CEN

WORKSHOP

AGREEMENT

CWA 14167-1

June 2003

ICS 03.120.20; 34.040

Supersedes CWA 14167-1:2001

English version

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

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, Spain, Sweden, Switzerland and United Kingdom.

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

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No. CWA 14167-1:2003 D/E/F

Contents

Foreword

Successful implementation of European Directive 1999/93/EC on a Community framework for electronic signatures [Dir.1999/93/EC] 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.

In 1999 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, to create the European Electronic Signature Standardisation Initiative (EESSI).

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

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

The purpose of this CWA is to describe the security requirements for trustworthy systems managing certificates for electronic signatures. This purpose of this CWA is to define overall system security requirements, whereas other parts specific security requirements for cryptographic modules.

The CWA is intended for use by designers and developers of systems managing certificates for electronic signatures, as well as customers of such systems.

This CWA consists of the following parts:

- Part 1: System Security Requirements;
- Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP);
- Part 3: Cryptographic Module for CSP Key Generation Services – Protection Profile (CMCKG-PP).

This version of this CWA 14167-1:2003 was published on 2003-06-19.

A list of the individuals and organizations which supported the technical consensus represented by this CEN Workshop Agreement is available to purchasers from the CEN Central Secretariat.

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

This CWA is specifically relevant for manufacturers of Trustworthy Systems (TWSs) used for managing certificates, but may be adopted by anyone deploying trusted systems and wanting to meet the requirements of [Dir.1999/93/EC]. It provides an overview of a CSP system broken down into a number of services. Some of these services are mandatory, termed ‘Core Services' whereas others are optional, ‘Supplementary Services'.

A CSP must implement systems that provide all Core Services. If the CSP additionally provides optional services, they must meet the corresponding Supplementary Service requirements. These services are to be provided by the TWSs adopted by the CSP, whose security requirements are specified in this CWA.

For all services, some "General security requirements" are initially specified. These are mandatory and are applicable to all services. Furthermore, specific security requirements relating directly to each Core Service or Supplementary Service are also specified.

Core Services covers the following CSP services:

- Registration Service - to verify the identity and, if applicable, any specific attributes of a Subject
- Certificate Generation Service - to create certificates;
- Dissemination Service - to provide certificates and policy information to Subjects 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 Services covers two optional CSP services:

- Subject Device Provision Service – to prepare and provide a Signature Creation Device (SCDev) to Subjects. This includes Secure-Signature-Creation Device (SSCD) provision;
- Time-stampingService – provides a Time-stamping Service which may be needed for signature verification purposes.

This specification provides standards for Trustworthy Systems (TWSs) providing Core and Supplementary Services, issuing both Qualified Certificates (QCs) and Non-Qualified Certificates (NQCs). Meeting the requirements for issuing of QCs automatically implies meeting the requirements for issuing NQCs.

Manufacturers of TWSs are required to produce systems that provide functionality meeting the security requirements specified in this CWA. Guidance for Conformity Assessment can be found in [CWA 14172.3]. Once compliance has been established, a CSP may use the approved TWS, thus ensuring that they meet the requirements of the [Dir.1999/93/EC].

A CSP may adopt a 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 been independently assessed and approved as being conformant to this CWA.

Introduction

The European Directive [Dir.1999/93/EC] 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 [Dir.1999/93/EC] 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 [Dir.1999/93/EC], CSPs must:

“ 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 may 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 TWSs certified as being conformant to this CWA may be adopted by CSPs to reduce their effort in deploying systems meeting [Dir.1999/93/EC]. This procedure should enable maximum flexibility for industry in developing 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 TWSs conformant to this CWA will require minimal configuration by CSPs using them, to meet the system (policy) requirements of [TS101456]. The diagram below illustrates the relationship:

