TSP Signing Keys.

An 'offline' Revocation Status Service may provide a response which is just the forwarding of the latest periodical message. This periodical message is signed by its issuer.

[RS2.2]

The signature algorithm used for status response SHALL be shall be one recognized as being fit for the purpose.

NOTE See ETSI/TS 119 312 for guidance on algorithms and their parameters.

[RS2.3]

The response message from an 'online' Revocation Status Service SHALL contain the time at which the Revocation Status Service/Issuer signed the response.

5.3.6.2.3 RS3 Certificate Revocation Status Audit

[RS3.1]

The following Certificate Revocation Status Service specific event SHALL be logged:

- all certificate status requests and responses.

5.4 Supplementary Services Security Requirements

5.4.1 Subject Device Provision Service

5.4.1.1 Functionalities

Subject Device Provision Service consisting of SCDev Preparation, SCDev Provision, and Activation Data Creation and Distribution is a customary but optional service for TSPs managing certificates.

a) SCDev Preparation:

The TSP's TWS prepares the SCDev by performing the necessary initialization, formatting and, if applicable, file structure creation.

The TWS either:

1) creates the private/public key pair and loads the private key into the SCDev, or;

2) if applicable, commands the SCDev to generate the key pair inside the SCDev.

b) SCDev Provision:

SCDev Provision is the distribution of the SCDev (after preparation) to the subject.

c) Activation Data Creation and Distribution:

The SCDev and its contents are protected with (secret) activation data. The TSP is responsible for generation of this initial activation data and subsequent secure distribution of this to the subject.

5.4.1.2 Security Requirements

5.4.1.2.1 SP1 SCDev Preparation

[SP1.1]

If the SCDev is procured from/provided by a third party, the TWS SHALL verify, before the SCDev is prepared, that the SCDev is a genuine SCDev from an approved manufacturer.

[SP1.2]

The initialization, formatting and file structure creation SHALL use secure values, parameters and access control conditions, leaving the SCDev in a secure configuration, which cannot be misused at any time.

[SP1.3]

Where a SCDev is a QSCD, it SHALL be evaluated and certified to the EN 419211 series or another suitable specification at a comparable assessment level that contains the requirements laid down in the Directive [Dir.1999/93/EC] or the Regulation [Reg.910/2014/EU].

NOTE Suitable specifications could be other Common Criteria [CC] Protection Profiles or Common Criteria Security Targets for QSCDs.

[SP1.4]

Where the key pair is generated outside the SCDev, the cryptographic device generating the key pairs SHALL be evaluated and certified to comply either with the EN 419211 series or the following requirements:

a) the cryptographic device SHALL ensure the confidentiality and integrity of the keys so long as they are under the control of the device;

b) the cryptographic device SHALL ensure the confidentially of private keys transferred from the device to a SCDev;

c) the cryptographic device SHALL ensure the integrity of public keys exported to other systems or applications;

d) the cryptographic device SHALL be able to identify and authenticate its users;

e) the cryptographic device SHALL restrict access to its services;

f) the cryptographic device SHALL be able to run a suite of tests to verify that it is operating correctly, and to enter a secure state when it detects an error;

g) the cryptographic device SHALL detect attempts of physical tampering and enter a secure state when a tampering attempt is detected.

When evaluated against the above list of requirement, the evaluation SHALL be performed against [CEN CMCKG-PP] or another suitable specification at a comparable assessment level.

NOTE Suitable specifications could be other Common Criteria [CC] Protection Profiles or Common Criteria Security Targets for cryptographic devices.

[SP1.5]

If the key pair is generated outside the SCDev, it SHALL be transferred to the SCDev in a secure manner. A trusted channel SHALL exist between the cryptographic device and the SCDev. This trusted channel SHALL provide source authentication, integrity and confidentiality using suitable cryptographic mechanisms.

NOTE The trusted channel between the cryptographic device and the SCDev will typically be initiated by a TWS component managing the cryptographic device and/or the SCDev.

[SP1.6]

After a cryptographic device generates a key pair for a SCDev and achieves successful transfer to that SCDev, the key pair SHALL be securely destroyed in the cryptographic device in conformance with Requirement [KM5.4].

5.4.1.2.2 SP2 SCDev Provision

[SP2.1]

If applicable, the TSP SHALL ensure, through appropriate TWS configuration, that the SCDev is distributed to the intended and authenticated subject.

