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

# WORKSHOP AGREEMENT

**CWA 14167-1**

November 2001

ICS 03.120.20; 35.040

## Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements



**Ref. No CWA 14167-1:2001 E**

Rue de Stassart, 36 • B-1050 Bruxelles
Tel : +32 2 550 08 11 • Fax : +32 2 550 08 19

# Contents

page

# Foreword

Successful implementation of the European Directive 1999/93/EC on a Community framework for electronic signatures 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. Therefore, the European ICT Standards Board, with the support of the European Commission, undertook an initiative bringing together industry and public authorities, experts and other market players: the European Electronic Signature Standardisation Initiative (EESSI).

In July 1999, EESSI delivered its initial recommendations in the EESSI Expert Report. The report contained an overview of the requirements for standards-related activities, as well as a work programme to meet these requirements. A work repartition was drawn up, allocating between CEN/ISSS and ETSI the standardisation activities. The work was carried out by CEN/ISSS in the E-Sign project and by ETSI SEC in the ESI WG. The results are documented in a series of CEN Workshop Agreements (CWA) and ETSI standards.

The production of this CEN Workshop Agreement (CWA) was formally agreed at the Kick-Off meeting of the CEN/ISSS Electronic Signatures Workshop (WS/E-SIGN) on 16-17 December 1999, in response to the initial work plan of the European Electronic Signature Standardization Initiative (EESSI). Later, during the execution of the work, the requirement for a Protection Profile became clear, which activity was formally accepted as part of the Workshop's business plan at the meeting of 7 February 2001.

This CWA has been developed through the collaboration of a number of contributing partners in the E-SIGN Workshop, gathering a wide mix of interests, representing different sectors of industry (manufacturers, end-users, service providers, legal experts, academia, accreditation bodies, standardization organisations and national standards bodies) as well as representatives of the national public and European authorities.

The present CWA has received the support of representatives of these sectors. A list of company experts who have supported the document's contents may be obtained from the CEN/ISSS Secretariat.

The final review/endorsement round for this CWA-part was started on 2001-08-01 and was successfully closed on 2001-08-24. The final text of this CWA-part was submitted to CEN for publication on 2001-10-19.

This CWA on "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures" is currently composed of two parts:

- Part 1: System Security Requirements
- Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)

The CEN/ISSS Electronic Signatures Workshop may develop further parts to this as part of its ongoing work programme.

# Executive summary

This CEN Workshop Agreement (CWA) specifies security requirements on products and technology components, used by Certification Service Providers (CSPs), to create Qualified and Non-Qualified Certificates. These certificates are used in conjunction with electronic signatures and advanced electronic signatures in accordance with the *"Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures" [EC 1999/93].*

This CWA is specifically relevant for manufacturers of Trustworthy Systems (TWSs) used for managing certificates, but may be adopted by anyone deploying systems and wanting to meet the requirements of [EC 1999/93]. It provides an overview of a CSP system broken down into a number of services. These services provide a number of functions. Some of these services provide mandatory functionality, termed 'Core Functionality' whereas others are optional services and provide 'Supplementary Functionality'. A CSP must implement systems that provide all Core Functionality and if they provide optional services, they must meet all Supplementary Functionality requirements. This functionality is provided by the TWSs adopted by the CSP, whose security requirements are specified in this CWA.

To provide a baseline of generic security, some general security requirements are initially specified. These are mandatory and are applicable to all services. Furthermore specific minimum security requirements relating either directly to Core Functionality or directly to Supplementary Functionality are provided.

Core Functionality covers the following CSP services:

- Registration Service - to verify the identity and, if applicable, any specific attributes of a Subscriber
- Certificate Generation Service - to create certificates.
- Dissemination Service - to provide certificates and policy information to Subscribers and Relying Parties.
- Revocation Management Service - to allow the processing of revocation requests
- Revocation Status Service - to provide certificate revocation status information to relying parties

Supplementary Functionality covers two optional CSP services:

- Subscriber Device Provision Service – to prepare and provide a Signature Creation Device (SCD) to Subscribers. This includes Secure-Signature-Creation Device (SSCD) provision.
- Time Stamp Service – provides a CSP Time Stamp Service which may be needed for signature verification purposes.

This specification provides standards for Trustworthy Systems (TWSs) providing core and supplementary functionality, issuing both Qualified Certificates (QCs) and Non-Qualified Certificates (NQCs). Issuing of QCs automatically translates to the TWS meeting the requirements for issuing NQCs.

Manufacturers of TWSs are required to produce systems that provide the required functionality meeting the security requirements specified in this CWA. Once compliance has been proved[1], a CSP may use these approved TWSs thus ensuring they meet the requirements of the [EC 1999/93].

A CSP may adopt specific policy when managing Qualified Certificates (e.g. by adopting *Policy Requirements for Certification Authorities Issuing Qualified Certificates [TS101456]* ). Where this is the case, the easiest way to meet the policy requirements would be to use approved TWSs that have shown conformance to this CWA. An informational appendix is provided to help determine which requirements of [TS101456] are automatically covered when a CSP adopts TWSs conformant to this CWA. This appendix also provides a generic table of CSP functionality against this CWA for helping to relate this CWA to other/national policy requirements.

[1] The last section of this document provides some guidance for compliance and specifies conformance requirements for this CWA

# Introduction

The European Directive [EC 1999/93] establishes a framework of requirements for the use of electronic signatures which are legally equivalent to hand-written signatures. It introduces the notion of “advanced electronic signatures” which can be verified using “Qualified Certificates”.

Annex II of [EC 1999/93] provides the requirements for a Certificate Service Provider (CSP) issuing Qualified Certificates (QCs). This CWA principally concentrates on providing all the technical security requirements for the Trustworthy Systems (TWSs) a CSP needs to deploy. Specifically according to Annex II (f) of [EC 1999/93], CSPs must:

*“(f) use trustworthy systems and products which are protected against modification and which must ensure the technical and cryptographic security of the processes supported by them“*

Non-Qualified Certificates (NQCs) used for Electronic Signatures effectively require less security provisions when compared to QCs and therefore this CWA caters for both and indicates the areas where differentiation is required.

This document establishes the required functionality for CSPs to perform their task and then formulates general security requirements and assumptions. It is assumed that conformant TWSs to this CWA may be adopted by CSPs to reduce their effort in deploying systems meeting [EC 1999/93]. This procedure should enable maximum flexibility for industry in developing such systems which meet the security requirements laid down in Annex II of the EU Directive.

For defining the requirements in this document, *Policy Requirements for Certification Authorities Issuing Qualified Certificates [TS101456]* has been taken into account as an informative reference. This means that a CSP using TWSs conformant to this CWA will require minimal configuration to meet the system (policy) requirements of [TS101456]. The diagram below illustrates the relationship:

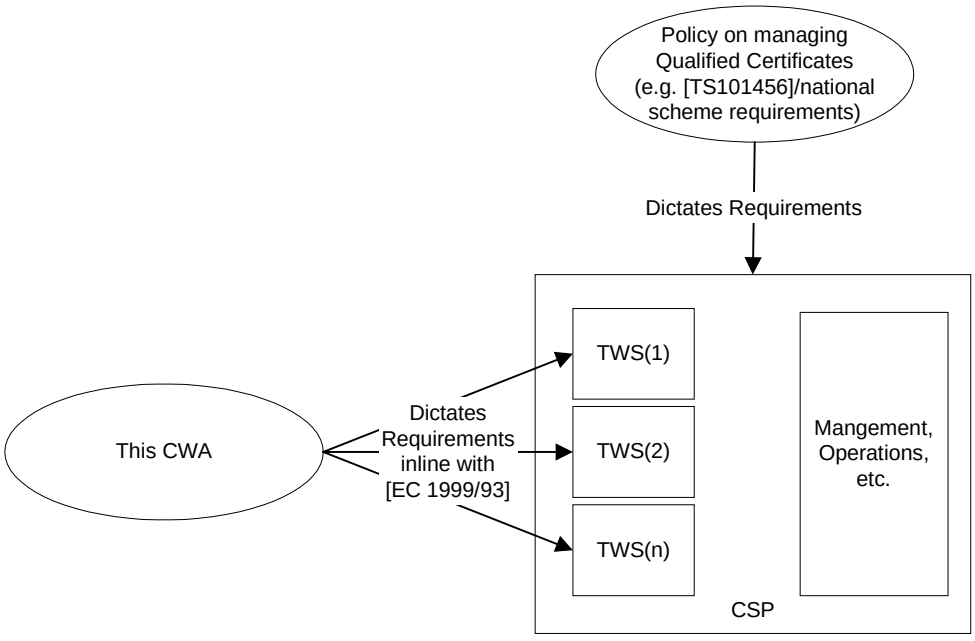


**Figure 1 - Relationship between Policy and this CWA**

To further assist in assessing CSPs using TWSs compliant to this CWA, an informative appendix (Appendix A) is provided in this CWA. The tables in this appendix allow [TS101456] and/or generic policy requirements to be compared against this CWA’s security requirements.

TWSs addressed by this CWA provide the following mandatory CSP services:

- Registration of subscriber information (Registration Service)
- Certificate generation (Certificate Generation Service)
- Certificate dissemination (Certificate Dissemination Service)
- Certificate revocation management (Revocation Management Service)
- Certificate revocation status provision (Revocation Status Service)

Furthermore, they may provide the following optional CSP services:

- Time stamping functions (Time Stamping Service)
- Signature-Creation/Secure-Signature-Creation Device production (Subscriber Device Provision Service)

Note: where a CSP is offering optional services in addition to the mandatory services, they must adopt the security requirements specified in this CWA for these optional services.

All security requirements of this CWA are clearly stated and may be:

- mandatory (indicated by MUST (NOT) or SHALL (NOT))
- optional (indicated by SHOULD (NOT) or (NOT) RECOMMENDED)
- permitted (MAY or MAY (NOT))

# 1 Scope

## 1.1 General

This document establishes security requirements for TWSs and technical components that can be used by a CSP in order to issue QCs and NQCs in accordance with [EC 1999/93].

Although [EC 1999/93] has a very general approach and speaks of electronic signatures of any kind, the underlying assumption in this document is that electronic signatures are created by means of public key cryptography, that the subscriber uses a cryptographic key pair consisting of a private and public component, and that a certificate produced by a system considered in this document essentially binds the public key of the subscriber to the identity and possibly other information of the subscriber by means of an electronic signature which is created with the private key (certificate signing key) of the CSP. Other forms of electronic signatures are outside the scope of this document.

With reference to Electronic Signatures, [EC 1999/93] provides two levels of signature, one a standard Electronic Signature and the other an Advanced Electronic Signature. Within this CWA, these are used in conjunction with NQCs and QCs respectively. This CWA provides security requirements for both these levels where the security requirements for TWSs issuing QCs are higher than for those just issuing NQCs.

Security requirements for TWSs also include a minimum set of requirements to be fulfilled by the signature algorithms and their parameters allowed for use by CSPs. These requirements are provided in [ALGO].

Although security requirements for the optional Subscriber Device Provision Service, which provides SCD/SSCD provision to Subscribers is included within the scope of this CWA, requirements of the actual SSCD devices themselves, as used by Subscribers of the CSP, are outside the scope of this document. Security requirements for SSCDs are provided in the separate document *Secure Signature Creation Devices [CENSSCD]* as part of this series of CWAs.

Following the principles of [EC 1999/93] this CWA is as technology neutral as possible. It does not require or define any particular communication protocol or format for electronic signatures, certificates, certificate revocation lists, certificate status information and time stamps. It only assumes certain types of information to be present in the certificates in accordance with Annex I of the European Directive. Interoperability between CSP systems and subscriber systems is outside the scope of this document.

This document is also applicable for bodies established in member states for voluntary accreditation of CSPs, as outlined in [EC 1999/93]. Use of TWSs conformant to QC requirements in this CWA indicates that the technology used by the CSP is capable of fulfilling Annex I and Annex II requirements of [EC 1999/93]. Details of how compliance of this CWA is reached are specified in section 6. By using TWSs that are compliant with this CWA, CSPs may reduce their auditing burden by leveraging these assessed components and only auditing the operating aspects of the TWSs.

## 1.2 European Directive Specific

The main focus of this CWA is on [EC 1999/93] Annex II (f) requirement, but in considering this it is important to additionally encompass the following [EC 1999/93] requirements:

1. Annex II (a) - demonstrate the reliability necessary for providing certification services
2. Annex II (b) - ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
3. Annex II (c) - ensure that the date and time when a certificate is issued or revoked can be determined precisely;
4. Annex II (g) - take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

5. Annex II (i) - record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

6. Annex II (j) - not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;

7. Annex II (l)- use trustworthy systems to store certificates in a verifiable form so that:

   - only authorised persons can make entries and changes,
   - information can be checked for authenticity,
   - certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
   - any technical changes compromising these security requirements are apparent to the operator.

8. Annex I - requirements on the data in a Qualified Certificate

# 2 References

## 2.1 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this CWA. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this CWA are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies.

| | |
|---|---|
| [CEN HSM-PP] | CEN Hardware Security Modules for CSPs, CC Protection Profile, EESSI Area D2 |
| [ALGO] | Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive. |
| [FIPS140-1] | Security Requirements For Cryptographic Modules, Federal Information Processing Standards Publication 140-1, 1994 January 11 |

## 2.2 Informative references

| | |
|---|---|
| [TS101456] | ETSI TS 101 456, Policy Requirements for Certification Authorities Issuing Qualified Certificates |
| [EC 1999/93] | Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures |
| [CENSSCD] | CEN/ISSS WS/E-Sign Workshop Agreement Group F, Security Requirements of Secure Signature Creation Devices (SSCD) |
| [RFC 2459] | RFC2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profiles, Housley et al. |
| [RFC 2510] | Internet X.509 Public Key Infrastructure Certificate Management Protocols, . Adams, S. Farrell, March 1999 |
| [ISO/IEC 9594-8] | Information technology - Open Systems Interconnection - The Directory: Authentication Framework, Recommendation X.509, ISO/IEC 9594-8 |
| [RFC 2527] | RFC2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Chokhani and Ford, March 1999 |
| [ISO/IEC 9798-1] | Information technology - Security techniques - Entity authentication - Part 1: General |
| [ISO/IEC 10118-1] | ISO/IEC 10118-1:1994 Information technology -- Security techniques -- Hash-functions -- Part 1: General |
| [ISO 7498-2: 1989] | Framework for Support of Distributed Applications - The OSI Security Architecture (ISO 7498-2) |
| [ETSI TS 101 862] | Qualified Certificate Profile, DTS/SEC-004003 (see also RFC3039, Internet X.509 Public Key Infrastructure Qualified Certificates Profile, Santesson, et al.) |
| [CC] | Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408-1:1999, ISO/IEC 15408-2:1999, ISO/IEC 15408-3:1999 |
| [TSP] | Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP), <draft-ietf-pkix-time-stamp-14.txt> Adams, Cain, Pinkas, Zuccherato |

# 3 Definitions and abbreviations

## 3.1 Definitions

### Definitions from [EC 1999/93]:

**electronic signature**: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication of that data. [EC 1999/93]

**advanced electronic signature**: an 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 maintain under his sole control; and
d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable; [EC 1999/93]

**signatory**: a person who holds signature-creation data and acts either on his own behalf or on behalf of the natural or legal person or entity he represents; Note: the term signer is sometimes used as a synonym. [EC 1999/93]

**signature-creation data**: unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature; [EC 1999/93]

**signature-creation device**: configured software or hardware used to implement the signature-creation data. [EC 1999/93]

**secure-signature-creation device**: a signature-creation device which meets the requirements laid down in Annex III of the Directive; [EC 1999/93]

**signature-verification-data**: data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature; [EC 1999/93]

**signature-verification device**: configured software or hardware used to implement the signature-verification-data; [EC 1999/93]

**certificate:** an electronic attestation which links signature-verification data to a person and confirms the identity of that person; [EC 1999/93]

**qualified certificate:** a certificate which meets the requirements laid down in Annex I of the Directive and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II of the Directive; [EC 1999/93]

**certification-service-provider**: an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures; [EC 1999/93]

**electronic-signature-product**: hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures; [EC 1999/93]

**voluntary accreditation**: any permission setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body. [EC 1999/93]

**Note**: The term "accreditation" is generally used in another way, meaning "accreditation of certification bodies performing conformity assessment of products and/or services".