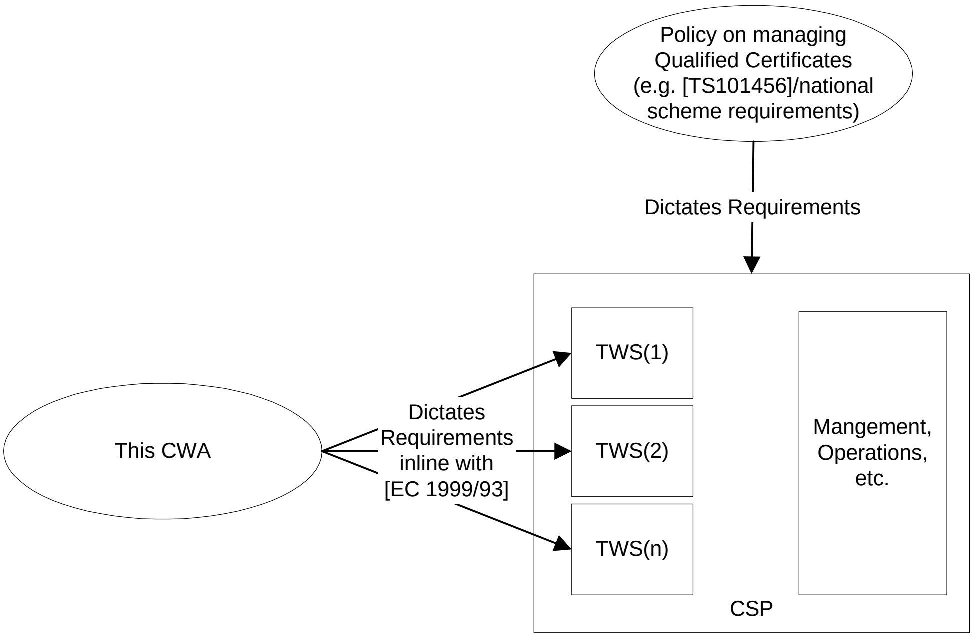
Policy on managing Qualified Certificates (e.g. [TS101456]/national scheme requirements)
Dictates Requirements
This CWA
Dictates Requirements inline with [EC 1999/93]
TWS(1)
TWS(2)
TWS(n)
Mangement, Operations, etc.
CSP

Figure 1 - Relationship between Policy and this CWA

TWSs addressed by this CWA provide the following mandatory CSP Core Services:

- Registration of subject information (Registration Service);
- Certificate generation (Certificate Generation Service);

- Certificate dissemination (Dissemination Service);
- Certificate revocation management (Revocation Management Service);
- Certificate revocation status provision (Revocation Status Service).

Furthermore, they may provide the following optional CSP Supplementary Services:

- Time-stamping functions (Time-Stamping Service);
- Signature-Creation/Secure-Signature-Creation Device production (Subject Device Provision Service).

Note: where a CSP is offering supplementary services in addition to the core services, they must adopt the security requirements specified in this CWA for these supplementary 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 [Dir.1999/93/EC].

Although [Dir.1999/93/EC] 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 subject 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 subject to the identity and possibly other information of the subject by means of an electronic signature which is created with the private key (certificate signing key) of the issuing CSP. Other forms of electronic signatures are outside the scope of this document.

With reference to electronic signatures, [Dir.1999/93/EC] 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].

Security requirements for the optional Subject Device Provision Service, which provides SCDev/SSCD provision to Subjects are included within the scope of this CWA. However, requirements for the actual SSCD devices themselves, as used by Subjects 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].*

Although this specification is based on the use of public key cryptography, it does not require or define any particular communication protocol or format for electronic signatures, certificates, certificate revocation lists, certificate status information and time stamp tokens. It only assumes certain types of information to be present in the certificates in accordance with Annex I of [Dir.1999/93/EC]. Interoperability between CSP systems and subject 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 [Dir.1999/93/EC]. 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 [Dir.1999/93/EC]. Details of how compliance with 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 the requirements in [Dir.1999/93/EC] Annex II (f), but in considering this it is important to additionally encompass the following [Dir.1999/93/EC] 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 document applies.

