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

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

Contents 2
Foreword 3
Executive Summary 4
Introduction 5
1 Scope 7
1.1 General 7
1.2 European Directive-specific 7
2 References 9
2.1 Normative References 9
2.2 Informative References 9
3 Definitions and Abbreviations 10
3.1 Definitions 10
3.2 Abbreviations 13
4 Description of a Certification Service Provider System 14
4.1 CSP Core Services 15
4.2 CSP Optional Supplementary Services 16
4.3 Overall Architecture 17
4.4 Security Levels 18
5 Security Requirements 19
5.1 General Security Requirements 20
5.1.1 Management 20
5.1.2 Systems & Operations 21
5.1.3 Identification & Authentication 22
5.1.4 System Access Control 23
5.1.5 Key Management 23
5.1.6 Accounting & Auditing 29
5.1.7 Archiving 31
5.1.8 Backup & Recovery 32
5.2 Core Services Security Requirements 33
5.2.1 General 33
5.2.2 Registration Service 33
5.2.3 Certificate Generation Service 35
5.2.4 Dissemination Service 37
5.2.5 Certificate Revocation Management Service 38
5.2.6 Certificate Revocation Status Service 40
5.3 Supplementary Services Security Requirements 42
5.3.1 Time-Stamping Service 42
5.3.2 Subject Device Provision Service 44
6 Conformity Assessment 47

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:

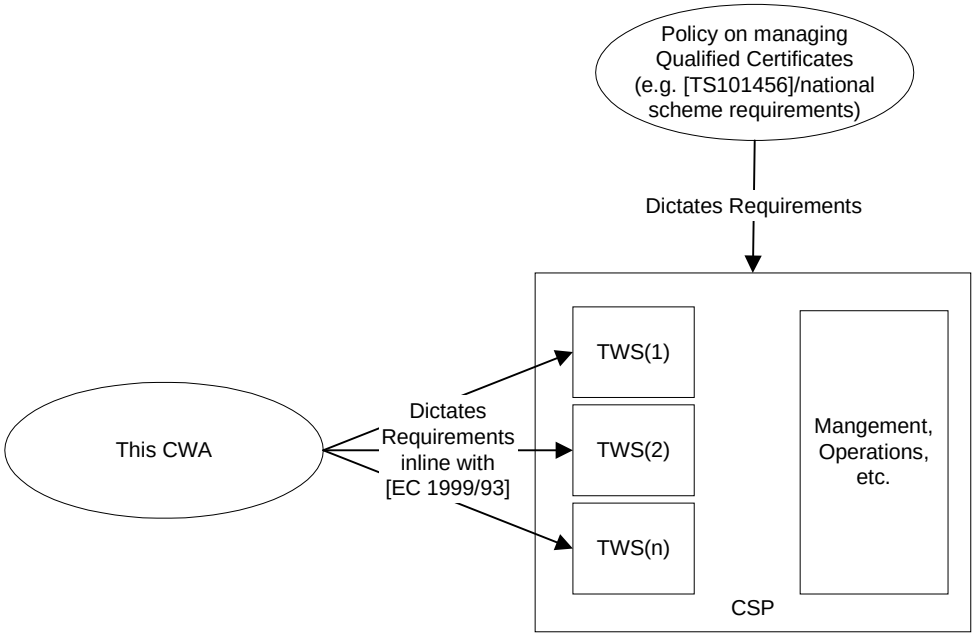

Figure 1 - Relationship between Policy and this CWA

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.