

CEN

CWA 14170

WORKSHOP

May 2004

AGREEMENT

ICS 03.160; 35.040

Supersedes CWA 14170:2001

English version

Security requirements for signature creation applications

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, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, 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

Contents

Contents.....	2
Foreword.....	5
Introduction.....	6
1. Scope.....	7
2. References.....	8
3. Definitions.....	9
4. Abbreviations.....	11
5. Signature Creation Functional Model.....	12
5.1 Signature Creation Objectives.....	12
5.2 Model.....	12
5.3 Signature Creation Applications.....	14
5.4 Secure Signature Creation Devices.....	15
5.5 Signature Creation Application Instantiation.....	16
5.6 Control and possession of Signature Creation Systems.....	16
6. Signed Data Object Information Model.....	17
6.1 Signer's Document (SD).....	17
6.2 Signature Attributes.....	18
6.3 Data To Be Signed (DTBS).....	18
6.4 Data To Be Signed (Formatted) (DTBSF).....	19
6.5 Data To Be Signed Representation (DTBSR).....	19
6.6 Advanced Electronic Signature.....	19
6.7 Qualified Electronic Signature.....	19
6.8 Signed Data Object.....	19
6.9 Signer's Authentication Data (not shown).....	19
7. Overall Security Requirements of the SCA.....	20
7.1 Introduction.....	20
7.2 Trusted Path.....	20
7.2.1 Basic Trusted Path Requirement.....	20
7.2.2 Requirements for Public SCA.....	20
7.2.3 Referencing the correct SD and Signature Attributes.....	20
7.3 Requirements for Distributed Signature Creation Applications.....	21
7.4 Requirements resulting from un-trusted processes and communications ports.....	21
7.5 Post signature verification of the Signed Data Object.....	22
7.6 Requirements of the DTBS.....	22
8. SD Presentation Component (SDP).....	23
8.1 Purpose.....	23
8.2 Background.....	23
8.3 Data Content Type Requirements.....	24
8.4 SD Non-ambiguity Requirements.....	25
8.5 Requirements for Presentation Insensitive SDs.....	25
8.6 Hidden Text and Active Code Requirements.....	25
9. Signature Attribute Viewer (SAV).....	27
10. Signer Interaction Component (SIC).....	29
10.1 High level user interface principles.....	29
10.2 Signature Invocation.....	29
10.3 Signature process inactivity timeout.....	30
10.4 Signer Control Functions.....	30
10.5 Retrieval of Signer's Characteristics.....	30
10.6 User Interface Aspects.....	31

11.	Signer's Authentication Component (SAC)	32
11.1	General Aspects	32
11.2	Obtaining the Signer's Authentication Data	32
11.3	Knowledge based Signer Authentication	33
11.4	Biometric Signer Authentication	33
11.5	Provision of the wrong Signer's Authentication Data	34
11.6	Change of Signer's Authentication Data and Reset of the Retry Counter	34
11.7	Signer's Authentication Data User Interface Aspects	34
11.8	Security Requirements for the SAC Component	34
12.	Data To Be Signed Formatter (DTBSF)	37
12.1	Functions of the DTBSF component	37
12.2	Security Requirements for the DTBSF component	37
13.	Data Hashing Component (DHC)	38
13.1	Functions of the DHC Component	38
13.2	Production of the DTBS Representation	38
13.3	Formatting of the electronic signature input	39
13.4	Security Requirements for the DHC Component	40
14.	SCDev /SCA Communicator (SSC)	41
14.1	Interaction Sequences	41
14.2	Establishing the Physical Communication	42
14.3	Retrieval of SCDev Token Information	42
14.4	Selection of the SCDev functionality on a multi-application platform	44
14.5	Retrieval of Certificates	44
14.6	Selection of Signature Creation Data	44
14.7	Performing Signer Authentication	44
14.8	Digital Signature Computation	45
14.9	Signature Logging	45
14.10	Security requirements for the SSC Component	45
15.	SCD/SCA Authenticator (SSA)	46
15.1	SCA - SCDev Authentication for SCA under service provider's control	46
15.2	Security Requirements for the SSA Component	47
16.	SD Composer (SDC)	48
16.1	Security Requirements for the SDC Component	48
17.	Signed Data Object Composer (SDOC)	49
18.	External Interface for Input/Output	50
18.1	Risks to the SCA	50
18.2	Import of Certificates	50
18.3	Import of an SD and Signature Attributes	50
18.4	Download of SCA Components	50
18.5	Security Requirements for Input Control	51
Annex A	(Informative) – General Recommendations	52
A.1	Operation of the Signature Creation Application	52
A.2	Requirement on the environment	53
A.3	Presentation insensitive SD	53
Annex B	Guidance to implement a User Interface	54
B.1	Purpose	54
B.2	User interface consistency	54
B.3	Use of colour	54
B.4	Feedback	54
B.5	Security Breach detection	55
B.6	Invalid choice	55
B.7	Preservation of information presentation	55
B.8	Personalisation	55
B.9	Signer's Control when integrating with user profiling techniques	55
B.10	Configure /Edit Signature Creation process	55
B.11	Distinguishing between certificates	55