5.4.1.2.3 SP3 Activation Data Creation and Distribution

[SP3.1]

The TWS SHALL generate the initial activation data in a secure manner.

[SP3.2]

TWSs SHALL ensure that the TSP's personnel cannot misuse the SCDev at any time.

This MAY be achieved either through:

a) security procedures during SCDev preparation and provision or;

b) by providing the subject the means by which they MAY verify that the private key has not been used before they have received the SCDev.

5.4.1.2.4 SP4 Subject Device Provision Service Audit

[SP4.1]

TWSs SHALL log all security related events relating to SCDev preparation.

5.5 Core Services Security Requirements for TWS managing electronic time-stamps

5.5.1 Time-Stamping Service

5.5.1.1 General

A time-stamping authority (TSA) is a third party trusted to provide time-stamping services, i.e. generate time-stamp tokens, which can serve as evidence that a data item existed before a certain point in time (proof of existence).

The time-stamping service within this specification provides only a time-stamping process, which cryptographically binds time values to data values.

Figure 2 illustrates the TSA's functions and therefore is referred to within this section.

5.5.1.2 Functionalities

— Check Request Correctness:

This component is designed to check the correctness and the completeness of the request. If the result is positive, the data item is sent as input to the Time-Stamp Token Generation.

— Time Parameter Generation:

This component uses a reliable source to deliver accurate time parameters. These parameters are used as input in the time-stamp generation process.

— Time-Stamp Token Generation:

This function is responsible for creating a time-stamp by binding the current time, a unique serial, the data provided for time-stamping and ensuring any policy requirements are adhered to.

— Time-Stamp Token Computation

This component computes the time-stamp token that is returned to the client. It effectively cryptographically signs the data provided by the Time-Stamp Token Generation function.

5.5.1.3 Security Requirements

5.5.1.3.1 TS1 Request Correctness

[TS1.1]

The TSA MAY control the origin of each request before checking its correctness. A solution to perform such a control could be to make use of a data origin authentication mechanism.

[TS1.2]

The TSA SHALL verify that the request for time-stamping uses a hash algorithm that is recognized as being fit for the purpose.

NOTE See ETSI/TS 119 312 for guidance on algorithms and their parameters.

5.5.1.3.2 TS2 Time Parameter Generation

[TS2.1]

The TSA's trusted time source(s) SHALL be synchronized to Coordinated Universal Time (UTC) within the tolerance dictated by TSA policy e.g. to within 1 s. This MAY be the same source as specified in requirement SO3.

[TS2.2]

The TSA's trusted time source(s) SHALL be synchronized with UTC using a mechanism that is demonstrated to be reliable.

[TS2.3]

The TWS SHALL detect missing synchronization with UTC and not issue any time-stamp tokens if the time deviation is outside the defined tolerance.

5.5.1.3.3 TS3 Time-Stamp Token (TST) Generation

[TS3.1]

The serial number used within the TST SHALL be unique for each TST issued by a given TSA. This property SHALL be preserved even after a possible interruption (e.g. crash) of the service.

[TS3.2]

As well as time parameter inclusion, the TST SHALL include the accuracy of the time source used if this is required by the TSA policy.

This MAY be by way of a pointer to relevant policy documentation.

[TS3.3]

An indication of the policy under which the TST was created SHALL be included. The details of the policy provisions are outside the scope of this document but MAY indicate conditions under which the TST MAY be used.

[TS3.4]

All TST SHALL be digitally signed by the Time-Stamping Service using its TST Signing Keys.

5.5.1.3.4 TS4 Time-Stamp Token (TST) Computation

In addition to the requirements stated in 5.2.5, the following security requirements are applicable and in some cases supersede the requirements specified in 5.2.5.

The TST computation may include the TSA's certificate and any associated certificate status information; although it is RECOMMENDED that the relying party make use of the Revocation Status Service of the CA that has issued the TSA's certificate for certificate status information.

[TS4.1]

TST Signing Keys SHALL be generated and stored in a cryptographic device that fulfils the requirements of [KM1.2].

[TS4.2]

Control Keys SHALL be stored in a cryptographic device that fulfils the requirements of [KM1.4].

[TS4.3]

The TST Signing Key SHALL ONLY be used for signing TSTs produced by the TSA.

[TS4.4]

The TSA SHALL ensure that the TST response contains the same datum that was sent with the request.