[CEN CMCSO-PP] CWA 14167-2 Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP).

[CEN CMCKG-PP] CWA 14167-3 Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP).

[CENSSCD] CWA 14169 Secure Signature Creation Devices EAL4+.

[TS101862] ETSI TS 101 862, Qualified Certificate Profile.

[ALGO] ETSI SR 002 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures.

2.2 Informative References

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

[TS101456] ETSI TS 101 456, Policy Requirements for Certification Authorities Issuing Qualified Certificates.

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

[RFC 3280] RFC3280, 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, ISO/IEC 95948.

[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.

3 Definitions and Abbreviations

3.1 Definitions

Definitions from [Dir.1999/93/EC]:

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. [Dir.1999/93/EC].

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 [Dir.1999/93/EC].

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 [Dir.1999/93/EC].

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

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

Secure-signature-creation device: a signature-creation device which meets the requirements laid down in Annex III of the Directive [Dir.1999/93/EC].

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

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

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

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 [Dir.1999/93/EC].

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

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 [Dir.1999/93/EC].

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 [Dir.1999/93/EC].

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 3280 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 3280].

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 3280].

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 3280].

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 private 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 3280].

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: That 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:

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).

Subject: An entity identified in a certificate as the holder of the private key associated with the public key given in the certificate.

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

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

Dissemination Service: A service that disseminates certificates to Subjects, and if the subject consents, to Relying Parties. This service also disseminates the CA’s policy & practice information to Subjects 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.

Subject Device Provision Service: A service that prepares and provides a Signature Creation Device to Subjects.

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

Time-Stamping Service: A service that generates and provides time-stamp tokens.

Hardware Cryptographic Device: A hardware-based cryptographic device that generates, stores and protects cryptographic keys and provides a secure environment in which to perform cryptographic functions. Note: examples of such devices are PC boards, smart cards and USB tokens.

3.2 Abbreviations

ARL	Authority Revocation List
CA	Certification Authority
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CEN/ISSS	CEN Information Society Standardization System
CP	Certificate Policy
CRL	Certificate Revocation List
CSP	Certification Service Provider
EC	European Commission
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunications Standards Institute
ETSI SEC	ETSI Security Technical Committee
HW	Hardware
HCD	Hardware Cryptographic Device
ISSS	Information Society Standardisation System
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
SCDev	Signature-Creation Device
SF	Security Function
SSCD	Secure-Signature-Creation Device
TSA	Time-Stamping Authority
TSS	Time-Stamping Service
TST	Time-Stamp Token
TWS	Trustworthy System
WS/E-SIGN	CEN/ISSS Electronic Signatures workshop

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 approach adopted in 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 services. Although this specification considers security requirements for the subsystems involved in the CSP's service, the aim is to provide the Subject (Signatory) 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.

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

TWSs used for issuing and managing certificates are required to fulfil the General Security Requirements in §5.1 as well as specific Core Services Security Requirements in §5.2, and Supplementary Services Security Requirements in §5.3. In summary, a CSP MUST deploy TWSs meeting all General and Core Security Requirements. It is important to note that this technical/security integration does not necessarily impede on the freedom of the CSP to run the different components of the service using different business entities.

When choosing TWSs for issuing NQCs/QCs, a CSP MUST ensure that it is conformant to this specification. Conformity assessment guidance can be found in [CWA 14172-3].

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 Subject. The results of this service are passed to the Certificate Generation Service.

Certificate Generation Service: Creates and signs certificates based on the identity and other attributes of a Subject as verified by the Registration Service.

Dissemination Service: Disseminates certificates to subjects, and if the Subject consents, to Relying Parties. This service also disseminates the CA's policy and practice information to Subjects and Relying Parties.

Revocation Management Service: Processes requests and reports relating to revocation 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.