B.12	Timing of operations.....	56
B.13	Security of terminals in public domain	56
B.14	User retention of secrets	56
B.15	User instructions.....	56
B.16	Presentation of operational sequence	56
B.17	Presentation of distinguishable parts	57
B.18	Guidance.....	57
B.19	Terminology.....	57
B.20	Error tolerance	57
B.21	Informative error messages	57
B.22	Single handed operation of public SCAs.....	57
B.23	Cancellation of operation.....	57
B.24	Undo operation.....	58
B.25	Signer's Authentication Component (SAC).....	58
B.25.1	Choice of signer authentication method	58
B.25.2	Biometric signer authentication	58
Annex C	Signature Logging Component (SLC)	60
Annex D	(Informative) - SCDev Holder Indicator (SHI).....	61
Annex E	(Informative) - References.....	62

Foreword

Successful implementation of European Directive Dir. 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 specify security requirements and recommendations for Signature Creation Applications. The CWA is intended for use by developers and evaluators of a Signature Creation Application and of its components.

This version of this CWA [Part] was published on May 2004.

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

This document supersedes CWA 14170:2001.

Introduction

This document specifies security requirements and recommendations for Signature Creation Applications.

Sections 3 to 7 contain the definitions, modelling and technical introductions to the Signature Creation Application that are necessary to support the specification of security requirements. They do not contain requirements.

Sections 8 to 19 specify the security requirements for each functional component of a Signature Creation Application together with their rationale. Security requirements are always expressed in tabular form.

Annexes detail recommendations, and any supportive rationale.

Guidance on how to conduct a conformity assessment on applications and/or processes claiming conformance with this document is provided in CWA 14172-4 "EESSI Conformity Assessment Guidance: Part 4 - Signature creation applications and procedures for electronic signature verification".

1. Scope

This document specifies security requirements and recommendations for Signature Creation Applications that generate advanced electronic signatures by means of a hardware signature-creation device. It is not required that they are based on a qualified certificate.

The signature-creation device (SCDev) addressed by this document must be implemented in a separate piece of physical hardware, with its own processing capabilities for PIN code verification and for performing cryptographic functions. Unless otherwise specified, this SCDev needs not be a secure-signature-creation device (SSCD), i.e. an SCDev that has been assessed as compliant with the requirements set in the Annex III of the EU Directive [Dir. 1999/93/EC].

Therefore advanced electronic signatures which are created by a signature creation application compliant with the requirements of this document fall under the provisions of Art 5.2 of the EU Directive [Dir. 1999/93/EC].

If, instead, an advanced electronic signature, that is produced with a Signature Creation Application conformant with the security requirements and recommendations specified in this document, is also based on a qualified certificate and is created by a secure-signature-creation device, that electronic signature is a Qualified Electronic Signature that complies with the provision of Art. 5.1 of the EU Directive [Dir. 1999/93/EC].

This document:

- provides a model of the Signature Creation Environment and a functional model of Signature Creation Applications;
- specifies overall requirements that apply across all of the functions identified in the functional model;
- specifies Security Requirements for each of the functions identified in the Signature Creation Application excluding the Signature Creation Device.

A Signature Creation Application is intended to deliver to the user or to some other application process in a form specified by the user, an Advanced, or where applicable a Qualified, Electronic Signature associated with a Signer's Document as a Signed Data Object.

This document is intended to be independent of particular technologies that might be employed in products. The following aspects are considered to be out of scope:

- generation and distribution of Signature Creation Data (keys etc.), and the selection and use of cryptographic algorithms;
- the legal interpretation of any form of signature (e.g. the implications of countersignatures, of multiple signatures and of signatures covering complex information structures containing other signatures).

This document specifies security requirements that are intended to be followed by implementers of SCAs.

2. References

The following documents contain provisions which, through reference in this text, constitute provisions of this standard.

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

For a specific reference, subsequent revisions do not apply

For a non-specific reference, the latest version applies.

- [1]. ETSI TS 101 733 – Electronic Signature Formats;
- [2]. PKCS#15: Cryptographic Token Information Standard;
- [3]. EN 1332-4 Identification card Systems: Man-Machine Interface – Part Four “Coding of user requirements”;
- [4]. EC Directive Dir. 1999/93/EC of the European Parliament and the council of 13 December 1999 on a Community framework for electronic signatures;
- [5]. CWA 14169 - Secure Signature-Creation Devices, version 'EAL 4+';
- [6]. CWA 14171 - Procedures for Electronic Signature Verification;
- [7]. ETSI SR 002 176 – Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures;
- [8]. ETSI TS 101 903 – XML Advanced Electronic Signatures (XAdES).