[TS4.5]

The signature algorithms/keys used by the TSA, if applicable, SHALL be recognized as being fit for the purpose.

NOTE See ETSI/TS 119 312 for guidance on algorithms and their parameters.

5.5.1.3.5 TS5 Time-Stamping Service Audit

[TS5.1]

The following Time-Stamping Service specific events SHALL be logged:

- all events relating to TSA Certificate re-key/renewal requests;
- all events relating to the life-cycle management of the TST Signing Key;
- all failures (including time drift outside of allowed tolerance) associated with the trusted time sources.

5.5.1.3.6 TS6 Time-Stamping Service Archiving

[TS6.1]

All Time-Stamp Tokens SHALL be archived in accordance with Requirement [AR1.1].

Annex A
(informative)

Physical security requirements for the operational environment

A.1 General

The following (non-IT) physical security requirements for the operational environment of the TWS are necessary to protect TWS against unauthorized access and to provide the infrastructure for the availability of services in terms of power, air conditioning, and fire protection. They do not constitute requirements on TWS itself but on its operational environment at the TSP site. They solely need to be fulfilled when operating the TWS at the TSP's site.

NOTE This annex is informative. See ETSI EN 319 401 and the ETSI EN 319 411 series for normative requirements on physical security.

Requirements:

a) P1 Intrusion Resistant Security Perimeter;

b) P2 Access Control System;

c) P3 Intrusion Alarm System

focus on protection against unauthorized access and apply to all TSP services while requirements:

d) P4 Fire Protection and Prevention;

e) P5 Power Supply;

f) P6 Air Conditioning and Ventilation

focus specifically on service availability and apply to TSP services indicated in [SO2.1] (dissemination, revocation management and revocation status service).

A.2 P1 Intrusion Resistant Security Perimeter

[P1.1]

The security perimeter composed of the rooms where the TWS components are located and the rooms with relevant technical equipment SHOULD be outside of streams of visitors, persons and material. No indications to the security perimeter SHOULD exist. This requirement does not apply to rooms dedicated for customer contacts in the context of the registration service.

[P1.2]

Walls, roofs and floors of the security perimeter SHOULD be of solid construction to provide protection against fire, gas and intrusion.

[P1.3]

Limiting walls, doors, windows and shutters of the security perimeter SHOULD be resistant against breakthrough to at least level RC2 according to EN 1627 or equivalent. Ducts, risers and outer openings SHALL be protected against sabotage, equivalently.

A formal certification of limiting walls, doors, windows and shutters against level RC2 of EN 1627 is not required. Equivalence to resistance class may be obtained by the combination of means.

[P1.4]

Smoke proof doors SHOULD be deployed to protect the security perimeter against damage resulting from corrosive outside smoke.

A.3 P2 Access Control System

[P2.1]

An access control system SHOULD be in place to control access to the security perimeter. The central unit managing the access control system SHOULD be located inside the security perimeter and protected by an intrusion alarm system.

[P2.2]

The access control system for the security perimeter including cabling and readers SHOULD be protected against sabotage. Sabotage detection SHOULD be handled as an alarm and indicated to a permanently occupied control centre.

[P2.3]

The operation of the access control system for the security perimeter SHOULD be unaffected from external power failures of up to 24 h.

[P2.4]

The access control system for the security perimeter SHOULD use a strong 2-factor authentication mechanism, e.g. possession and knowledge or possession and biometry.

NOTE Another 2-factor mechanism could be a security team that controls access plus and an access token.

[P2.5]

The access control system for the security perimeter SHOULD implement a zone concept.

[P2.6]

The access control system for the security perimeter SHOULD implement an anti-pass-back mechanism where adequate.

[P2.7]

The access control system for the security perimeter SHOULD log every access attempt with the person's identity requiring access, date and time. It SHOULD store log entries for at least 30 days. The retention period SHOULD respect applicable laws and privacy regulations.

[P2.8]

The access control system for the security perimeter SHOULD provide the capability to search access attempts in the log based on date and time of access attempt, and/or person's identity requiring access. The results SHOULD be presented in a format suitable to interpret the information.

[P2.9]

The access control system for the security perimeter SHOULD support door opening time monitoring and alarming if selected doors are open for more than a defined period of time, e.g. one minute.