**trustworthy system:** An 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.

### Useful X.509 and RFC 2459 definitions:

**certificate:** The public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it. [ISO/IEC 9594-8; ITU-T X.509]

**CA-certificate**: A certificate for one CA issued by another CA. [ISO/IEC 9594-8; ITU-T X.509]

**self-signed certificate:** A certificate for one CA signed by that CA. [RFC 2459]

**certificate policy***:* A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. [ISO/IEC 9594-8; ITU-T X.509]

**certification authority (CA)**: An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys. [ISO/IEC 9594-8; ITU-T X.509]

**certification path**: A chain of multiple certificates, comprising a certificate of the public key owner (the end entity) signed by one CA, and zero or more additional certificates of CAs signed by other CAs. [RFC 2459]

**certificate validity period:** The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. [RFC 2459]

**CRL distribution point***:* A directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs. [ISO/IEC 9594-8; ITU-T X.509]

**end entity**: A certificate subject which uses its public key for purposes other than signing certificates. [ISO/IEC 9594-8; ITU-T X.509]

**relying party:** A user or agent that relies on the data in a certificate in making decisions. [RFC 2459]

**security policy**: The set of rules laid down by the security authority governing the use and provision of security services and facilities. [ISO/IEC 9594-8; ITU-T X.509]

### Useful definitions from RFC 2527

**Activation data**: Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share). [RFC 2527]

**Certification Practice Statement:** A statement of the practices that a Certification Authority employs in issuing certificates. [RFC 2527]

**Registration authority (RA):** An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). [RFC 2527]

**Policy qualifier**: Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate. [RFC 2527]

### Useful definitions from ISO

**public key**: That key of an entity's asymmetric key pair which can be made public. [ISO/IEC 9798-1]

**private key: T**hat key of an entity's asymmetric key pair which should only be used by that entity [ISO/IEC 9798-1]

**Hash function:** A function which maps string of bits to fixed-length strings of bits, satisfying the following two properties:

- It is computationally infeasible to find for a given output an input which maps to this output
- It is computationally infeasible to find for a given input a second input which maps to the same output

[ISO/IEC 10118-1]

**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. [ISO 7498-2: 1989]

### Additional definitions from EESSI final report and ETSI's [TS101456]:

**Qualified electronic signature**; an advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device (Note: Definition of 5.1 signature taken from the Directive)

**Subscriber:** An entity subscribing with a CSP to have its public key and identity certified in a public key certificate.

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

**Certificate Generation Service:** A service that creates and sign certificates based on the identity and other attributes verified by the registration service.

**Certificate Dissemination Service:** A service that disseminates certificates to Subscribers, and if the subscriber consents, to Relying Parties. This service also disseminates the CA's policy & practice information to Subscribers and Relying Parties.

**Revocation Management Service:** A service that processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the Revocation Status Service.

**Revocation Status Service:** A service that 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.

**Subscriber Device Provision Service:** A service that prepares and provides a Signature Creation Device to Subscribers.

**Time Stamping Service:** A service that provides a trusted association between a datum and a particular point in time, in order to establish reliable evidence indicating the time at which the datum existed.

## 3.2 Abbreviations

| | |
|---|---|
| ARL | Authority Revocation List |
| CA | Certification Authority |
| CP | Certificate Policy |
| CRL | Certificate Revocation List |
| CSP | Certification Service Provider |
| HW | Hardware |
| I/O | Input/Output |

| | |
|---|---|
| NQC | Non-Qualified Certificate |
| OCSP | Online Certificate Status Protocol |
| OS | Operating System |
| PKI | Public Key Infrastructure |
| POP | Proof of Possession |
| PP | Protection Profile |
| QC | Qualified Certificate |
| RA | Registration Authority |
| SCD | Signature-Creation Device |
| SF | Security Function |
| SSCD | Secure-Signature-Creation Device |
| TSA | Time Stamping Authority |
| TSS | Time Stamping Service |
| TWS | Trustworthy System |

# 4 Description of a Certification Service Provider System

A Certification Service Provider (CSP), within this specification, provides and manages certificates used for the support of electronic signatures. It is a primary assumption that a CSP will use a Public Key Infrastructure (PKI) for the management of certificates. The adopted approach of this specification is for a CSP 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 CSP's TWSs may consist of a number of subsystems each providing specific CSP functionality. Although this specification considers security requirements of the subsystems involved in the CSP's service, the aim is to provide the Subscriber and Relying Party a single view of the CSP and hence a single view of the TWSs employed by it. To ensure this, the customer interface, in this specification, is to the 'CSP Service' and not directly to the individual services offered by the CSP. As subsystems are further decomposed, any functionality, defined by other acceptable standards has been referenced.

The CSP provides mandatory services by deploying TWSs with Core Functionality and provides optional services by deploying TWSs with Supplementary Functionality. All CSPs MUST implement Core Functionality to meet the requirements of [EC 1999/93]. A CSP can choose to implement any Supplementary Functionality as deemed necessary by national, business and market requirements. However, if a CSP implements an optional service, in addition to the mandatory services, the CSP MUST implement the security requirements specified in this document for that service.

TWSs issuing and managing certificates are required to have some generic security functionality ('General Security Requirements' §5.1) as well as specific security functionality related to their defined function ('Core Functionality Security Requirements' §5.2) and 'Supplementary Functionality Security Requirements' §5.3'). In effect a CSP MUST deploy TWSs meeting General and Core Security Requirements. It is important to note that this technical/security integration does not necessarily impede on the freedom of the CSP to run the different components of the service using different business entities.

A CSP when choosing TWSs for issuing NQCs/QCs MUST ensure they are conformant to this specification (see Conformance Requirements §6).

## 4.1 CSP Core Services

The core services a CSP MUST provide are:

**Registration Service:** Verifies the identity and, if applicable, any specific attributes of a Subscriber. 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 Subscriber as verified by the Registration Service.

**Certificate Dissemination Service:** Disseminates certificates to subscribers, and if the Subscriber consents, to Relying Parties. This service also disseminates the CA's policy and practice information to Subscribers and Relying Parties.

**Revocation Management Service:** Processes requests and reports relating to revocation 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 CSP Certificate Status Database whereas Message B is either data 'pushed' to the Revocation Status Service or is a query/response message.

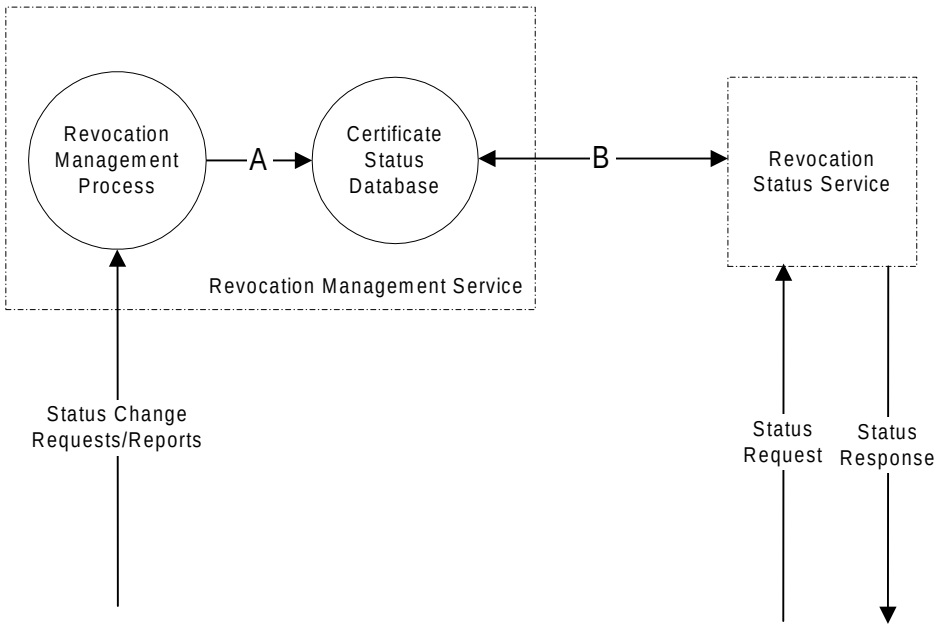


**Figure 2 - Messaging between Revocation Management Service and Revocation Status Service**

## 4.2 CSP Optional Services

The optional services a CSP may provide are:

**Subscriber Device Provision Service:** Prepares and provides a Signature Creation Device (SCD) to Subscribers.

Note: examples of this service are:

- A service which generates the subscriber's key pair and distributes the private key to the subscriber;
- A service which prepares the subscriber's Secure Signature Creation Device (SSCD) and device enabling codes and distributes the SSCD to the registered subscriber.

It is important to note that this service may provide a SCD and/or a SSCD. Within this CWA the security requirements applicable to SCDs are equally applicable to SSCDs, where SSCDs meet the additional requirements stated in Annex III of [EC 1999/93]. No distinction is made whether the SCD/SSCD is implemented in hardware or software.

**Time Stamp Service:** A third party, trusted to provide a Time Stamp Service. The Time Stamp Service provides proof that a data item existed before a certain point in time (proof of existence). If the data item has been signed by the requester before being submitted to the Time Stamp Authority (TSA), then the Time Stamp Service provides proof that the data item existed before a certain point in time.

Within this CWA, 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.

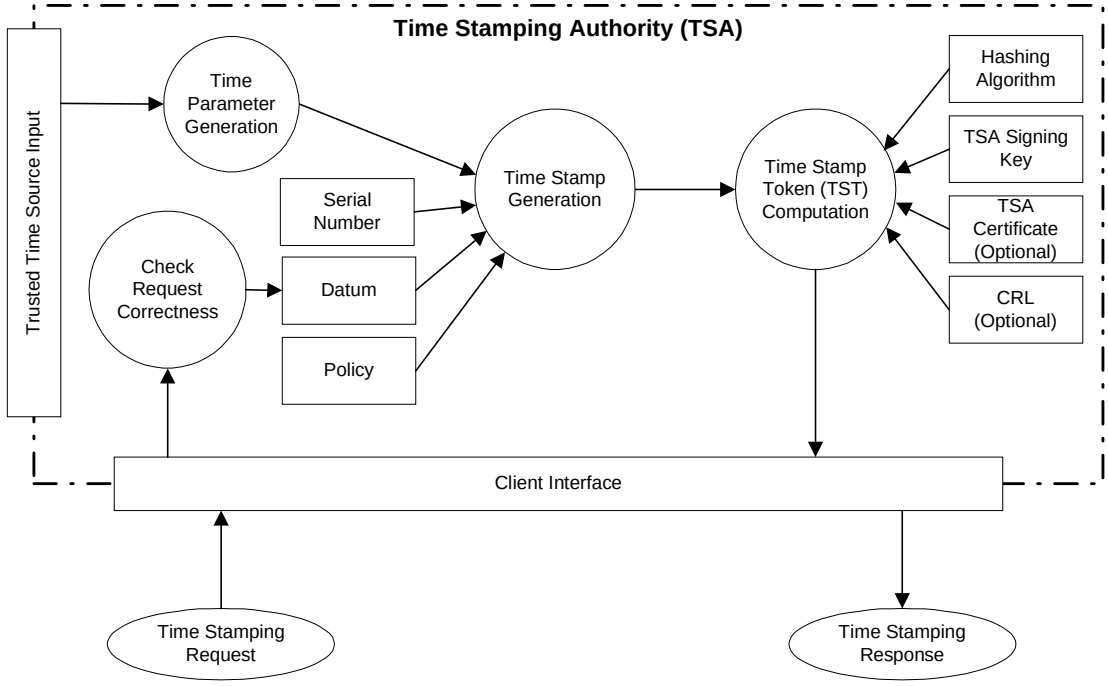


**Figure 3 - Time Stamping Service**

## 4.3 Overall architecture

A CSP'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 Subscriber to a Relying Party. This figure illustrates both mandatory and optional services along with the CSP's interfaces to its Subscribers, Relying Parties and to any external Trust Services.

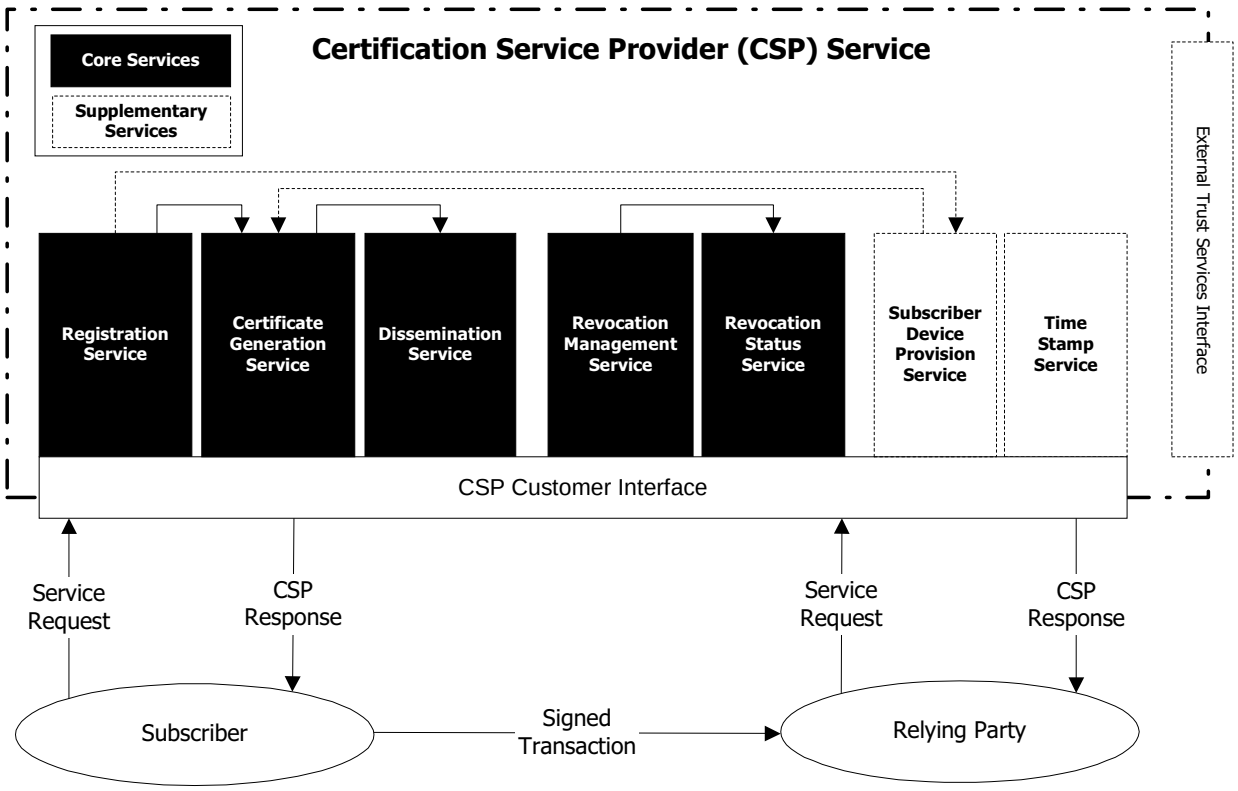


**Figure 4 - CSP Logical Architecture**

As shown, the CSP provides both initial registration and certificate generation as well as subsequent distribution. 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) are provided by the Revocation Management and Revocation Status Services.