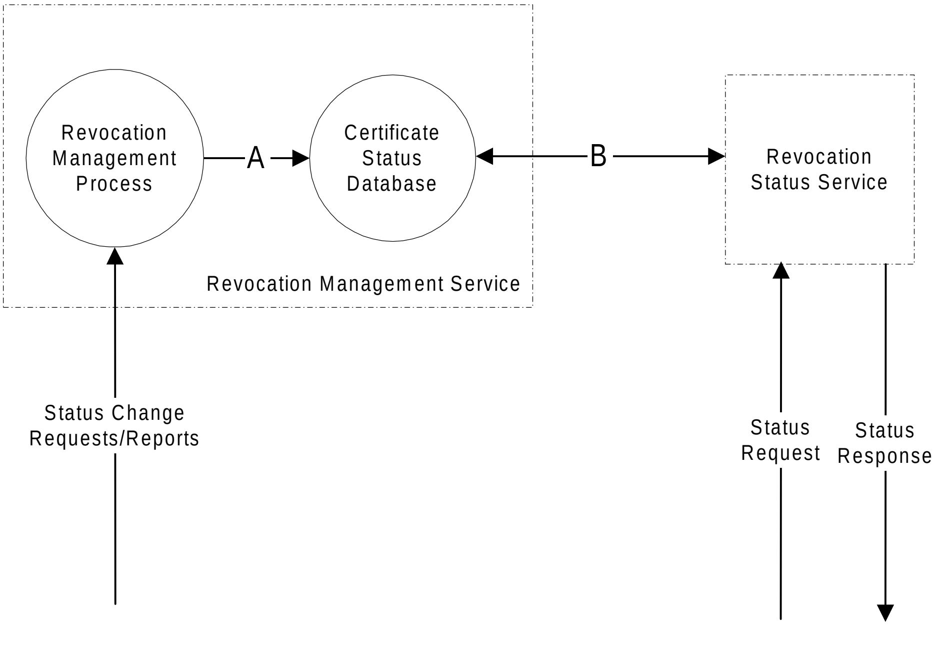
Revocation Management Process
A
Certificate Status Database
B
Revocation Status Service
Revocation Management Service
Status Change Requests/Reports
Status Request
Status Response

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

4.2 CSP Optional Supplementary Services

The supplementary services a CSP may provide are:

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

Note: examples of this service are:

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

It is important to note that this service may provide a SCDev 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 [Dir.1999/93/EC]. No distinction is made whether the SCDev/SSCD is implemented in hardware or software.

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

Within this 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.

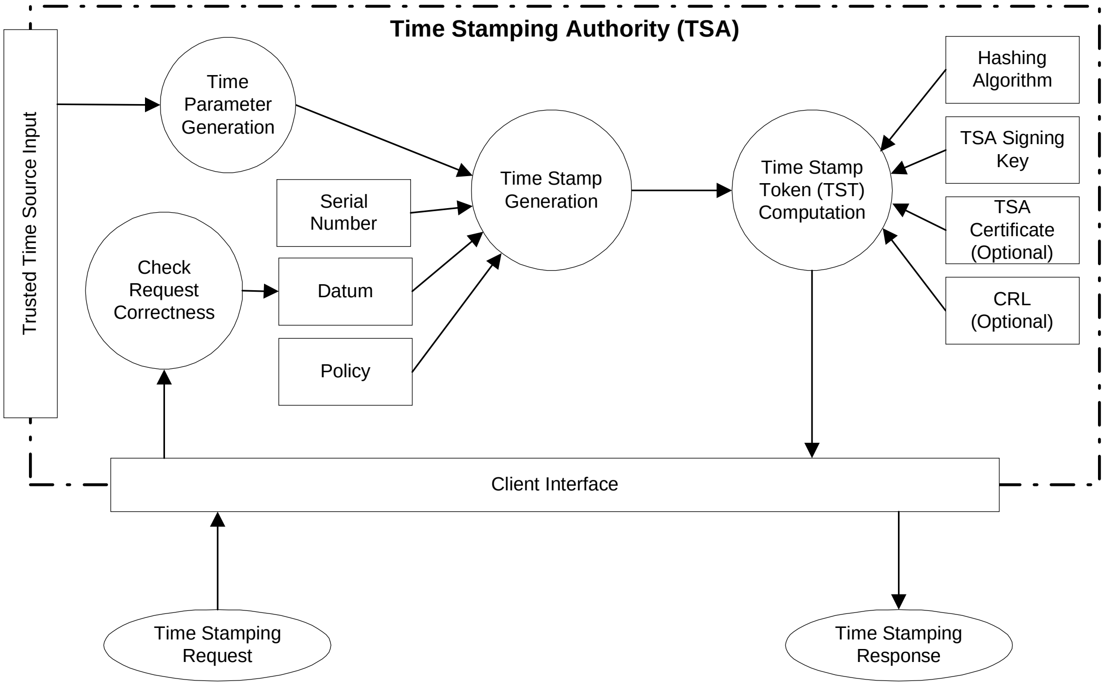
Time Stamping Authority (TSA)
Trusted Time Source Input
Time Parameter Generation
Check Request Correctness
Serial Number
Datum
Policy
Time Stamp Generation
Time Stamp Token (TST) Computation
Hashing Algorithm
TSA Signing Key
TSA Certificate (Optional)
CRL (Optional)
Client Interface
Time Stamping Request
Time Stamping Response