A.4 P3 Intrusion Alarm System

[P3.1]

An intrusion alarm system SHOULD be in place to monitor the security perimeter. The central unit managing the intrusion alarm system SHOULD be located inside the security perimeter and protected by this system.

[P3.2]

The intrusion alarm system including cabling, sensors and readers SHOULD be protected against sabotage in armed and unarmed state. Alarms SHOULD be indicated to a permanently occupied control centre.

[P3.3]

The operation of the intrusion alarm system SHOULD be unaffected from external power failures of up to 24 h.

[P3.4]

The intrusion alarm system SHOULD use a strong 2-factor authentication mechanism, e.g. possession and knowledge or possession and biometry, for disarming the alarm.

NOTE Another 2-factor mechanism could be a security team that controls access plus and an access token.

A.5 P4 Fire Protection and Prevention

[P4.1]

A fire alarm system SHOULD be in place to monitor the security perimeter. A “Very Early Smoke Detection System” SHOULD monitor power carrying cabling and IT hardware.

[P4.2]

Alarms of fire alarm system SHOULD be indicated to a permanently occupied control centre.

[P4.3]

The operation of the fire alarm system SHOULD be unaffected from external power failures of up to 24 h.

[P4.4]

The type and number of fire detectors installed in every room of the security perimeter SHOULD be appropriate for early fire detection. It is RECOMMENDED that the area per fire detector does not exceed 25 m^2 and at least 2 detectors are installed in every room.

[P4.5]

A fire extinguishing system SHOULD be in place to protect the security perimeter. It is RECOMMENDED that the fire extinguishing system automatically extinguishes fires if detected by two detectors simultaneously.

[P4.6]

In supplement to the fire extinguishing system, CO_2 hand-held fire extinguishers SHOULD be in place for early human fire fighting and damage limiting.

A.6 P5 Power Supply

[P5.1]

Two independent power supply paths SHOULD exist to support redundant power supplies. Each path SHALL be able to fully power the IT systems by itself.

[P5.2]

A central Uninterruptable Power Supply (UPS) SHOULD exist and SHOULD be located in a dedicated room and/or fire zone. Batteries and UPS SHOULD be located in separate fire zones.

[P5.3]

The UPS SHOULD be equipped with an external bypass that SHOULD be located in a separate fire zone.

NOTE The bypass will typically be used to avoid downtime in case of maintenance and in case of a fire in the UPS room.

[P5.4]

A power generator SHOULD exist that is able to deliver necessary power to the security perimeter for at least 24 h in case of external power failure.

A.7 P6 Air Conditioning and Ventilation

[P6.1]

The air conditioning and ventilation system cooling capacity SHOULD be sufficient for the operational needs of the TWS located in the security perimeter. The installation of the air conditioning and ventilation system SHOULD support maintenance and exchange that allows continuous TWS operation.

[P6.2]

Temperature and humidity of the security perimeter SHOULD be monitored and controlled to ensure appropriate operational conditions.

[P6.3]

A redundant layout of the air conditioning and ventilation system SHOULD be realized.

[P6.4]

The air conditioning and ventilation system SHOULD be protected against sabotage.

NOTE This applies particularly to air conditioning and ventilation system components located outside the security perimeter, e.g. heat exchangers.

[P6.5]

Air conditioning and ventilation system failures SHOULD be handled as an alarm and indicated to a permanently occupied control centre.

[P6.6]

Air inlets of the air conditioning and ventilation system SHOULD be equipped with smoke detectors and SHOULD be closed in case of smoke detection.

Annex B
(informative)

Network Security Requirements for the Operational Environment

B.1 General

The following (IT) network security requirements for the operational environment of the TWS are necessary to protect TWS against unauthorized access and to provide the infrastructure for the availability of TSP services in terms of network connectivity. They do not constitute requirements on TWS providing the TSP services itself but on dedicated TSP IT network systems in the operational environment of the TWS that protect them at the location of the TSP. They solely need to be fulfilled when operating the TWS at the TSP's site.

NOTE 1 This annex is informative. See ETSI EN 319 401 and See ETSI EN 319 411 for normative requirements on network security.

NOTE 2 Additional detailed network and certificate system security requirements relevant for publicly trusted CAs can be found in the document [CA/B-NetSec].

B.2 NET1 Protected TWS Architecture

[NET1.1]

The network SHOULD be configured in such a way that only connections/communications needed for the operation of the TWS are allowed. Not needed connections and services SHOULD be explicitly forbidden or deactivated. The established rule set SHOULD be reviewed on a regular basis.