The CSP Customer Interface provides access to the CSP's services by Subscribers and Relying Parties. The optional External Trust Services Interface provides access to external services e.g. Cross-certification with other CSPs, trusted archiving services, etc. A CSP may utilise multiple TWSs to provide core and if applicable, supplementary services.

## 4.4 Security levels

The certificates produced by a CSP fall into the following categories:

1. Non-Qualified Certificates (NQCs):
   - Used for Electronic Signatures, meeting [EC 1999/93], article 5.2
   - Used for Electronic Signatures in internal tasks of the TWS

2. Qualified Certificates (QCs):
   - Used for Advanced Electronic Signatures (AES) which are created by a Secure-Signature-Creation Device (SSCD), meeting [EC 1999/93], article 5.1
   - Used for Advanced Electronic Signatures (AES) which are created by a Signature-Creation Device (SCD)

Effectively all security requirements in this CWA are necessary for TWSs issuing QCs, whereas TWSs issuing NQCs can meet a lower set of security requirements. To cater for this, this CWA highlights the requirements that are also necessary for a TWS wishing to issue QCs. The example below shows how this is presented:

> **[SR1.1]**
>
> This is a Security requirement applicable to both NQCs and QCs.

> **[SR1.2] - NQC ONLY**
>
> This is a requirement for TWSs only issuing NQCs.

> **[SR1.2] - QC ONLY**
>
> This is a requirement for TWSs issuing QCs. It is important to note that a TWS meeting this requirement can issue both NQCs and QCs.

A TWS SHOULD either implement **[SR1.2] – NQC ONLY** or **[SR1.2] – QC ONLY**, and not both.

# 5 Security requirements

This section specifies the mandatory processes and related security requirements that are applicable to both core and supplementary services a CSP provides.

TWS **general** functionality and security requirements are provided in §5.1. These are applicable to all CSP services.

TWS **core** services functionality and security requirements are provided in §5.2. These are applicable to all CSP core services (see §4.1).

TWS **supplementary** services functionality and security requirements are provided in §5.3. These are applicable to all CSP supplementary services (see §4.2).

The figure below shows the relationship between these security requirements.

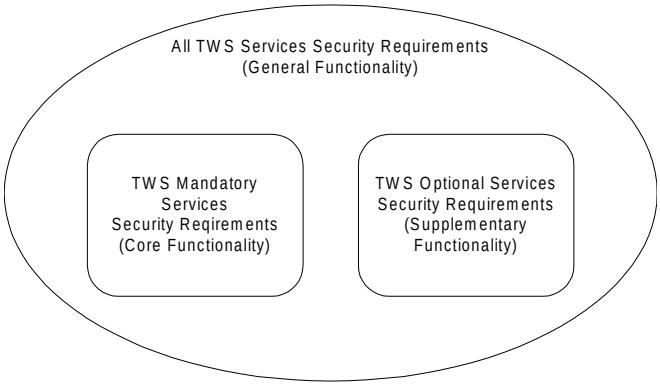


**Figure 5 - Security Requirements Relationships**

# 5.1 General security requirements

## 5.1.1 Management

### M1 Systems and Security Management

A CSP 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 SHALL provide the following privileged roles:

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

**Registration Officers**: Responsible for approving end entity Certificate generation/revocation/ suspension.

**System Administrators:** Are authorised to install, configure and maintain TWSs, but with controlled access to security related configuration.

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

**System Auditors:** Authorised to view archives and audit logs of TWSs.

**[M1.3]**

TWSs MUST be able to associate users with these roles.

It is important that one user cannot perform all the functions specified for TWSs. To prevent this a single user SHOULD NOT be authorised to perform multiple roles.

**[M1.4] – NQC ONLY**

TWSs SHALL be capable of ensuring:

- A user that is authorised to assume a Security Officer role is not authorised to assume a System Auditor role.

**[M1.4] – QC ONLY**

TWSs SHALL be capable of ensuring:

- A user that is authorised to assume a Security Officer role is not authorised to assume a System Auditor role.
- A user that is authorised to assume a System Administrator role is not authorised to assume a Security Officer or a System Auditor role.

## 5.1.2 Systems and operations

### SO1 Operations Management

A CSP operating TWSs needs to ensure that its operations management functions are adequately secure.

**[SO1.1]**

In particular, to support this requirement, a TWS manufacturer MUST ensure instructions are provided to allow the TWS to be:

1. Correctly and securely operated;
2. Deployed in a manner where the risk of systems failure is minimised;
3. Protected against viruses and malicious software to ensure the integrity of the systems and the information they process is upheld.

Note: To meet the conformance requirements of this CWA the TWS manufacturer MUST provide the following system documentation:

- Installation Guidance
- Administration Guidance
- User Guidance

### SO2 Business Continuity

Business Continuity ensures CSP's services are available in case of failure in a TWS.

**[SO2.1]**

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

- Certificate Dissemination Service
- Revocation Management Service
- Revocation Status Service

It is RECOMMENDED that these services provide at least 99.9% availability.

**[SO2.2]**

In the event of a disaster, TWSs must provide functions to enable the CSP to continue operations using alternative TWSs.

Note: Availability requirements are not applicable in a disaster situation. The TWS must meet applicable policy requirements which will specify the maximum acceptable delay in service resumption.

**[SO2.3]**

Migration from primary to disaster recovery systems MUST NOT put undue risk on the trustworthy nature of the systems.

### SO3 Time Synchronisation

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

**[SO3.1] – NQC ONLY**

TWS manufacturers MUST state the time accuracy of TWSs and how this is ensured. It is RECOMMENDED that a trusted time source is used to ensure time accuracy.

**[SO3.1] – QC ONLY**

All clocks of TWSs used for delivering CSP services that are time dependant MUST be synchronised to within 1 second of Co-ordinated Universal Time (UTC).

It is RECOMMENDED two independent sources of UTC are used to maintain a resilient time source.

## 5.1.3 Identification and authentication

### 5.1.3.1 Functional requirements

The Identification and Authentication functions control access and use of TWSs to authorised persons only. This is applicable to all management components of the CSP. Identification and Authentication may be provided either, by the underlying operating software, or directly by the actual component itself.

### 5.1.3.2 Security requirements

### 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]**

Re-authentication MUST be mandatory after log out.

**[IA1.3]**

Authentication challenge data, where used, MUST be unique and not reused.

### 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 (unless the role is of an administrator).

**[IA2.2] – QC ONLY**

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 an inbuilt PIN pad.

**IA3 Verification of Secrets**

**[IA3.1]**

TWSs SHALL provide a mechanism(s) to verify that secrets meet the requirements defined for each component. In any case, the probability of guessing or false acceptance per try SHALL be negligible.

## 5.1.4 System Access Control

### 5.1.4.1 Functional requirements

System Access Control functions control use of objects of TWSs to authorised persons only. This is applicable to all sensitive objects of the CSP. 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 in the identity of the subject attempting the access and:

a) The access rights to the object granted to the subject or;

b) The privileges held by the subject.

### 5.1.4.2 Security requirements

**[SA1.1]**

TWSs MUST provide the capability of controlling and limiting access by identified individuals to the system/user objects they own or are responsible for.

**[SA1.2]**

TWSs MUST ensure they provide access protection to sensitive residual information.

## 5.1.5 Key management

### 5.1.5.1 Functional requirements

A TWS may use cryptographic keys to provide integrity, confidentiality and authentication functions within its own subsystems and in between subsystems. As such, the unauthorised use, disclosure, modification, or substitution would result in a loss of security in the TWSs. It is essential that throughout the key lifecycle management of private and/or secret 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 categorise keys according to their risk profile. For this specification, keys are separated into the following categories:

1. QC/NQC Signing Keys - Certificate Generation Service's key pair for producing Qualified Certificates or /Non-Qualified Certificates

2. Infrastructure Keys – these are keys used by the TWSs for processes such as signing certificate status responses, key agreement, subsystem authentication, audit log signing, encrypting transmitted or stored data, etc. Short term session keys are not categorised as Infrastructure keys.

3. TWS Control Keys – these are keys used by personnel managing or using the TWS and may provide authentication, signing or confidentiality services for those personnel interacting with the system.

In terms of security requirements, QC/NQC 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 cf. to signing keys. The lowest risk keys, used by CSP TWSs, are considered to be those used by personnel for controlling TWSs as these are used by trusted individuals and have even shorter lifespan. Session keys, used for single/short transactions are treated as sensitive information but with lower security requirements to the above stated categories.

Infrastructure and Control 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 Certificate Generation Service's QC/NQC public 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:

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

### 5.1.5.2 Security requirements

**KM1 Key Generation**

**[KM1.1]**

QC/NQC Signing Keys MUST be generated in a secure cryptographic module.

**[KM1.2]**

This secure cryptographic module of [KM1.1] MUST be evaluated and certified to at least one of the following standards or another suitable standard:

- [FIPS140-1], Level 3
- [CEN HSM-PP]
- [ITSEC]

Note: In the case that the secure cryptographic module is evaluated under [ITSEC], the ITSEC Security Target MUST meet the requirements specified in either [FIPS140-1], Level 3 or [CEN HSM-PP] and the secure cryptographic module MUST be evaluated to at least ITSEC E3/high. Provided these criteria are met, it will be accepted as fulfilling the requirements of [KM1.2], [KM1.5], and [TS4.2].

**[KM1.3]**

The secure cryptographic module MUST ONLY generate QC/NQC Signing Keys under dual person control.

Note: Dual control of the required function MAY be achieved either directly by the secure cryptographic module or by the TWS implementing suitable dual controls.

**[KM1.4]**

Infrastructure Keys MUST be generated in a secure cryptographic module.

**[KM1.5] – QC ONLY**[2]

This cryptographic module of [KM1.4] MUST be evaluated and certified to at least [FIPS140-1], Level 2 or another suitable standard.

**[KM1.6] – QC ONLY**

Control Keys MUST be generated in a secure cryptographic module.

Note: This secure cryptographic module must be capable of meeting [FIPS140-1] Level 1 or another suitable standard.

**[KM1.7]**

[2] See additional note in KM1.2

All key generation, if applicable, SHALL also meet the cryptographic requirements specified in [ALGO].

Subscriber keys may be generated centrally or generation may be distributed. Depending upon policy, subscriber keys may be generated and distributed in hardware or software. The Subscriber Device Provision Service §5.3.2 provides details of the applicable security requirements.

### KM2 Key Distribution

**[KM2.1]**

Private and secret keys MUST NOT be distributed in the clear.

**[KM2.2]**

Public keys that have not been certified MUST be kept secure to prevent interception or manipulation.

**[KM2.3]**

The TWSs of a CSP SHALL distribute cryptographic keys in accordance with a specified cryptographic key distribution method.

**[KM2.4]**

The public key associated with the QC/NQC Signing Keys and/or Infrastructure Keys (e.g. Revocation Status Service, Time Stamp Service) MAY need to be distributed to Subscribers and Relying Parties. The integrity and authenticity of this public key and any associated parameters MUST be maintained during initial and subsequent distribution.

The public key associated with the QC/NQC Signing Keys may be distributed in a certificate signed by itself or issued by another Certification Authority (CA). By itself a self-signed certificate cannot be known to come from the CA.

**[KM2.5]**

A self-signed certificate of a CSP MUST have the following properties:

1. The certificate signature MUST be verifiable using data provided within the certificate;
2. The certificate subject and issuer fields MUST 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, is RECOMMENDED to give assurance of the correctness of this certificate.

**[KM2.6]**

The TWS MUST be capable of producing a fingerprint of a self-signed certificate using the hashing algorithms defined in [ALGO].

## KM3 Key Usage

**[KM3.1]**

Access controls SHALL be in place for all secure cryptographic modules used for QC/NQC Signing, Infrastructure and Control Keys.

**[KM3.2] – QC ONLY**

The Certificate Generation Service MUST provide support for dual person control when using Control Keys.

Note: Typically, this would provide administration functionality of the CG service.

**[KM3.3] – QC ONLY**

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 Subscriber Device Provision Service, MUST ensure that subscriber keys for creating electronic signatures are separate from those used for other functions e.g. encryption.

Note: TWSs SHALL ensure that the key usage extension is be present in the signature certificate being issued. If the key usage nonRepudiation bit is asserted then it SHOULD NOT be combined with any other key usage , i.e., if set, the key usage non-repudiation SHOULD be set exclusively.

**[KM3.5]**

Authorised key usage MUST ONLY occur within the operational life of the key (as determined by policy).

**[KM3.6]**

Before TWSs rely on asymmetric Infrastructure or Controls Keys they MUST 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).

## KM4 Key Change

**[KM4.1]**

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

Note: If any of the algorithms used in TWSs is considered to have become unsuitable (as specified in [ALGO]), keys based on that algorithm MUST be changed immediately.

**[KM4.2]**

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

## KM5 Key Destruction

**[KM5.1]**

When QC/NQC Signing Keys reach the end of their life they MUST be destroyed such that the signing keys cannot be retrieved.

**[KM5.2]**

When systems have been used to generate, use or store secret/private keys and they are about to be withdrawn from service or transferred their keys MUST be destroyed.

**[KM5.3]**

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

**[KM5.4]**

Software key destruction MUST be carried out using secure wiping processes that positively overwrite the keys. Examples of this (dependant upon the level of risk exposure) are: overwriting (multiple times)/degaussing magnetic storage media multiple times, or shredding the media.

## KM6 Key Storage, Backup & Recovery

**[KM6.1]**

All private/secret keys MUST by securely stored.

**[KM6.2]**

The QC/NQC Signing Key MUST be stored in a secure cryptographic module which meets the evaluation and certification requirements outlined in KM1.2 (Key Generation).

Private/secret Infrastructure Keys MUST be stored in secure cryptographic modules which meet the certification requirements outlined in KM1.5 (Key Generation).

**[KM6.3] – QC ONLY**

Private/secret Control Keys MUST be stored in secure cryptographic module(s).

**[KM6.4]**

If any private/secret key in a secure cryptographic module is exported from that module, it MUST be protected, to ensure its confidentiality, by the module before being stored outside that module. Any other sensitive key material SHALL never be stored in an unprotected state.

Note: Where the private/secret key is protected by encryption, the cryptographic requirements specified in [ALGO], MUST be met.

The QC/NQC Signing Key of the Certificate Generation Service may be stored and backed up only when additional security mechanisms are in place. For instance, this may be accomplished using m of n techniques, where m component parts out of a total of n component parts are required for successful key initialisation. For recovery from failure purposes, it is RECOMMENDED m ≥ 60% * n (i.e. if n = 3, then m = 2. If n = 4, then m = 3, if n = 5, then m = 3, etc.)

**[KM6.5]**

TWSs MUST ensure that backup, storage and restoration of private/secret NQC/QC Signing, Infrastructure and Control Keys is only performed by authorised personnel (e.g. Security Officer role).

**[KM6.6]**

TWSs MUST ensure that backup, storage and restoration of private NQC/QC Signing Keys is only performed under dual person control.