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

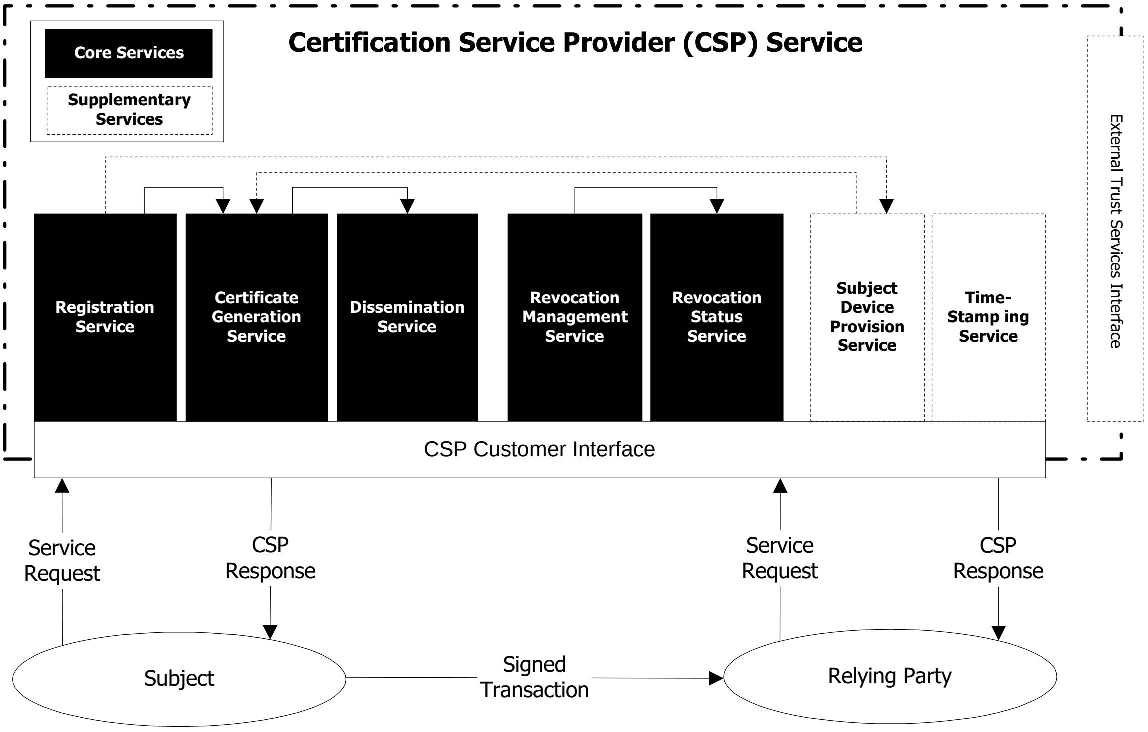

Figure 4 - CSP Logical Architecture

As shown, the CSP provides initial registration and certificate generation as well as subsequent dissemination. Primary certificate lifecycle management (where no revoked or suspended states exist) is provided by way of the Registration, Certificate Generation and Dissemination Services. Secondary certificate lifecycle management, where exceptional certificate states exist (e.g. revoked or suspended states), is provided by the Revocation Management and Revocation Status Services.

The CSP Customer Interface provides access to the CSP's services by Subjects 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 [Dir.1999/93/EC], 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 [Dir.1999/93/EC], Article 5.1
   - Used for Advanced Electronic Signatures (AES) which are created by a Signature-Creation Device (SCDev)

Effectively all security requirements in this CWA are necessary for TWSs issuing QCs, whereas TWSs issuing NQCs can meet a subset 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.

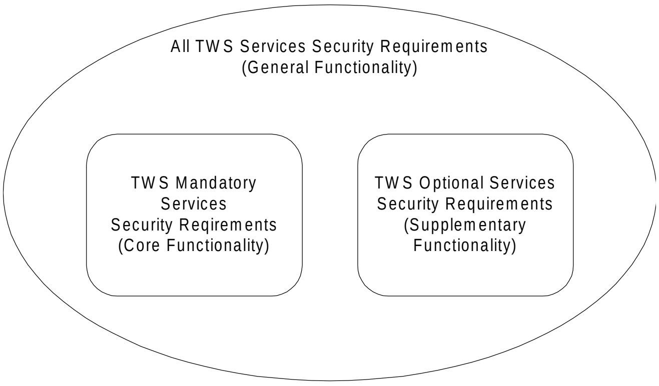
All TWS Services Security Requirements
(General Functionality)
TWS Mandatory Services Security Reqirements (Core Functionality)
TWS Optional Services Security Requirements (Supplementary Functionality)

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 information.

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 or Registration 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 & 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 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 that the CSP's services are quickly and securely restored in case of failure in a TWS.

[SO2.1]

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

- Dissemination Service
- Revocation Management Service
- Revocation Status Service

It is RECOMMENDED that these services provide at least 99.9% availability on a monthly basis.