[NET1.2]

The network SHOULD be suitably segmented in at least two security zones with increasing level of protection to isolate and limit exposures of TWS from other non-TSP systems. In one zone only TWS with similar security requirements SHOULD be operated. The segmentation SHOULD be based on the assumed risks and the logical and functional relationship between the TWS. Zones with higher security level SHOULD NOT be directly accessible from non-TSP systems. Credentials to authenticate administrators in a high security zone SHOULD not be valid in the zone with the lowest security level.

[NET1.3]

A dedicated network for administration of TWS that is separated from the operational network SHOULD be established. Systems used for administration SHOULD NOT be used for non-administrative purposes.

[NET1.4]

Communication between distinct TWS components SHOULD only be established through trusted channels that are logically distinct from other communication channels and provide ensured identification of its end points and protection of the channel data from modification or disclosure.

[NET1.5]

The (external) network connection to the internet SHOULD be redundant to ensure availability of the services in case of a single failure. This MAY be achieved by two different network connections to one of more internet providers.

B.3 NET2 Logging

[NET2.1]

The TSP IT network systems SHOULD be able to generate network activity related logging data for the following events:

a) access to the TSP network from non-TSP systems;

b) modification of access rights and/or security controls;

c) successful and unsuccessful authentication attempts to TWSs and underlying operating systems.

[NET2.2]

The TSP IT network systems SHOULD record within each logging data record at least the following information:

- date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event.

[NET2.3]

All logging data SHOULD be stored together in such a way that allows a common analysis of all events. The storage area SHOULD be physically separated from the TSP IT network systems producing the logging data and protected in such a way that the integrity of logging data are ensured and deletion is either prevented (e.g. using WORM media) or solely possible under at least dual person control. Administrative access to the central log data SHOULD only be granted through a dedicated account that is not used elsewhere.

[NET2.4]

The TWS SHOULD provide System Auditors with the capability to read logging data in a manner suitable to interpret the information.

B.4 NET3 Monitoring and Alerting

[NET3.1]

The TSP IT network systems SHOULD be able to monitor network system activities concerning each TWS, user of TWS and request for registration, certificate generation, dissemination, revocation, revocation status and time-stamping.

NOTE 1 Monitoring user accounts includes privileged users (i.e. administrators, and user associated to a privileged role defined in [M1.2]), too.

NOTE 2 Monitoring network system activities does not require analysing traffic contents that might be encrypted.

[NET3.2]

The TSP IT network systems SHOULD be able to detect abnormal network system activities that indicate a potential security violation and report them as alarms.

NOTE Abnormal network system activities could comprise (external) network scans or packet drops.

[NET3.3]

The TSP IT network systems SHOULD be able to monitor the following events:

a) start-up and shutdown of the logging functions;

b) availability and utilization of needed services with the TSP network.

Bibliography

[1] *CA / Browser Forum Network and Certificate System Security Requirements, version 1.0* [CA/B-NetSec]

[2] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, CCMB-2012-09-001, September 2012* [CC]

[3] *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 4, CCMB-2012-09-002, September 2012*

[4] *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 4, CCMB-2012-09-003, September 2012*

[5] *EESSI Conformity Assessment Guidance - Part 3: Trustworthy Systems Managing Certificates for Electronic Signatures* [CWA 14172-3]

[6] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures* [Dir.1999/93/EC]

[7] EN 1627, *Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Requirements and classification*

[8] ETSI/TS 119 312, *Electronic Signatures and Infrastructures (ESI); Cryptographic Suites*

[9] ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[10] ISO/IEC 9594-8:2014, *Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks*

[11] ISO/IEC 9798-1:2010, *Information technology — Security techniques — Entity authentication — Part 1: General*

[12] ISO/IEC 10118-1:2000, *Information technology — Security techniques — Hash-functions — Part 1: General*

[13] ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

[14] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [Reg.910/2014/EU]

[15] RFC 3647:2014, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC 3647]

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

[17] EN 419221-2, *Cryptographic Module for TSP Signing Operations — Protection Profile — CMCSO-PP*

[18] EN 419221-3, *Cryptographic Module for TSP Key Generation Services — Protection Profile — CMCKG-PP*

[19] ETSI EN 319 401, *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™