**[KM6.7]**

TWSs MUST NOT contain functions that allow for backup or escrow of Subscriber signature keys (private keys).

### KM7 Key Archival

**[KM7.1]**

TWSs MUST NOT contain functions that allow archiving of Subscriber signature keys (private keys).

## 5.1.6 Accounting and auditing

Note: Each service has additional specific auditing requirements that must be addressed in addition to these general requirements.

### AA1 Audit Data Generation

**[AA1.1]**

As a minimum, the following events MUST be logged:

- significant TWS environmental, key management and certificate management events
- start-up and shut-down of the audit function
- changes to the audit parameters
- actions taken due to audit storage failure

Additionally it is RECOMMENDED that all access attempts to TWSs are logged.

### 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.

## AA3 Audit Data Parameters

**[AA3.1]**

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

- date and time of event
- type of event
- identity of the entity responsible for the action
- success or failure of the audited event

## AA4 Selectable Audit Review

**[AA4.1]**

All CSP TWSs MUST provide the capability to search for events in the audit log based on the type of event and/or identity of the user.

**[AA4.2]**

The audit records MUST be presented in a manner suitable for the user to interpret the information.

## AA5 Restricted Audit Review

**[AA5.1]**

TWSs SHALL prohibit all user read access to the audit records, except those users that have been granted explicit read access (e.g. those with System Auditor role).

**[AA5.2]**

Modifications of the audit records MUST be prevented.

## AA6 Generation of Alarm

**[AA6.1]**

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

### AA7 Guarantees of Audit Data Integrity

**[AA7.1] – NQC ONLY**

TWSs MUST ensure the integrity of the audit data.

**[AA7.1] – QC ONLY**

TWSs MUST ensure the integrity of the audit data.

To achieve this, 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.

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

### AA8 Guarantees of Audit Timing

**[AA8.1]**

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

## 5.1.7 Archiving

### AR1 Archive Data Generation

**[AR1.1]**

TWSs SHALL be capable of generating an archive.

**[AR1.2]**

At a minimum, the following items SHALL be archived:

- All certificates
- All CRLs/ARLs
- 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 in an unprotected form.

**AR2 Selectable Search**

**[AR2.1]**

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

**AR3 Integrity of Archived Data**

**[AR3.1]**

Each entry in the archive SHALL be protected from modification.

## 5.1.8 Backup and recovery

**BK1 Backup Generation**

**[BK1.1]**

CSP 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 (e.g. System Operator in conjunction with Security Officer)

**BK2 Integrity and Confidentiality of Backup Information**

**[BK2.1] – NQC ONLY**

Backups SHALL be protected against modification.

**[BK2.1] – QC ONLY**

Backups SHALL be protected against modification through use of digital signatures, keyed hashes or authentication codes.

**[BK2.2]**

Critical security parameters and other confidential information SHALL be stored in encrypted form only. The encryption MUST meet the cryptographic requirements specified in [ALGO].

**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]**

A user linked to a role with sufficient privileges SHALL be capable of invoking the recovery function on demand (e.g. System Operator in conjunction with Security Officer).

# 5.2 Core Functionality Security Requirements

## 5.2.1 General

**[GE.1]**

All messages created by any core service MUST:

- Be protected (e.g. by using message authentication codes, digital signatures, etc.) by using the service's Infrastructure Keys.
- Contain a message time, to indicate the time at which the sender created the message
- Include replay attack protection (e.g. by using nonces)

## 5.2.2 Registration service

### 5.2.2.1 Functional requirements

**Certificate Application**

Certificate application is carried out by the Registration Service after identification of the Subscriber has been carried out meeting the requirements specified in the associated Certificate Policy, e.g., [TS101456].

**Subscriber Data Management**

The Registration Service by its nature must manage end entity subscriber data. The data may be affected by many different data protection requirements.

### 5.2.2.2 Security requirements

**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 NQC/QC is issued.

**[R1.1]**

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

**[R1.2]**

This service MUST implement a suitable mechanism to obtain proof-of-possession (POP) to ensure the entity requesting Certification is the actual holder of the private key related to the public key requiring Certification.

An example of this would be to include a signature block with each certificate application, which is created by the private key associated with the public key requiring Certification. Suitable algorithms for creating the signature are detailed in [ALGO].

**[R1.3] – QC ONLY**

The Registration Service MUST be configured to allow collection of enough data from the subscriber to satisfy the requirements for QCs as specified in Annex I of [EC 1999/93].

**[R1.4]**

TWSs MUST provide a mechanism to allow approval of certificate applications, by a Registration Officer, before leaving the Registration Service.

**[R1.5] – QC ONLY**

The following attributes MUST accompany the application:

- Time of application
- Publication Information Control – to allow subscribers to control the Certificate Generation Service's publication of the QC via the Dissemination Service

**[R1.6]**

Messages from the Registration Service MUST be authenticated or digitally signed using its Infrastructure or Control Keys.

### R2 Subscriber Data Management

**[R2.1]**

TWSs SHALL implement mechanisms and security controls to protect the privacy and confidentiality of Subscriber information.

### R3 Registration Service Audit

**[R3.1]**

The following Registration Service specific events MUST be logged:

- All events relating to registration including certificate re-key/renewal requests
- All events relating to approved requests for Certification

## 5.2.3 Certificate Generation Service

### 5.2.3.1 Functional requirements

#### Certificate Generation

After receiving a certificate application from the Registration Service, TWSs generate a certificate using the public key supplied. This ensures the CSP has 'locked' the binding of the Subscriber's public key to 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 distributed via the Certificate Dissemination Service, via the supplementary Subscriber Device Provision Service or to the Subscriber 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 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 and Subscriber Certificates.

### Cross Certification

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

## 5.2.3.2 Security requirements

### CG1 Certificate Generation

**[CG1.1]**

The Certificate Generation Service MUST ensure the integrity, data origin authenticity, and where necessary, the privacy and confidentiality of the certificate request message.

**[CG1.2]**

The message MUST be processed securely and checked for conformance with the applicable Certificate Policy.

**[CG1.3]**

Before certificate generation, the TWS MUST ensure Proof of Possession is validated.

**[CG1.4] – QC ONLY**

The key used to sign a QC SHOULD ONLY be used for signing QCs and, optionally, the related Revocation Status Data

**[CG1.5]**

This service SHALL ONLY generate certificates that are consistent with the allowed profiles as determined by the Security Officer.

**[CG1.6] – NQC ONLY**

All NQCs issued by a TWS MUST have the following properties:

1. Indication of the signatory's name or pseudonym. Where a pseudonym is used this MUST be clearly indicated;

2. The public key in the NQC is related to the signatory's private key;
3. The electronic signature of the CSP, created using the CSP NQC Signing Keys;
4. A unique distinguished name and serial number assigned by the TWS. This MUST be unique with respect to the issuing CSP;
5. The NQC 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*;
6. The signature algorithms/keys used by the TWS to sign the NQC SHOULD be conformant to the algorithm specifications standard [ALGO].
7. Reference to the Certificate Policy under which the NQC is issued.

**[CG1.6] – QC ONLY**

All QCs issued by a TWS MUST meet the requirements specified in ANNEX 1 of [EC 1999/93]. In particular the following properties MUST be present:

1. The public key in the QC is related to the signatory's private key;
2. The advanced electronic signature of the CSP, created using the QC Signing Keys;
3. A unique distinguished name and serial number assigned by the TWS. This MUST be unique with respect to the issuing CSP;
4. The QC 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;
5. The signature algorithms/keys used by the TWS to sign the QC MUST be conformant to the algorithm specifications standard [ALGO].
6. Reference to the Certificate Policy under which the QC is issued.

Additionally QCs issued by the TWS SHOULD meet the certificate profiles stated in [ETSI TS 101 862]. This defines the required subject and issuer fields as well as certificate extensions for subject directories, certificate polices, key usage, biometric data storage and QC declaration statement.

### CG2 Certificate Renewal

**[CG2.1]**

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

**[CG2.2]**

Re-certification of Control and Infrastructure Certificates MUST comply with KM.4 - Key Change (§5.1.5.2).

Control and Infrastructure Certificates may be re-keyed or re-certified online or out-of-band.

**[CG2.3]**

TWSs MUST ensure QC/NQC Signing Keys are updated prior to their expiry. The related (renewed) public keys MUST provide at least the same level of trust as when they were initially distributed.

This MAY be accomplished by providing at least the following intermediary certificates to prove possession of the new private key as follows:

1. Providing a certificate of the old public key signed with the new private key
2. Providing a certificate of the new public key signed with the old private key
3. Providing the new self signed certificate (signed with the new private key)

**[CG2.4]**

TWSs MUST provide a secure mechanism for the re-certifying and/or re-keying of Subscriber keys.

Note: It is RECOMMENDED that Subscriber Certificates be renewed prior to their expiry as the messaging between CSP and subscriber can be secured using the old keys/certificates.

## CG3 Cross Certification

**[CG3.1]**

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

- Authentication and integrity of messages is maintained by both TWSs
- When conducted online, replay attacks of cross certification messages are not possible e.g. by including a nonce in the message

Processes to prove possession of the cross-certification key pair by the requester TWS, as detailed in R.1 Certificate Application (§5.2.2.2) MAY be implemented.

**[CG3.2]**

The responder TWS MUST ensure that the policies and practices adopted by the requester TWS are acceptable to the Subscribers/Relying Parties of the responder TWS.

## CG4 Certificate Generation Service Audit

**[CG4.1]**

The following Certificate Generation Service specific events MUST be logged:

- All events relating to the life-cycle management of QC/NQC Signing, Infrastructure, and Control Certificates
- All events relating to the life-cycle management of QC/NQC Signing keys
- All events relating to the life-cycle management of Subscriber Certificates
- All events relating to cross-certification

## 5.2.4 Certificate Dissemination Service

### 5.2.4.1 Security requirements

**D1 Dissemination Management**

**[D1.1]**

Certificate dissemination by TWSs MUST be limited to the Subscriber, and to Relying Parties according to the limits expressed by the Subscriber.

**[D1.2]**

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

**D2 Import/Export of Objects**

**[D2.1]**

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

- Read access privileges MUST be granted to Subscribers and to authorised entities according to the rules defined by the Subscriber and the Security Policy;
- Write access privileges MUST be limited to authorised roles, according to the definition of roles proposed in §5.1.1.

## 5.2.5 Certificate Revocation Management Service

Figure 2 provides details of the Revocation Management Service, the Revocation Status Service and their relationship with other entities. This section (§5.2.5) and the following section (§5.2.6) make use of this figure for illustrating the requirements.

### 5.2.5.1 Functional requirements

**Certificate Status Change Requests**

Where a Subscriber determines their private key may be compromised, a request for suspension (temporary revocation) of their certificate is sent to their CSP's TWS. A corresponding request to restore a certificate from suspension to operational use may be made by the Subscriber.

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

The CSP 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 CSP.

**Certificate Suspension/Revocation**

The TWS having obtained a suspension or revocation request via this service, changes the certificate status to either Suspended or Revoked (Fig1: message A) in its Certificate Status Database, and this in turn is used by the CSP's Revocation Status Service.

### 5.2.5.2 Security requirements

**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 delay between receipt of a revocation and/or suspension request and the change to certificate status information SHALL NOT exceed one day (24 hr).

Note: **Rauth** + **MP** < 24 Hrs, therefore the TWS MUST be capable of processing requests within **MP.**

Where: **Rauth** is revocation authentication (procedural or automatic) time; **MP** is revocation message propagation time from Revocation Management Service to Revocation Status Service (TWS system requirement).

**[RM1.2]**

All requests for suspension, unsuspension and revocation MUST be suitably authenticated and validated.

**[RM1.3]**

Once a certificate is definitely revoked the TWS MUST ensure it cannot be reinstated.

**[RM1.4]**

Revocation of certificates related to QC/NQC Signing and Infrastructure Keys MUST ONLY be possible under dual control.

**[RM1.5]**

Status changes MUST ONLY be instigated by authenticated:

- CSP Security Officers for Infrastructure/Control Certificates
- Registration/Security Officers for Subscriber Certificates
- Subscribers for their own certificates

Note: As determined by policy, a Subscriber's Certificate maybe revoked/suspended/ unsuspended by a third party (e.g. employer of a Subscriber) by the third party sending a suitable request to the CSP, for instigation of a status change.

**[RM1.6]**

The Certificate Status database MUST be updated immediately after request/report processing (Rauth) is complete.

**RM2 Certificate Suspension/Revocation**

A CSP is responsible for updating/providing the status of certificates on the Revocation Status Service (Fig1: message B). TWSs may implement this using:

- Periodical Messaging: where periodical update messages (e.g. CRLs/ARLs) are sent from the Revocation Management System to the Revocation Management Status Service or;
- 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 MUST be able to revoke any certificate it has issued, even after a disaster.

**[RM2.2]**

Where Periodical Messaging is used, a TWS MUST support the following requirements:

- For an offline status repository (e.g. CRL accessible through directories) the Certificate Revocation Status Service MUST be updated at least on a daily basis.
- For an online status repository (e.g. OCSP responder) the Certificate Revocation Status Service MUST be updated when a status change occurs and additionally at least on a daily basis.
- Each update message MUST include the name and digital signature of the message issuer.
- This issuer MUST either be trusted by the Relying Party directly or be trusted by the Revocation Status Service which in turn is trusted by the Relying Party.
- The messages MAY indicate merely which certificates are revoked/suspended.
- 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 MUST meet the following requirements:

- Where the Revocation Status Service queries a certificate status, the Certificate Status database MUST reply by providing the current status of that certificate.
- A trusted path (Fig1: Message B) MUST exist between the Revocation Management Service and the Revocation Status Service.
- This trusted path MUST be configured to minimise denial of service attacks on the messaging.
- Request and response messages MUST be protected from replay attacks (e.g. by using nonces).

### RM3 Revocation Management Audit

**[RM3.1]**

The following Revocation Management Service specific events MUST be logged:

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

## 5.2.6 Certificate Revocation Status Service

### 5.2.6.1 Functional requirements

**Revocation Status Data**

The Revocation Status Service provides certificate revocation status information to Relying Parties. The Revocation Status Service reflects changes to certificate status as status change requests either by the Subscriber or by the CSP are processed by the Revocation Management Service. This data may also be made available to Subscribers if policy requires Subscribers to have access to revocation status data.

**Status Request/Response**

A Relying Party having obtained the certificate(s) from the Certificate Dissemination Service, required for signature verification, needs to check the status of these certificates. The CSP provides a Revocation Status Service for this purpose. This Revocation Status Service may be an 'online' service (providing real-time certificate status) or an 'offline' service (where certificate status is not real-time).

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 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 reply is thus created and sent to the Relying Party indicating the status of the requested certificate(s).

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.

### 5.2.6.2 Security requirements

**RS1 Revocation Status Data**

**[RS1.1]**

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

**[RS1.2]**

TWSs providing an 'online' revocation status service MUST validate the integrity and authenticity of Real-time or Periodic messages sent to it.

**[RS1.3]**

TWSs providing an 'online' revocation status service using Real-time messaging MUST ensure replies to responses from the Certificate Status database are for the requested certificates.

**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 NQC/QC Signing, Infrastructure and Control Certificates.

**[RS2.1]**

All certificate status responses from an 'online' Revocation Status Service MUST be digitally signed by the Revocation Status Service using its infrastructure keys.

Note: 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 algorithms/keys used for status response SHALL be compliant with [ALGO].