[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 unacceptable 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 & 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 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 a built-in 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 on 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 and keys for signing certificate status information;

2. Infrastructure Keys – these are keys used by the TWSs for processes such as key agreement, subsystem authentication, audit log signing, encrypting transmitted or stored data, etc. Short term session keys are not 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 in comparison 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 an 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 where justified.

5.1.5.2 Security Requirements

KM1 Key Generation

[KM1.1]

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

[KM1.2]

This secure cryptographic module of [KM1.1] MUST be evaluated and certified to fulfil the following requirements:

- The module MUST ensure the confidentiality and integrity of the keys during their whole life time;
- The module MUST be able to identify and authenticate its users;
- The module MUST restrict access to its services, depending on the user and his role, to those services explicitly assigned to this user and his role;
- The module MUST be able to run a suite of tests to verify that it is operating correctly, and to enter a secure state when it detects an error;
- The module MUST detect attempts of physical tampering and enter a secure state when a tampering attempt is detected;
- The module MUST be able to create audit records for any security-relevant changes;
- The module MAY optionally support backup and restore of keys, but MUST then protect the confidentiality and integrity of the backup data, and require at least dual control for both backup and restore operations.

The evaluation MUST be performed against [CEN CMCSO-PP] or another suitable specification at a comparable assessment level.

[KM1.3]

The secure cryptographic module MUST ONLY generate QC/NQC Signing Keys under at least 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 and Control Keys MUST be generated and maintained in a hardware cryptographic device (HCD.

