CEN

WORKSHOP

AGREEMENT

CWA 14170

May 2004

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

Ref. No.:CWA 14170:2004 E

Contents

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).