**[RS2.3]**

The signing key used for the response MUST be either:

- Directly trusted by the relying party or;
- Issued by a CA trusted by the relying party

**[RS2.4]**

The response message MUST contain the time at which the Revocation Status Service/Issuer signed the response.

### RS3 Certificate Revocation Status Audit

**[RS3.1]**

The following Certificate Revocation Status Service specific events MUST be logged by an ‘online’ Revocation Status Service:

- All certificate status requests and responses.

# 5.3 Supplementary functionality security requirements

## 5.3.1 Time Stamping Service

A time stamping authority (TSA) is a third party trusted to provide a time stamp service. A time stamp service provides proof 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 3, Time Stamping Service illustrates the TSA's functions and therefore is referred to within this section.

### 5.3.1.1 Functional requirements

**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 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 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 (TST) Computation**

This component is aimed at computing the time stamp token that is returned to the client. It effectively cryptographically signs the data provided by the Time Stamp Generation function.

### 5.3.1.2 Security requirements

**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 ensure that the request for time stamping uses a hash algorithm that is approved as provided by [ALGO].

**TS2 Time Parameter Generation**

Trusted time source requirements when used for Time Parameter Generation in a TSA are more stringent when compared with SO3 – Time Synchronisation. Therefore TS2 requirements supersede SO3 requirements for the TSA.

**[TS2.1]**

The TSA's trusted time source(s) MUST be synchronised to Co-ordinated Universal Time (UTC) within the tolerance dictated by policy e.g. to within 1 second. This MAY be the same source as specified in requirement SO3.

**[TS2.2]**

The TSA's clock SHALL be synchronised with UTC using a mechanism that is demonstrated to be reliable.

### TS3 Time Stamp Generation

**[TS3.1]**

The Serial Number used within the time stamp MUST be unique for each TST issued by a given TSA. This property MUST be preserved even after a possible interruption (e.g. crash) of the service.

**[TS3.2]**

As well as Time Parameter inclusion, the time stamp MUST include the accuracy of the time source used if this is better than that required by the TSA policy.

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

**[TS3.3]**

An indication of the policy under which the time stamp was created MUST be included. The details of the policy provisions are outside the scope of this CWA but MAY indicate conditions under which the time stamp MAY be used (e.g. in reference to QCPs), accreditation status of the TSA, etc.

### TS4 Time Stamp Token (TST) Computation

In addition to the requirements stated in §5.1.4 – Key Management, the following security requirements are applicable and in some cases supersede the requirements specified in §5.1.4 – Key Management.

The TST computation may include the TSA's certificate and any associated certificate status information, although it is RECOMMENDED the Relying Party make use of the Revocation Status Service for certificate status information.

**[TS4.1]**

TSA Signing Keys MUST be generated and stored in a secure cryptographic module.

**[TS4.2]**

The cryptographic module of [TS4.1] MUST be evaluated and certified to at least one of the following standards or another suitable standard[3]:

- [FIPS140-1], Level 3

[3] See additional note in KM1.2

- [CEN HSM-PP]
- [ITSEC]

**[TS4.3]**

TSA Control Keys MUST be stored in a secure cryptographic module.

**[TS4.4]**

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

**[TS4.5]**

The TSA SHALL ensure the time stamp response contains the same Datum that was sent with the request.

**[TS4.6]**

The signature algorithms/keys used by the TSA, if applicable, SHALL meet the cryptographic requirements specified in [ALGO].

**TS5 Time Stamping Service Audit**

**[TS5.1]**

The following Time Stamping Service specific events MUST be logged:

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

## 5.3.2 Subscriber Device Provision Service

### 5.3.2.1 Functional requirements

**SCD Preparation**

The CSP's TWS prepares the SCD by performing the necessary initialisation, formatting and file structure creation.

The TWS either:

- Creates the private/public key pair and loads the private key into the SCD, or
- If applicable, commands the SCD to generate the key pair inside the SCD.

**SCD Provision**

SCD Provision is the distribution of the SCD (after preparation) to the Subscriber.

**Activation Data Creation & Distribution**

The SCD is protected with (secret) activation data to protect the SCD contents. The CSP is responsible for generation of this initial activation data and subsequent secure distribution of this to the subscriber.

### 5.3.2.2 Security requirements

**SP1 SCD Preparation**

**[SP1.1]**

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

**[SP1.2]**

SCD preparation MUST be performed in a secure environment.

**[SP1.3]**

The initialisation, formatting and file structure creation MUST use secure values, parameters and access control conditions, leaving the SCD in a secure configuration, which can not be misused at any time.

**[SP1.4]**

Where a SCD is a SSCD, it MUST be evaluated and certified to [CENSSCD] or another applicable standard.

Note: The chosen standard should specify requirements for internal Signature-Creation Data/Signature-Verification Data Generation, SVD Export, SSCD access control, personalisation and signature creation.

**[SP1.5]**

Where the key pair is generated outside the SCD, the cryptographic device generating the key pairs (SCD-CD) MUST be evaluated and certified to at least one of the following standards:

- [FIPS140-1], Level 3
- [CEN HSM-PP]
- [CENSSCD]

The SCD-CD MAY also be evaluated under [ITSEC] provided the manufacturer/CSP can prove that the ITSEC Security Target meets the requirements specified in one of the above standards and has been evaluated to at least ITSEC E3/high.

**[SP1.6]**

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

**[SP1.7]**

After a SCD-CD generates a key pair for a SCD and achieves successful transfer to that SCD, the SCD-CD key pair MUST be securely destroyed.

### SP2 SCD Provision

**[SP2.1]**

If applicable, the CSP MUST ensure, through appropriate TWS configuration, that the SCD is distributed to the intended and authenticated subscriber.

### SP3 Activation Data Creation & Distribution

**[SP3.1]**

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

**[SP3.2]**

TWSs MUST ensure that the CSP's personnel can not misuse the SCD at any time.

This MAY be achieved either through:

- security procedures during SCD preparation and provision or;
- by providing the subscriber the means by which they MAY verify that the private key has not been used before they have received the SCD.

### SP4 Subscriber Device Provision Service Audit

**[SP4.1]**

TWSs SHALL log all security related events relating to SCD Preparation.

# 6 Conformance requirements

## 6.1 Conformance of CSPs

CSPs SHALL only claim conformance to this CWA if the CSP uses TWSs that have been audited and determined to be conformant to this CWA. In doing so CSPs may benefit by being able to demonstrate a degree of pre-qualification when applying for recognition under an approval scheme.

## 6.2 Conformance of manufacturers

Manufacturers of TWSs SHOULD only claim the TWS's conformance to this CWA by having them audited and determined to be conformant to this CWA. So as to assist CSPs in providing evidence in support of the assessment of their services, manufacturers of TWSs SHOULD make available the results of these audits.

## 6.3 Nature of audit

Audit of these TWSs SHALL be conducted by an independent body qualified to perform the task.

Audits MAY be conducted in the form of an Electronic Data Processing (EDP) Audit, where auditors would:

- determine whether the TWS is conformant to only NQC requirements OR to only QC requirements OR to both NQC and QC requirements - this is indicated for each requirement and is explained in §4.4 - Security Levels;
- collect and evaluate evidence;
- determine whether the TWS meets all requirements specified in sections 4 & 5 of this CWA.

When submitting their TWSs for conformance audits, manufacturers SHOULD provide documentary evidence of:

1. Their development methodology, including configuration management, used for the development of the TWS;
2. Installation Guidance, including procedures for secure installation, generation, and start-up of the TWS. This should include a list of configuration parameters to allow the TWS to be configured to fulfil the requirements of this CWA;
3. Administration Guidance, for configuring, maintaining and administering the TWS such that the required level of security is ensured. Administrator guidance is intended to help administrators understand the security functions provided by the TWS;
4. User Guidance, intended for use by non-administrative users of the TWS, and by others (e.g. developers) using the TWS's external interfaces. User guidance describes the security functions provided by the TWS and provides instructions and guidelines, including warnings, for secure use of the TWS.

When auditing a TWS, evidence of prior formal Information Technology Security Evaluation Criteria [ITSEC] or Common Criteria [CC] evaluations of the TWS MAY be provided. Previously evaluated components would not require re-evaluation. However, assessment of any non-evaluated aspects of the component and its overall use within the TWS is included within the scope of the EDP audit.

The diagram below depicts a typical scenario of a CSP claiming conformance to [TS101456], using TWSs conformant to the present CWA, one of which is an [ITSEC] evaluated TWS. Additionally it outlines the scope of the audit for each case.

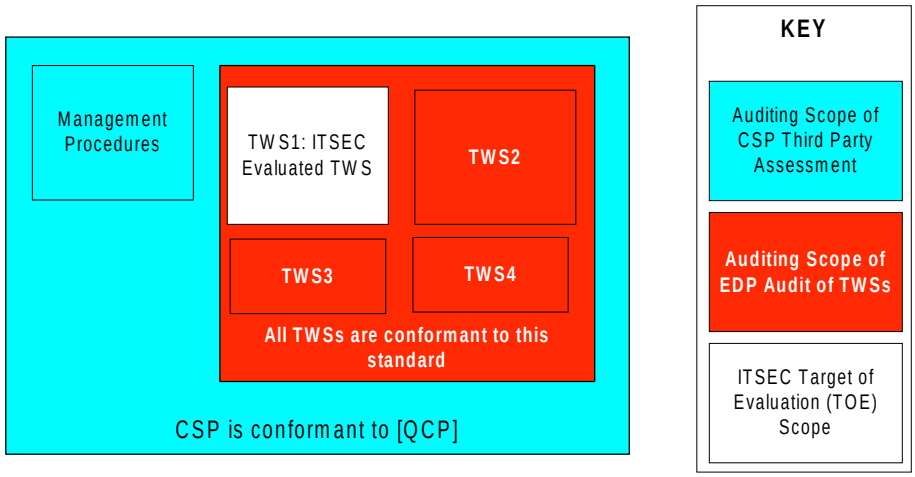


**Figure 6 - Conformance Scopes**

# Appendix A (informative) - Policy to CWA Mapping

In order to help CSPs/CSP auditors better understand how this CWA relates to [TS101456] or other QC policies this appendix is provided as an informational appendix to this CWA. It provides details of how [TS101456] policy requirements are met by using TWSs evaluated against this CWA.

Two tables are provided, a Compliance Checklist of [TS101456] requirements against the requirements of this CWA (Table A) and general CSP requirements against both [TS101456] and this CWA. (Table B)

Usage of this appendix is split into two distinct scenarios:

1. Where a CSP has adopted [TS101456] and is using TWSs (evaluated against this CWA)
2. Where a CSP has adopted a national/other scheme (which differs in policy to [TS101456]) and is using TWSs (evaluated against this CWA)

For (1) above, Table A is provided for auditors of this type of CSP. Here Table A shows which [TS101456] requirements are automatically covered by using evaluated products. This leaves the auditors to audit CSP requirements that are not provided by the TWSs i.e. the unshaded rows in the table[4].

For (2) above, a national/other scheme should create a table similar to Table A against the requirements of their policy. This would be used for checking compliance of the CSP. Table B provides useful cross-referencing against standard functional requirements to facilitate this task.

[4] It is important to note that this CWA strictly covers security requirements of TWS used in a CSP, whereas [TS101456] also encompasses policies affecting other entities: subscribers, relying parties, subcontractors, etc. In addition, [TS101456] covers non security-related organisation items that are outside the scope of this CWA, such as the CSP being a legal entity, liability, personnel background screening, etc. It is this gap that will be assessed by external auditors in scenario 1. Moreover [TS101456] does not provide any policy on Cross Certification, CSP Infrastructure and Control keys or Timestamping.

# TABLE A - [TS101456] v CWA14167-1

This table has the following headings:

**TS Ref:** Reference within [TS101456]

**TS Requirement:** A brief overview of the requirement referenced

**CWA Ref:** A cross reference to same requirements in CWA14167-1

**CWA TWS Compliant?:** Indication of whether a system evaluated to CWA14167-1 meets the TS Ref (✓). Where the requirements are partially met and may require some supplementary auditing of the CSP, they are indicated by (★).