[KM1.5] – QC ONLY

DELETED

[KM1.6] – QC ONLY

DELETED

[KM1.7]

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

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

KM2 Key Distribution

[KM2.1]

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

[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-Stamping Service) MAY need to be made available to Subjects and Relying Parties. The integrity and authenticity of this public key and any associated parameters MUST be maintained during initial and subsequent distribution.

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

[KM2.5]

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 Certificate Generation 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 Subject Device Provision Service, MUST ensure that subject 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 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 certificates for 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: Should any of the algorithms used in TWSs be considered to have become unsuitable (as specified in [ALGO]), keys based on those algorithms 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 are to be withdrawn from service or transferred their associated 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 be 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).

[KM6.3]

Private/secret Infrastructure and Control Keys MUST be stored in a Hardware Cryptographic Device (HCD).

[KM6.4]

If any private/secret key in a secure cryptographic module or HCD is exported from that module, it MUST be protected by the module, to ensure its confidentiality, 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 that 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 at least under dual-person control.

[KM6.7]

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

KM7 Key Archival

[KM7.1]

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

5.1.6 Accounting & 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 data generation 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 date and time of event, 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 or actual 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 on media appropriate for storage and subsequent processing in providing necessary legal evidence in support of electronic signatures.

[AR1.2]

At a minimum, the following items SHALL be archived:

- 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 & Recovery

Backup and Recovery in this section only covers system information, subject information and all other data necessary to restore the system after a failure or disaster. It does NOT cover backup and recovery of keys, security requirements for which are found in section 5.1.5.

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.

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.

5.2 Core Services 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 Subject has been carried out meeting the requirements specified in the associated Certificate Policy, e.g., [TS101456].

Subject Data Management

The Registration Service by its nature must manage end entity subject 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 subject sensitive information, the certificate request 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 subject to satisfy the requirements for QCs as specified in Annex I of [Dir.1999/93/EC].

[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
- Information Publication Control – to allow subjects to control the Certificate Generation Service's publication of the QC via the Dissemination Service

[R1.6]

Certificate requests from the Registration Service MUST be digitally signed for authentication and data integrity using its Infrastructure or Control Keys.

R2 Subject Data Management

[R2.1]

TWSs SHALL implement mechanisms and security controls to protect the privacy and confidentiality of Subject 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 Subject’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 made available via the Dissemination Service, via the supplementary Subject Device Provision Service or to the Subject directly.

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

Certificate Renewal

During the period prior to the expiration of the certificate, such period being defined by applicable 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 Subject 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 subjects 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 certificate request 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]

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

1. Indication of the subject's name or pseudonym. Where a pseudonym is used this MUST be clearly indicated;
2. The public key in the certificate is related to the subject's private key;
3. The advanced electronic signature of the CSP, created using the CSP 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 certificate SHALL specify a *valid from time* that does not precede the current time and a *valid until time* that does not precede the *valid from time*;
6. The signature algorithms/keys used by the TWS to sign the certificate MUST be conformant to the algorithm specifications standard [ALGO];
7. Reference to the Certificate Policy under which the certificate is issued.

[CG1.6] – QC ONLY

All QCs issued by a TWS MUST conform to [TS101862].

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 by out-of-band means.

[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]

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

Note: It is RECOMMENDED that Subject Certificates be renewed prior to their expiry as the messaging between CSP and subject can be secured using the old keys/certificates. A TWS MUST reject a renewal request signed with an expired or revoked key.

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 that:

- Authentication and integrity of messages are 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]

(Deleted) Subject

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 Subject Certificates;
- All events relating to cross-certification.

5.2.4 Dissemination Service

5.2.4.1 Security Requirements

D1 Dissemination Management

[D1.1]

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

[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 Subjects and to authorised entities according to the rules defined by the Subject 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 Subject determines that 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 Subject.

Where the Subject knows for certain that 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, reinstating and revocation MUST be suitably authenticated and validated.