**Notes:** General notes on the cross reference

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| 6.1 | CA Obligations | | | Outside the scope of CWA, organisational requirement. |
| 6.2a | Subscriber Obligations: accurate information | | | Outside the scope of CWA, procedural requirement |
| 6.2b | Subscriber Obligations: key usage | Section 5.1.5.2 [KM3.4] | ✓ | |
| 6.2c | Subscriber Obligations: key usage | | | Outside the scope of CWA, procedural requirement |
| 6.2d | Subscriber Obligations: Key Gen/Algorithms | EESSI Algorithms: Section 2.1<br><br>Section 5.1.5.2 Key Generation: [KM1.7]<br><br>Section 5.2.2.2 Signature | ✓ | CWA requires use of EESSI Acceptable algorithms in section 2.1. |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| | | Algorithm [R1.2] | | |
| 6.2d | Subscriber Obligations: Key length | EESSI Algorithms: Section 2.1 | ✓ | CWA requires use of EESSI Acceptable algorithms in section 2.1. |
| 6.2e | Subscriber Obligations:<br>SSCD requirement | | | Outside the scope of CWA – requirement on SSCD |
| 6.2f | Subscriber Obligations: KeyGen in SSCD | | | Outside the scope of CWA, requirement on SSCD |
| 6.2g | Subscriber Obligations: CA notification | | | Outside the scope of CWA, procedural requirement |
| 6.3 | Relying Party Obligations | | | Outside the scope of CWA, Relying Party obligations reside substantially in verifying the certificate validity and its use in compliance to its limitations. – requirement is on signature validation product. |
| 6.4 | CA liability | | | Outside the scope of CWA<br>Even if the CA makes use of subcontractors the CSP overall responsibility and liability (section 6.4) resides on the CA. |
| 7.1 | Certification Practice Statement | | | Outside the scope of CWA |
| 7.2.1a | Certification Authority Signing key Generation:<br>Physically Secured Environment | | | Outside the scope of CWA, although requirements for use of secure cryptographic module are required. |
| 7.2.1a | Certification Authority Signing key Generation:<br>Dual Control | Section 5.1.5.2 [KM1.3] | ✓ | |
| 7.2.1b | Certification Authority Signing key Generation:<br>Secure Cryptographic Module Requirements | Section 5.1.5.2 [KM1.1], [KM1.2] | ✓ | CWA has same evaluation criteria requirements for QC key generation secure cryptographic modules |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| 7.2.1.c | Certification Authority Signing key Generation:<br><br>Algorithm Requirement | Section 5.1.5.2 [KM1.7] | ✓ | |
| 7.2.1.d | Certification Authority Signing key Generation:<br><br>Key Length | Section 5.1.5.2 [KM1.7] | ✓ | |
| 7.2.2. | Certification Authority Key storage, backup and recovery:<br><br>Key Integrity & Confidentiality | Section 5.1.5.2 [KM6.1] | ✓ | |
| 7.2.2a | Certification Authority Key storage, backup and recovery:<br><br>Certificate Signing Key Secure Cryptographic Device | Section 5.1.5.2 [KM6.2], [KM6.3] | ✓ | |
| 7.2.2b | Certification Authority Key storage, backup and recovery:<br><br>Key Export | Section 5.1.5.2 [KM6.4] | ✓ | |
| 7.2.2c | Certification Authority Key storage, backup and recovery:<br><br>Dual Control for backup/recovery | Section 5.1.5.2 Trusted Roles: [KM6.5]<br><br>Dual Control: [KM6.6] | ✓ | |
| 7.2.2d | Certification Authority Key storage, backup and recovery:<br><br>Security of Backup Keys | Section 5.1.5.2 [KM6.1] | ✓ | |
| 7.2.2e | Certification Authority Key storage, backup and recovery: | Section 5.1.5.2 [KM6.1], [KM6.4], | ✓ | |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| | Certificate Signing Key Secure Cryptographic Device Access | [KM3.1], [KM3.2] | | |
| 7.2.3 | Certification Authority public key distribution | Section 5.1.5.2 [KM2.4] | ✓ | CWA 14167 section 5.1.4.2 KM2 provides for distribution not only of CA signing key but also of infrastructure keys. |
| 7.2.4 | Key Escrow | Section 5.1.5.2 [KM6.7] | ★ | Auditor needs to ensure no other procedural key escrow mechanisms are being used. |
| 7.2.5 | CA key usage restriction | Section 5.1.5.2 [KM3.1], Section 5.2.3.2 [CG1.4] | ★ | TS 101 456 requires also for physically secure premises, that must be audited separately. |
| 7.2.6 | End of CA key life cycle | Section 5.1.5.2 KM5 | ✓ | |
| 7.2.6a | End of CA key life cycle: Destruction | Section 5.1.5.2 KM5 | ✓ | |
| 7.2.6a | End of CA key life cycle: Archival | | | Outside the scope of CWA, procedural requirement |
| 7.2.7a | Cryptographic Hardware lifecycle:<br>Tampering whilst in transit | | | Outside the scope of CWA, procedural requirement |
| 7.2.7b | Cryptographic Hardware lifecycle:<br>Tampering whilst in storage | | | Outside the scope of CWA, procedural requirement |
| 7.2.7c | Cryptographic Hardware lifecycle:<br>Dual control of Control Keys | Section 5.1.5.2 [KM3.1], [KM3.2] | ✓ | |
| 7.2.7d | Cryptographic Hardware lifecycle:<br>Correctly operating hardware | | ★ | This is partially covered by requiring evaluated cryptographic modules. (See Section 5.1.5.2 [KM1.2]). Mostly procedural requirement. |
| 7.2.7e | Cryptographic Hardware lifecycle: | Section 5.1.5.2 | ★ | CSP Procedures are also required for this. |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| | Key Destruction | [KM5.1], [KM5.2], [KM5.3], [KM5.4] | | |
| 7.2.8a | CA-generated subscriber keys :<br><br>Algorithm requirement | Section 5.1.5.2<br><br>[KM1.7] | ✓ | |
| 7.2.8b | CA-generated subscriber keys:<br><br>Key length requirement | Section 5.1.5.2<br><br>[KM1.7] | ✓ | |
| 7.2.8c | CA-generated subscriber keys:<br><br>Generated and stored securely before delivery to the subscriber. | Section 5.3.2.2. [SP1] | ✓ | |
| 7.2.8d | CA-generated subscriber keys:<br><br>The subscriber's private privacy is not compromised on delivery and only the subscriber can access it. | Section 5.3.2.2. [SP1.1], [SP1.4], [SP1.5], [SP1.6], [SP2.1] | ✓ | |
| 7.2.9a | CA-issued SSCD:<br><br>SSCD preparation | Section 5.3.2.2. [SP1.1], [SP1.2], [SP1.3], [SP1.4], [SP1.5], [SP1.6] | ✓ | CWA 14167 section 5.3.2.2 SP1.5 specifies the security standards the SSCD must be certified against |
| 7.2.9b | CA-issued SSCD:<br><br>SSCD storage and distribution | Section 5.3.2.2 [SP2.1] | ★ | CSP Procedures are also required for this. |
| 7.2.9c | CA-issued SSCD:<br><br>Controlling SSCD activation and deactivation | Section 5.3.2.2 [SP3.1], [SP3.2] | ★ | Activation data protection does not depends solely on TWS features, so additional auditing of procedures is necessary |
| 7.2.9d | CA-issued SSCD:<br><br>Activation data to be securely prepared and | Section 5.3.2.2 [SP3.1], [SP3.2] | ★ | Although some aspects of activation data are covered, this is a procedural requirement and thus outside the scope of CWA. |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| | distributed separately from the SSCD | | | |
| 7.3.1a | Subscriber Registration:<br><br>CA to provide subscribers with Terms and Conditions regarding use of certificate | | | Outside the scope of CWA: procedural / legal requirement. |
| 7.3.1b | Subscriber Registration:<br><br>CA to provide previous Terms and Conditions as per section 7.3.1a through durable electronic means in easily understandable language | | | Outside the scope of CWA: procedural / legal requirement. |
| 7.3.1c | Subscriber Registration:<br><br>CA to securely identify the subscriber as per national laws | | | Outside the scope of CWA: procedural / legal requirement. |
| 7.3.1d,e,f,g,h | Subscriber Registration:<br><br>Subscriber data are to be collected | Section 5.2.2.2 [R1.3] | ★ | TS details which subscriber data are to be collected, and rules on how they must be recorded and on how long they must be retained.<br><br>CWA specifies that the Registration Service MUST allow collection of data as per Directive Annex I |
| 7.3.1i | Subscriber Registration:<br><br>Records retention for a period suitable to provide forensic evidence | | | Procedural requirement. |
| 7.3.1j | Subscriber Registration:<br><br>Where the key pair is not generated by the CA, the subscriber must provide Proof of Possession (POP) of the private key | Section 5.2.2.2 [R1.2]<br><br>Section 5.2.3.2 [CG1.3] | ★ | TS 101 456 compliance implies that the user is provided with a client capable of generating such POP and sending it to TWS. The CWA ensures POP checking is in place at the registration service, therefore additional auditing at the subscriber application may be necessary. |
| 7.3.1k | Subscriber Registration:<br><br>Subscriber data must be kept according to the | Section 5.2.2.2 [R1.1], [R2.1] | ★ | TWS provide functionality to deal with privacy of subscriber data. The CSP must be audited to ensure |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| | national privacy protection laws | | | conformance to local data protection requirements. |
| 7.3.1 | Registration Service (additional requirements) | | | In addition to what is detailed in the previous rows, CWA 14167 (section 5.2.2) and TS 101 456 (sections 7.3.1 and – partly – 7.4.11) cover the registration service from two complementary viewpoints.<br>• TS 101 456 details the subscriber registration process and which are the required information, such as:<br>– Terms and Condition provision and means of provision;<br>– secure identification of the subscriber as per national law;<br>– data the subscriber must provide evidence of;<br>– CA to record all subscriber application related information and subscriber signed agreements.<br>• CWA 14167 details the security requirements, such as:<br>– Application approval by a Registration Officer;<br>– Application Approval to be digitally signed via Infrastructure or Control keys<br>– Application to specify Time of Application and a reference to the Dissemination Service to allow subscribers to verify certificate correctness |
| 7.3.2 | Certificate renewal, rekey and update | Section 5.2.3.2 [CG2.1], [CG2.4] | ★ | TS point out the need for the CA to ascertain that no certificate-related information have changed since previous certification, and that the algorithm / key length are still cryptographically secure enough. |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| | | | | CWA 14167 section details the security requirements, by: providing secure mechanisms for re-certification, avoiding substitution attacks, updating the key pair before their expiry date, and for the CA to issue old-with-new, new-with-old, new-with-new certificates (as per RFC 2510 section 2.4)<br><br>Therefore the two standards scopes are different. It is important to ensure that the CSP checks TS requirements and uses CWA provided secure functionality for Certificate/key renewal. |
| 7.3.3a | Certificate Generation:<br><br>Compliance with 1999/93/EC Directive Annex I and Annex II (g) | Section 5.2.3.2 [CG1.1], [CG1.6] | ✓ | Compliance with CWA 14167-1 [CG1.6] implies issuance of a QC, as specified in TS 101 862, which meets the Directive requirements mentioned in TS 101 456 7.3.3.a |
| 7.3.3b | Certificate Generation:<br><br>Securely linked to the associated process, including the provision of any subscriber generated public key. | Section 5.2.3.2 [CG1.1], [CG1.2], [CG1.3], [CG1.5], [CG1.6], CG2 | ✓ | |
| 7.3.3c | Certificate Generation:<br><br>CA generated subscribers key | Section 5.2.3.2 [CG1.1], [CG1.2], Section 5.3.2.2 [SP1.6], [SP2.1] | ✓ | The TS 101 456 requirement that the procedure of issuing the certificate is securely linked to the key pair generation by the CA process is fulfilled by the CWA 14167-1 [CG1.2] requirement to abide by the Policy. |
| 7.3.3d | Certificate Generation:<br><br>Uniqueness of the distinguished name assigned to the subscriber within the domain of the CA. | Section 5.2.3.2 [CG1.6] item 3 | ★ | Depending on the implementation this could be a procedural or technical issue. Auditors are therefore requested to ascertain which case applies and, where necessary, to perform additional procedural inspections |
| 7.3.3e | Certificate Generation:<br><br>Protection of registration data | Section 5.2.2.2 [R1.1], [R2.1], Section 5.2.3.2 | ✓ | |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| | | [CG1.2] | | |
| 7.3.3f | Certificate Generation:<br><br>External and recognised registration service providers identity is authenticated, where applicable. | Service 5.2.2.2 [R1.6], Section 5.2.3.2 [CG1.1] | ★ | TS 101 456 section 7.3.3f scope is broader than CWA 14167 R1.6, therefore, where external Registration Service Providers are involved, they must be separately audited. |
| 7.3.4 | Dissemination of Terms and conditions | | | Outside the scope of CWA, legal requirement |
| 7.3.5a | Certificate Dissemination:<br><br>Complete and accurate certificate to be available to its owner. | Section 5.2.4.1 [D1.1], [D2.1], Section 5.2.2.2 [R1.5] | ✓ | |
| 7.3.5.b | Certificate Dissemination:<br><br>Certificates to be retrievable, under Subscriber consent. | Section 5.2.4.1 [D1.1] | ★ | Obtaining consent is procedural |
| 7.3.5c | Certificate Dissemination:<br><br>Certificate usage terms and conditions to be made available to relying parties. | | | Outside the scope of CWA, legal requirement |
| 7.3.5d | Certificate Dissemination:<br><br>Applicable terms and conditions shall be readily identifiable for a given a certificate. | | | Outside the scope of CWA, legal requirement |
| 7.3.5e | Certificate Dissemination:<br><br>Certificates and Terms and Conditions shall be available 24 hours per day, 7 days per week. Disaster are to be addressed in its CPS. | Section 5.1.2 [SO2.1], [SO2.2], [SO2.3] | ★ | The availability of Terms and Conditions needs to be audited. Availability may also include some service management aspects. |
| 7.3.5f | Certificate Dissemination:<br><br>Certificates, where applicable, and Terms and | Section 5.2.4.1 [D2.1] | ★ | CWA D2.1 specifies that access is to be granted to Subscribers and relying parties for whom the Subscriber gave its consent, as per Security Policies. No limitation is |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| | conditions shall be publicly and internationally available. | | | set on cross border availability, which should be separately audited. |
| 7.3.6a | Certificate Revocation Management - Procedures<br><br>The maximum delay between receipt of a revocation related request and the change to revocation status information shall be at most 1 day. | Section 5.2.5.2 [RM1.1], [RM1.2], [RM1.6], [RM2.2] | ★ | TS 101 456, in addition to CWA stipulations, specifies some procedural requirements, such as procedures for invoking revocation, who can activate them, revocation reason, etc.<br><br>CWA, on the other hand, details security requirements, such as protection form reply attacks, existence of a trust path between the revoking authority and the requester of one certificate status.<br><br>Therefore additional auditing is required for TS. |
| 7.3.6b | Certificate Revocation Management - Requests and reports<br><br>Shall be processed on receipt. | Section 5.2.5.2 [RM1.1], [RM1.6] | ★ | TS 101 456 implies that procedures are in place to be complied with by users and other parties: such procedures require ad hoc auditing. |
| 7.3.6c | Certificate Revocation Management - Authentication<br><br>Revocation requests are to be authenticated and authorised. | Section 5.2.5.2 [RM1.2], [RM1.5] | ★ | Additional inspections to be performed by auditors on procedures referring to this topic. |
| 7.3.6d | Certificate Revocation Management:<br><br>Suspension - A certificate is not kept suspended for longer than is necessary to confirm its status. | | | Outside the scope of CWA, procedural requirement |
| 7.3.6e | Certificate Revocation Management:<br><br>Information to the subscriber - The subject of a revoked or suspended certificate shall be informed of the change of status of its certificate. | Section 5.2.6.1<br><br>[RS1], [RS2] | ✓ | This is provided by way of the Revocation Status Service. Access to the Subscriber needs to be provided to enable this. |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| 7.3.6f | Certificate Revocation Management:<br><br>A definitively revoked certificate shall not be reinstated. | Section 5.2.5.2 [RM1.3] | ✓ | |
| 7.3.6g | Certificate Revocation Management:<br><br>CRL properties | Section 5.2.5.2 CRL Requirements: [RM2.2]<br><br>Trusted Signing: Section 5.1.5.2 [KM3.3], Section 5.2.3.2 [CG1.4], Section 5.2.5.2 [RM2.2] | ✓ | |
| 7.3.6h | Certificate Revocation Management<br><br>Revocation management services shall be available 24 hours per day, 7 days per week. | Section 5.1.2 [SO2.1], Section 5.2.5.2 [RM2.1] | ✓ | May also include some service management aspects. |
| 7.3.6i | Certificate Revocation Status<br><br>Revocation status information, shall be available 24 hours per day, 7 days per week. | SO2.1 | ✓ | May also include some service management aspects. |
| 7.3.6j | Certificate Revocation Status<br><br>The integrity and authenticity of the status information shall be protected. | Section 5.2.6.2 RS1, [RS2.1], [RS2.3] | ✓ | CWA adds specific security requirements, such as time of status reply issuance. |
| 7.3.6k | Certificate Revocation Status<br><br>Revocation status information shall be publicly and internationally available. | Section 5.2.6.1 | ★ | CWA is targeted at providing revocation status information to Relying Parties and if needed to Subscribers.<br><br>If a CSP provides access to this information publicly this needs to be audited. |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| 7.4.1 | CA security management | | | Outside the scope of CWA: procedural / legal requirements. |
| 7.4.2 | Asset classification and management | | | Outside the scope of CWA, procedural requirement |
| 7.4.3a | Personnel security:<br>HR Policy | | | Outside the scope of CWA, procedural requirement |
| 7.4.3b | Personnel security:<br>Security roles and responsibilities, shall be documented in job descriptions. | Section 5.1.1 [M1.1] | ★ | TWSs provide functionality for roles. TS 101 456 covers also job description documentation, thus additional auditing is required |
| 7.4.3c | Personnel security:<br>Separation of duties | Section 5.1.1 [M1.1], [M1.2], [M1.3], [M1.4] | ★ | TWSs provide separation/separation for roles. TS 101 456 covers job description based on separation of duties. |
| 7.4.3d | Personnel security:<br>Management Procedures | | | Outside the scope of CWA, organisational requirement |
| 7.4.3e | Personnel security:<br>Management Responsibility | | | Outside the scope of CWA, organisational requirement |
| 7.4.3f | Personnel security:<br>Conflicting interests | Section 5.1.1 [M1.4] | ★ | TS 101 456 envisages a broader range of conflicting interests than the sheer technical ones provided for by CWA 14167-1, thus additional auditing is required. |
| 7.4.3g | Personnel security:<br>Trusted roles | Section 5.1.1 [M1.2] | ✓ | |
| 7.4.3h | Personnel security:<br>Trusted roles assignment | | | Outside the scope of CWA, organisational requirement |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| 7.4.3i | Personnel security:<br><br>HR Policy on convictions | | | Outside the scope of CWA, organisational requirement |
| 7.4.4 | Physical and Environmental Security<br><br>Physical access shall be limited to authorised individuals and certificate issuance facilities are protected from environmental hazards. | | | Outside the scope of CWA, organisational requirement |
| 7.4.5a | Operations Management – General<br><br>Protection against viruses, malicious and unauthorised software. | Section 5.1.2 [SO1.1] | ✓ | |
| 7.4.5b | Operations Management – General<br><br>Incident reporting and response procedures. | | | Outside the scope of CWA, procedural requirement |
| 7.4.5c | Operations Management – General<br><br>Media shall be securely handled | | | Outside the scope of CWA, procedural requirement |
| 7.4.5d | Operations Management – General<br><br>Procedures established and implemented for all involved trusted and administrative roles. | | | Outside the scope of CWA, procedural requirement |
| 7.4.5e | Media handling and security<br><br>Media to be handled according with classification scheme.<br><br>Media containing sensitive data shall be securely disposed of when no longer required. | Media Destruction: Section 5.1.5.2 [KM5.4] | ★ | Information classification scheme outside the scope of the CWA.<br><br>CWA 14167-1 covers only destruction of key material related media.<br><br>TS 101 456 refers to all sensitive data, thus specific auditing shall be implemented. |
| 7.4.5f | System Planning: | | | Outside the scope of CWA, organisational requirement |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| | Future capacity planning to ensure adequate processing power and storage. | | | |
| 7.4.5g | Incident reporting and response:<br><br>All incidents shall be reported as soon as possible. | | | Outside the scope of CWA, procedural requirement |
| 7.4.5h | Operations procedures and responsibilities<br><br>CA security operations shall be separated from normal operations. | | | Outside the scope of CWA, procedural requirement<br><br>TS lists the responsibilities to be separated from normal operations. CWA enforces some of them in specific sections. |
| 7.4.6a | System Access Management:<br><br>CA General - Network and Communications Security | | | Outside the scope of CWA, CSP requirement |
| 7.4.6b | System Access Management:<br><br>CA General - Sensitive data protection over insecure networks. | Section 5.2.2.2 [R1.1], [R2.1], [CG1.2] | ★ | CWA, in the referenced items, covers mainly subscriber data related messages and certificate request message. TS covers all sensitive data, so additional auditing is to be performed on sensitive data out of the limits specified in CWA. |
| 7.4.6c to 7.4.6e | System Access Management:<br><br>CA General - Identification & Authentication | Section 5.1.3.2 [IA1], [IA2], [IA3] | ✓ | CWA 14167 section 5.1.3. |
| 7.4.6f | System Access Management:<br><br>CA General - CA personnel accountability | Section 5.1.3.2 [IA1.1],<br>Section 5.1.6 [AA3.1] | ★ | This is achieved by auditing against roles.<br><br>Personnel accountability may also be implemented with procedures out of the TWS control. In such case additional auditing is to be performed. |
| 7.4.6g | System Access Management:<br><br>CA General - Sensitive data protection against data/media reuse. | Section 5.1.4.2 [SA1.2]<br><br>Section 5.1.5.2 [KM5.1], [KM5.2], | ✓ | |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| | | [KM5.4] Section 5.3.2.2 [SP1.7] | | |
| 7.4.6h | System Access Management:<br>CA General - Logical and physical access management and control | Section 5.1.4.1 [SA1.1], [SA1.2] | ★ | Auditing is outside the scope of CWA, procedural requirement |
| 7.4.6i | System Access Management:<br>CA General - Monitoring and Alarming | Section 5.1.4.2 [SA1.1], Section 5.1.6 [AA6.1] | ✓ | Security requirement AA6.1 is to be intended extensively, in that any unauthorized attempt to access the CSP TWS must be detected and reacted against. |
| 7.4.6k | System Access Management:<br>Dissemination Service - Access Control | Section 5.1.4.2 [SA1.1], Section 5.2.4.1 [D2.1] | ✓ | |
| 7.4.6.l | System Access Management:<br>Revocation Management Service - Monitoring and Alarming | Section 5.1.4.2 [SA1.1], Section 5.1.6 [AA6.1] | ✓ | Security requirement AA6.1 is to be intended extensively, in that any unauthorized attempt to access the CSP TWS must be detected and reacted against. |
| 7.4.6m | System Access Management:<br>Revocation Status – Access Control to objects | Section 5.1.4.2 [SA1.1], section 5.2.6.2 [RS1.1], [RS1.2] | ✓ | |
| 7.4.7 | Trustworthy Systems Deployment and Maintenance<br>CA General<br>a) Carry out an analysis of security requirements of any systems development project<br>b) Change control procedures to exist. | Whole of CWA | ✓ | Conformance to this CWA meets this requirement. Evaluation of systems against this CWA ensures manufacturers provide their design methodology, which for example includes configuration control. |
| 7.4.8a | BCP: CA Key Compromise | | | Outside the scope of CWA, procedural requirement |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| | | | | CWA 14167 section 5.1.2 – SO2 points out instead the key services to keep up and running and provides for technical indications on requirements to meet in case of disaster. |
| 7.4.8.b | BCP: Revocation Status | | | Outside the scope of CWA, procedural requirement |
| 7.4.9 | CA Termination | | | Outside the scope of CWA, procedural requirement<br><br>TS 101 456 details procedural requirements to prevent CA termination to abruptly disrupt subscribers' operations. |
| 7.4.10 | CSP compliance with legal requirements | | | Outside the scope of CWA, legal requirements |
| 7.4.11a | Recording of Information Concerning Qualified Certificates:<br><br>General - Confidentiality and integrity of current and archived records. | Section 5.1.6 [AA1.1], [AA2.1], [AA2.2], [AA5.1], [AA5.2], [AA6.1], [AA7.1], Section 5.1.7 [AR1.1], [AR1.4], [AR3.1], Section 5.2.2.2 [R2.1] | ★ | Also need to consider procedures for handling printed records. |
| 7.4.11b | Recording of Information Concerning Qualified Certificates:<br><br>General - Records concerning qualified certificates shall be completely and confidentially archived. | Section 5.1.6 [AA1.1] Section 5.1.7 [AR1.1], [AR1.2] | ★ | Also need to consider procedures for handling printed records. |
| 7.4.11c | Recording of Information Concerning Qualified Certificates:<br><br>General - Records concerning qualified certificates shall be made available to provide evidence in legal | | | Outside the scope of CWA, procedural requirement |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| | proceedings. | | | |
| 7.4.11d | Recording of Information Concerning Qualified Certificates:<br><br>General - The precise time of significant CA events shall be recorded. | Section 5.1.6 [AA3.1], [AA8.1], Section 5.1.7 [AR1.3] | ✓ | |
| 7.4.11e | Recording of Information Concerning Qualified Certificates:<br><br>General - Records concerning qualified certificates shall be held for a period of time as appropriate for providing necessary legal evidence in support of electronic signatures. | | | Outside the scope of CWA, procedural requirement |
| 7.4.11f | Recording of Information Concerning Qualified Certificates<br><br>General - Event logs must not be easily deleted or destroyed. | Section 5.1.6 [AA2.1], [AA2.2], [AA5.2], [AA6.1], [AA7.1]<br><br>Section 5.1.7 [AR3.1] | ✓ | |
| 7.4.11g | Recording of Information Concerning Qualified Certificates<br><br>General - The specific events and data to be logged shall be documented by the CA. | | | Outside the scope of CWA, procedural requirement |
| 7.4.11h | Recording of Information Concerning Qualified Certificates<br><br>Registration - All registration related events are | Section 5.2.2.2 [R3.1] | ✓ | SSCD preparation may be implemented out of CA premises (e.g.: at a subcontracted provider's) In such case additional inspections are to be performed to ascertain that suitable processes are in force. |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| | logged. | | | |
| 7.4.11i | Recording of Information Concerning Qualified Certificates:<br><br>Registration - All registration information is recorded. | Section 5.2.2.2 [R1.3], [R3.1] | ★ | TS specifies a minimal list of documents and data to be archived, which is out of the CWA scope. CWA refers to [EC 1999/93] annex1 as required TWS functionality. Therefore additional auditing is required for TS 101 456. |
| 7.4.11j | Recording of Information Concerning Qualified Certificates:<br><br>Registration - Privacy of subscriber information is maintained. | Section 5.1.4.2 [SA1.2]<br><br>Section 5.1.5.2 [KM6.4]<br><br>Section 5.1.8 [BK2.2]<br><br>Section 5.2.2.2 [R1.1], [R2.1]<br><br>Section 5.2.3.2 [CG1.1]<br><br>Section 5.3.2.2 [SP1.6] | ★ | NB: Procedural aspects need to be further audited. |
| 7.4.11k | Recording of Information Concerning Qualified Certificates:<br><br>Certificate Generation - The CA shall log all events relating to the life-cycle of CA keys. | Section 5.1.6 [AA1.1], Section 5.2.3.2 [CG4.1] | ✓ | |
| 7.4.11l | Recording of Information Concerning Qualified Certificates:<br><br>Certificate Generation - The CA shall log all events | Section 5.1.6 [AA1.1], Section 5.1.7 [AR1.2], Section 5.2.3.2 [CG4.1], Section | ✓ | |

| TS Ref | TS Requirement | CWA Reference | CWA TWS Compliant? | Notes |
|---|---|---|---|---|
| | relating to the life-cycle of certificates. | 5.2.5.2 [RM3.1] | | |
| 7.4.11m | Recording of Information Concerning Qualified Certificates<br><br>Subscriber Device Provision - The CA shall log all events relating to the life cycle of all keys managed by the CA. | Section 5.1.6 [AA1.1], Section 5.2.3.2 [CG4.1] | ✓ | |
| 7.4.11n | Recording of Information Concerning Qualified Certificates<br><br>Subscriber device provision - The CA shall log all events relating to the preparation of SSCDs. | Section 5.1.6 [AA1.1], section 5.3.2.2 [SP4.1] | ✓ | |
| 7.4.11o | Recording of Information Concerning Qualified Certificates<br><br>Certificate Revocation Management - Requests and reports relating to revocation and the resulting action are logged. | Section 5.1.6 [AA1.1], section 5.2.5.2 [RM3.1], Section 5.2.6.2 [RS3.1] | ✓ | |
| 7.5 | Organisational | | | Outside the scope of CWA, organisational requirements |

# TABLE B: Security Requirements V [TS101456] and CWA14167

| Topic | TS 101 456 Reference (section #) | CWA 14167-1 Reference (section # - Requirement ID) | Notes |
|---|---|---|---|
| Accounting and auditing – Certificate generation | 7.4.11 letters k), l) | Section 5.1.6 AA1,<br>Section 5.2.3.2 CG4 | CWA refers to audit records relevant to all types of certificates: QC/NQC signing, infrastructure, control, subscribers, cross certification, etc. |
| Accounting and auditing – Certificate generation | 7.4.11 letters k), l) | Section 5.1.6 AA1,<br>Section 5.2.3.2 CG4<br>Section 5.1.7 [AR1.2],<br>Section 5.2.5.2 [Rm3.1] | CWA refers to audit records relevant to all types of certificates: QC/NQC signing, infrastructure, control, subscribers, cross certification, etc. |
| Accounting and auditing – Certificate revocation status | | Section 5.2.6.2 RS3 | TS no stipulation, though the “Revocation Management” auditing can extensively be interpreted as referring to the Revocation Status service also. |
| Accounting and auditing – General | 7.4.11 letters a) to g) | Section 5.1.6 AA1, AA2, AA3, AA5, AA6, AA7, AA8,<br>Section 5.1.7 AR1, AR3<br>Section 5.2.2.2 R2 | TS defines requirements and procedures (including relevance to forensic and legal evidence) for integrity, confidentiality, disclosure and retention of archived records.<br>CWA specifies TWSs manage audit log data parameters, generation, availability, review, integrity, need for a trusted timestamp and for alarm generation. |
| Accounting and auditing – Registration | 7.4.11 letters h) to j) | Section 5.1.4.2 [SA1.2],<br>Section 5.1.5.2 [KM6.4],<br>Section 5.1.8 [BK2.2],<br>Section 5.2.2.2 [R1.1], [R1.3], [R2.1], R3 | TS defines types of documents / information to be recorded<br>CWA details as specified in – A & A General |

| Topic | TS 101 456 Reference (section #) | CWA 14167-1 Reference (section # - Requirement ID) | Notes |
|---|---|---|---|
| | | Section 5.2.3.2 [CG1.1]<br>Section 5.3.2.2 [SP1.6] | |
| Accounting and auditing – Subscriber device provision | 7.4.11 letters m) to n) | Section 5.1.6 AA1<br>Section 5.2.3.2 CG4<br>Section 5.3.2.2 SP4 | |
| Accounting and auditing – Time Stamp Service | | Section 5.3.1.2 TS5 | CWA: TSS key related events (certificate request, key life cycle management) and all failures must be logged. |
| Algorithms and key length | 6.2 letters d) and e),<br>7.2.1 letters c) and d),<br>7.2.8 letters a) and b) | Section 5.1.5.2 [KM1.7],<br>Section 5.2.2.2 [R1.2],<br>Section 5.2.3.2 [CG1.6],<br>Section 5.2.6.2 [RS2.2],<br>Section 5.3.1.2 [TS1.2] and [TS4.6] | TS 101 456 specifies algorithms and key lengths to be recognised as fit by the cryptographic advisory as per Directive 1999/93/ec article 9<br>CWA 14167 refers to a document to be issued by EESSI specifying acceptable algorithms and key lengths. |
| Archiving | 7.4.11 letters e) and f) | Section 5.1.7 | TS 101 456 section 7.4.11 covers in general the need for a CSP to keep its services relevant document and information for a suitable length of time, thus implying archiving.<br>CWA 14167 section 5.1.6 focuses mainly on data archival specifics. |
| Certificate Dissemination | 4.1 and 7.3.5 | Section 5.1.2 SO2,<br>Sections 5.2.2.2 [R1.5],<br>Section 5.2.4 | Certificates dissemination is limited to the subscribers (who need to verify the certificate correctness) and to the other cases for which the subscriber has given his consent.<br>CWA 14167 section 5.2.2.2 R1.5 specifies that subscribers may check their certificate publication by the dissemination service.<br>CWA 14167 section 5.1.2 SO2.1 lists the Dissemination Service among those that must withstand a single failure and provide a 99,9 % availability |