[RM1.3]

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

[RM1.4]

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

[RM1.5]

Status changes MUST ONLY be instigated by authenticated:

- CSP Security Officers for Infrastructure/Control Certificates;
- Registration/Security Officers for Subject Certificates;
- Subjects for their own certificates.

Note: As determined by policy, a Subject's Certificate may be revoked/suspended/ unsuspended by a third party (e.g. employer of a Subject) by sending a suitable request to the 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 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 Revocation Status Service MUST be updated at least on a daily basis;
- For an online status repository (e.g. OCSP responder) the 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, and the time of status change;
- 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 channel (Fig1: Message B) MUST exist between the Revocation Management Service and the Revocation Status Service;
- This trusted channel 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, based on status change requests either from the Subject, from the CSP, or from a third party, and processed by the Revocation Management Service. This data may also be made available to Subjects if policy requires Subjects to have access to revocation status data.

Status Request/Response

A Relying Party having obtained the certificate(s) from the Dissemination Service, 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 that 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]

(Deleted)

[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 event MUST be logged by an 'online' Revocation Status Service:

- All certificate status requests and responses.

5.3 Supplementary Services Security Requirements

5.3.1 Time-Stamping Service

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

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

Figure 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 Token Generation.

Time Parameter Generation

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

Time-Stamp Token Generation

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

Time-Stamp Token Computation

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

5.3.1.2 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 verify that the request for time-stamping uses a hash algorithm that is specified as approved 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 Token (TST) Generation

[TS3.1]

The Serial Number used within the TST 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 TST MUST include the accuracy of the time source used if this is exceeds 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 TST 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 TST 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 § 5.1.5– Key Management, the following security requirements are applicable and in some cases supersede the requirements specified in §5.1.5 – 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 fulfil the requirements of KM 1.2.

[TS4.3]

TSA Control Keys MUST be stored in a hardware cryptographic device (HCD).

[TS4.4]

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

[TS4.5]

The TSA SHALL ensure that the TST 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.

TS6 Time-Stamping Service Archiving

[TS6.1]

All Time-Stamp Tokens MUST be archived in accordance with [AR 1.1].

5.3.2 Subject Device Provision Service

5.3.2.1 Functional Requirements

SCDev Preparation

The CSP’s TWS prepares the SCDev by performing the necessary initialisation, formatting and, if applicable, file structure creation.

The TWS either:

- Creates the private/public key pair and loads the private key into the SCDev, or;

- If applicable, commands the SCDev to generate the key pair inside the SCDev.

SCDev Provision

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

Activation Data Creation & Distribution

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

5.3.2.2 Security Requirements

SP1 SCDev Preparation

[SP1.1]

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

[SP1.2]

(Deleted)

[SP1.3]

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

[SP1.4]

Where a SCDev 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 SCDev, the cryptographic module generating the key pairs MUST be evaluated and certified to comply either with [CENSSCD] or the following requirements:

- The module MUST ensure the confidentiality and integrity of the keys so long as they are under the control of the module;
- The module MUST ensure the confidentially of private keys transferred from the module to a SCDev;
- The module MUST ensure the integrity of public keys exported to other systems or applications;
- The module MUST be able to identify and authenticate its users;
- The module MUST restrict access to its services;

- The module MUST be able to run a suite of tests to verify that it is operating correctly, and to enter a secure state when it detects an error;
- The module MUST detect attempts of physical tampering and enter a secure state when a tampering attempt is detected.

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

[SP1.6]

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

[SP1.7]

After a cryptographic device generates a key pair for a SCDev and achieves successful transfer to that SCDev, the key pair MUST be securely destroyed in conformance with requirement KM 5.4.

SP2 SCDev Provision

[SP2.1]

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

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 cannot misuse the SCDev at any time.

This MAY be achieved either through:

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

SP4 Subject Device Provision Service Audit

[SP4.1]

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

6 Conformity Assessment

Conformity assessment guidance can be found in [CWA 14172-3].

(Chapter deleted)