| Topic | TS 101 456 Reference (section #) | CWA 14167-1 Reference (section # - Requirement ID) | Notes |
|---|---|---|---|
| | | | (roughly: maximum service unavailability for 40 minutes per month) |
| Certificate Generation | 7.2.5 and 7.3.3 | Section 5.1.5.2 [KM3.1],<br>Section 5.2.2.2 [R1.1], [R1.2], [R1.6], [R2.1],<br>Section 5.2.3.2 CG1, CG2 | Access control for crypto devices used for certificate signing.<br>Subscriber's data privacy to be protected.<br>POP: see "Proof of Possession".<br>Both TS 101 456 section 7.2.5 and CWA 14167 paragraph 5.2.3.2 CG1.4 recommend CA certificate signing key to be used solely for certificate/CRL signing.<br>CWA refers to all types of certificates: QC/NQC signing, infrastructure, Control, subscribers, cross certification, etc. |
| Certificate Renewal | 7.3.2 | section 5.2.3.2 CG2 | TS: CA to verify that data exchanged between CA and subscriber at registration time are still valid<br>CWA: specifies means by which the certificate renewal process is secured. |
| Certificate Revocation Management | 7.3.6 letters a) to h) | Section 5.1.2 SO2.1<br>Section 5.2.5.2 | Revocation (i.e.: certificate status change) must occur within one day from request.<br>CRLs must state by which time the next CRL will be issued, max 24 hours<br>Revocation Management is one of the services that CWA 14167 section 5.1.2 SO2.1 requires are available 99,9% (This means that the maximum accepted "down time" is 40 minutes per month). |
| Certificate Revocation Status | 7.3.6 letter I) to k) | Section 5.1.2 SO2.1<br>Section 5.2.6.2 | Revocation status is one of the services that CWA 14167 section 5.1.2 SO2.1 requires are available 99,9%. (This means that the maximum accepted "down time" is 40 minutes per month).<br>It may be "off-line" (e.g.: CRLs) or "on-line" (e.g. OCSP).<br>TS 101 456 specifies that when an online service is provided, its information base must be updated "on the fly", yet every 24 hours at most it must be updated. |

| Topic | TS 101 456 Reference (section #) | CWA 14167-1 Reference (section # - Requirement ID) | Notes |
|---|---|---|---|
| Certification Service Provider | 4.1 | Sections 4.1, 4.2 and 5.3 | TS 101 456 details in section 4.1 the services that a CA as a CSP is to provide: they are all the Core Services specified in CWA 14167 at section 4.1 plus the Optional – Supplementary Subscriber Device Provision Service defined in CWA 14167 at section 4.2 the security requirements of which are specified in section 5.3 |
| Certification Authority key destruction | 7.2.6 | Section 5.1.5.2 KM5 | CA Keys at the end of their life must be destroyed or (TS 101 456) archived in a manner they cannot be put back into use. CWA details the possible ways to carry out the key destruction. |
| Certification Authority Key HW life cycle management | 7.2.7 | Sections 5.1.5.2 KM3.1 | TS 101 456 section 7.2.7 points out additional requirements versus CWA 14167-1, like the need for the crypto HW to be verified for not having been tampered with and to be working properly. |
| Certification Authority Key storage, backup and recovery | 7.2.2 | Section 5.1.5.2 [KM3.1], [KM3.2], KM6 | The same stipulations apply as for CA Key generation hardware.<br>Private key may be exported for backup reason provided it is suitably protected. TS 101 456 specifies it must be encrypted with an algorithm and a key length approved by the cryptographic panel (Art. 9).<br>Key (and corresponding crypto hardware) handling requires at least dual control (TS 101 456).<br>CWA also specifies for the certificate signing keys a percentage of the authorised operators. |
| Certification Authority Key usage | 7.2.5 through 7.2.7 | Section 5.1.5.2 KM3, KM5<br>Section 5.2.3.2 [CG1.4] | CA Keys must be securely (at least under dual control) handled in secure premises with access control.<br>CA signing keys are recommended to be used solely for signing certificates.<br>CWA recommends separate CA Infrastructure keys to be generated for separate functions. |
| Certification Authority public | 7.2.3 | Section 5.1.5.2 [KM2.4], [KM2.5] | CA public key integrity and authenticity must be protected when distributed to subscribers and relying parties. |

| Topic | TS 101 456 Reference (section #) | CWA 14167-1 Reference (section # - Requirement ID) | Notes |
|---|---|---|---|
| key distribution | | | |
| Certification Authority Security management – Asset Management | 7.4.2 | N/A | Assets are to be classified consistently with a Risk Analysis (see Certification Practice Statement) and an inventory is to be maintained. |
| Certification Authority Security management – General | 7.4.5 | Section 5.1.2 SO1<br><br>Section 5.1.4.2 [SA1.1]<br><br>Section 5.1.5.2 [KM5.4] | |
| Certification Authority signing key Generation | 7.2.1 | Section 5.1.5.2 [KM1.1] , [KM1.2], [KM1.3], [KM1.7] | TS 101 456 section 7.2.1 and CWA 14167 section 5.1.4.2 KM1.1 - KM1.3 provide for CA Secure Signature Creation Device certification as per FIPS 140-1 level ≥ 3 and per an appropriate CC PP (still to be defined).<br><br>CWA 14167, in addition, accepts ITSEC E3 High, provided the ST is inline with CC PP or FIPS140-1 L3.<br><br>TS 101 456 mentions algorithms and key length approval by the cryptographic panel as per Article 9 of 1999/93/EC.<br><br>CWA 14167 refers to [ALGO]. |
| Certification Authority self-signed certificate | | 5.1.5.2 [KM2.5] | TS: no provision.<br><br>CWA specifies mandatory properties. |
| Certification Authority termination | 7.4.9 | N/A | TS states the minimum stipulations a CSP must conform to manage its termination without service disruption. |
| Certification Practice Statement | 7.1 | N/A | TS 101 456 section 7.1 – CA to carry out a Risk Assessment, on supporting subcontractors too, and to draw out a CPS:<br><br>• approved by a high level management, |

| Topic | TS 101 456 Reference (section #) | CWA 14167-1 Reference (section # - Requirement ID) | Notes |
|---|---|---|---|
| | | | • publicly available,<br>• the modifications to which are timely made public,<br>• matching both the QCP requirements and the Risk Assessment identified security features. |
| Cross Certification | N/A | Section 5.2.3.2 CG3 | CWA assigns a CSP the responsibility of ensuring that policies and practice of the CA, it cross certifies with, are acceptable to its own subscriber.<br>TS 101 456 doesn't cover the topic, as spelled out in its Scope Section. |
| CSP Business continuity | 7.4.8 | Section 5.1.2 SO2 | TS 101 456 (section 7.4.8) focuses on addressing the CA key compromise in the Disaster Management Plan.<br>CWA 14167 (section 5.1.2 – SO2) points out the following key services to be kept up and running:<br>• Dissemination service<br>• Revocation Management Service<br>• Revocation Status Service<br>It also provides for technical indications on requirements to meet in case of disaster. |
| CSP control keys – overall security requirements | | Sections 5.1.5.1<br>Section 5.1.5.2 [KM1.6], [KM1.7], [KM2.1] to [KM2.4], KM3 except [KM3.4], KM4, KM5 except [KM5.1], KM6 except [KM6.6] and [KM6.7], | TS 101 456 doesn't envisage control keys<br>CWA specifically addresses them.<br>TS 101 456 mentions Algorithms and key length approval by the cryptographic panel as per Article 9 of 1999/93/EC. CWA 14167 refers to [ALGO]. |
| CSP infrastructure key | | Sections 5.1.5.1<br>Section 5.1.5.2 [KM1.4], [KM1.5], | TS 101 456 doesn't envisage infrastructure keys that, hence:<br>• if used by human beings are to be likened to subscriber keys; |

| Topic | TS 101 456 Reference (section #) | CWA 14167-1 Reference (section # - Requirement ID) | Notes |
|---|---|---|---|
| | | [KM1.7], [KM2.1] to [KM2.4], KM3 except [KM3.4], KM4, KM5 except [KM5.1], KM6 except [KM6.6] and [KM6.7], | • if related to Time Stamp Service, are covered in the Time Stamp policy specific TS;<br>• if used by CSP to manage certificate revocation and/or to issue certificate status information are to be likened to CSP certificate signing keys.<br>CWA specifically addresses infrastructure keys as independent items.<br>TS 101 456 mentions Algorithms and key length approval by the cryptographic panel as per Article 9 of 1999/93/EC. CWA 14167 refers to [ALGO]. |
| CSP infrastructure key change | | Section 5.1.5.2 KM4 | Key changeover may be on-line or off-line |
| CSP infrastructure key destruction | | Section 5.1.5.2 KM5 | |
| CSP infrastructure key distribution | | Section 5.1.5.2 KM2 (except [KM2.5]) | CWA: infrastructure key may be distributed to subscriber and relying parties, provided its integrity and authenticity is maintained. |
| CSP infrastructure key generation | | Section 5.1.5.2 [KM1.4], [KM1.5], [KM1.7] | CWA: infrastructure keys device must be certified to one of the following:<br>• FIPS 140-1 at least level 2<br>• Or other suitable standard. |
| CSP infrastructure key revocation | | Section 5.2.5.2 [RM1.4] | CWA: infrastructure keys revocation must be under at least dual control |
| CSP infrastructure key storage | | Section 5.1.5.2 [KM6.1], [KM6.2], [KM6.4], [KM6.5] | CWA same device characteristics as for key generation |

| Topic | TS 101 456 Reference (section #) | CWA 14167-1 Reference (section # - Requirement ID) | Notes |
|---|---|---|---|
| CSP infrastructure key usage | | Section 5.1.5.2 [KM3.1], [KM3.3], [KM3.5], [KM3.6] | |
| CSP Network and Communications Security | 7.4.6 letters a), b), and from h) on<br><br>(see also section 7.4.5, letter h. 5th bullet) | Section 5.2.1<br><br>Section 5.2.2.2 [R1.1], [R2.1] | TS section 7.4.6.b) also mandates for sensitive data protection over insecure networks.<br><br>CWA implicitly provides for such requirement when requesting for data protection. |
| CSP officers – Personnel security | 7.4.3 | Section 5.1.1 | Both TS 101 456 (section 7.4.3) and CWA 14167 (section 5.1.1) give the same job description for the CSP officers. TS 101 456 additionally specifies the policy to comply with, regarding personnel hiring and appointing and their management system. CWA additionally specifies a registration role.<br><br>TS 101 456, in addition, specifies that the security senior management is to formally appoint to such roles adequately skilled personnel with a reliable background. |
| CSP Operations Management | 7.4.5 | Section 5.1.2,<br><br>Section 5.1.5.2 [KM5.4] | TS: Operational and organisation procedures must encompass and try to prevent security breaches as well as safety incidents. PKI operations must be separated from normal operations and covered by CA security personnel.<br><br>CWA strictly refers to the systems operations security. |
| CSP Physical and Environmental Security | 7.4.4 and 7.4.6 item i) | N/A | |
| CSP System Access Management | 7.4.6 | Section 5.1.4, Section 5.1.3.2 [IA1.1], Section 5.1.5.2 [KM5.1], [KM5.2], [KM5.4], Section 5.1.6 [AA3.1], [AA6.1], Section 5.2.4.1 [D2.1], Section 5.2.6.7 [RS1.1], [RS1.2]Section 5.3.2.2 [SP1.7], | TS 101 456 section 7.4.6 covers all System Access Management topics. CWA 14167 specific sections are relevant to the single items. Additionally, section 5.1.4 refers specifically to System Access Control. |

| Topic | TS 101 456 Reference (section #) | CWA 14167-1 Reference (section # - Requirement ID) | Notes |
|---|---|---|---|
| | | [SA1.1] | |
| Dissemination of Terms and conditions | 7.3.4 | N/A | TS remarks on the importance of trust in a CSP's services by the dissemination of terms and conditions (T&Cs) to subscribers and to relying parties. It lists the minimum content of such T&Cs. |
| Identification & Authentication | 7.4.6 letters from c) through f) | CWA section 5.1.3, Section 5.1.6 [AA3.1] | TS focuses on administration of user and personnel identification, privilege separation and accountability.<br><br>CWA details I & A implementation specifics. |
| Key change | 7.3.2 item d) (subscriber's) | Section 5.1.5.2 KM4<br><br>Section 5.2.3.2 CG2 | TS partially covers subscribers' key change.<br><br>CWA also covers CSP key changeover. Key changeover may be on-line or off-line. |
| Key escrow | 7.2.4 | Section 5.1.5.2 KM6.7 | No escrow is allowed. |
| Obligations – CA | 6.1 and 6.4 | | TS 101 456 section 6.1 – CSP's main obligation is to abide by the stipulations in the QCP. Even if the CA makes use of subcontractors the CSP overall responsibility and liability (section 6.4) resides on the CSP. |
| Obligations – relying party | 6.3 | | TS 101 456 section 6.3 – relying party obligations reside substantially in verifying the certificate validity and its use in compliance to its limitations. |
| Obligations – subscriber | 6.2 | | TS 101 456 section 6.2 – specifies the minimum obligations a CA shall oblige subscribers via specific agreements. |
| Proof Of Possession | 4.1 and 7.3.1 item j) | Section 5.2.2.2 [R1.2]<br><br>Section 5.2.3.2 [CG1.3] | Necessary if subscriber signature keys are not generated by CA.<br><br>TS 101 456 section 4.1 and CWA 14167 section 5.2.2.2 R1.2 both specify that the Registration Service must include a suitable mechanism to insure the subscriber is actually in possession of the private key corresponding to the public one the certification is requested for. |
| Registration Service (Security Requirements) | 7.3.1 and – partly – 7.4.11) | Section 5.2.2 | TS 101 456 details the subscriber registration process.<br><br>CWA 14167 details the security requirements, such as data privacy |

| Topic | TS 101 456 Reference (section #) | CWA 14167-1 Reference (section # - Requirement ID) | Notes |
|---|---|---|---|
| | | | protection, POP provision by the subscriber, event logging. |
| Subscriber Device Provision Service | 7.2.8 and 7.2.9 | Section 5.1.5.2 [KM1.7]<br><br>Section 5.3.2 | 1. Subscribers' key generation by the CA (or by a TSP):<br>• TS: key generation algorithm and key length must be recognised as fit by the crypto panel under the commission as per Directive art. 9.<br>• CWA: CA to verify SCD is created by an approved manufacturer [SP1.1], in a secure environment [SP1.2], on a device certified according to FIPS 140-1, at least level 3, or a specific CC PP. ITSEC is also permitted.<br>2. Subscribers' SSCD to be securely controlled and stored by the CA<br>3. Activation data must be securely created and distributed separately from the SSCD they refer to.<br>N.B.: TS 101 862 Qualified Certificate Profile section 4 states that the CA must have "some knowledge" of SSCDs used by the subscribers. |
| Subscriber Key archival | 7.2.4 | Section 5.1.5.2 KM7 | TS 101 456 section 7.2.4 forbids Key escrow. Its meaning is to be extended to Subscribers' key archival<br><br>CWA 14167 section 5.1.4.2 KM7 forbids such archival. |
| Subscriber key usage | 6.2 letter b) | Section 5.1.5.2 [KM3.4] | A Subscriber's signature key cannot be used for other functions |
| System and data backup and recovery | 7.2.2 and 7.4.8 | Section 5.1.5.2 KM6<br><br>Section 5.1.8 | TS 101 456 covers in detail only CA key backup and recovery (section 7.2.2). More broadly section 7.4.8 require CAs to restore their operations as soon as possible in case of disaster, which implies backup and recovery.<br><br>CWA 14167 covers this specific item in section 5.1.8 |
| Time Stamp Service | N/A | Sections 4.2, 4.3 and 5.3.1 | TS 101 456 does not cover this service since a TS specific to Time Stamp Service Policy is planned to be issued as part of the EESSI phase 3. |

| Topic | TS 101 456 Reference (section #) | CWA 14167-1 Reference (section # - Requirement ID) | Notes |
|---|---|---|---|
| | | | CWA 14167 briefly describes the TSS in section 4.2, mentions it in section 4.3 and fully details its security requirements in section 5.3.1 |
| Time Synchronization | No exact coverage in TS 101 456 | Section 5.1.2 SO3 | TS 101 456 section 7.4.11 letter d), by stating the *"precise time of significant CA … events shall be recorded"* implies that time synchronization must be in place.<br><br>CWA 14167 section 5.1.2 SO3 |