National Standards Authority of Ireland

TECHNICAL GUIDE

I.S. CWA 14365-1:2004

ICS 03.160
35.040
35.240.60

National Standards
Authority of Ireland
Dublin 9
Ireland

Tel: (01) 807 3800
Fax: (01) 807 3838

GUIDE ON THE USE OF ELECTRONIC SIGNATURES - PART 1: LEGAL AND TECHNICAL ASPECTS

This Irish Standard was published under the authority of the National Standards Authority of Ireland and comes into effect on:

May 12, 2004

Price Code J

Údarás um Chaighdeáin Náisiúnta na hÉireann

CEN

WORKSHOP

AGREEMENT

CWA 14365-1

March 2004

ICS 03.160; 35.040; 35.240.60

Supersedes CWA 14365:2003

English version

Guide on the Use of Electronic Signatures - Part 1: Legal and Technical Aspects

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 14365-1:2004 E

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 recognized 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 recognized standards. The present document is one such CWA.

The purpose of this CWA is to give guidance on the use of electronic signatures. Whilst the focus often has been on "qualified electronic signatures" as specified in Article 5.1 of the Directive, a side effect was that the requirements of employing general electronic signatures (referred to as "5.2 signatures") in e-commerce were not sufficiently addressed.

The purpose of this part of the CWA is therefore to describe the general legal and technical aspects of electronic signatures, and thus extend the work to e-commerce scenarios, paying special attention to technologies with a high deployment capacity, to enable trust, without the need to meet all the strict requirements for "Article 5.1 Signatures".

This part of the CWA is intended for use by both legal and technical experts in the area of electronic signatures, as well as designers of systems and products in this area.

The CWA consists of the following parts:

- Part 1 - Legal and technical aspects (this part)
- Part 2 - Protection Profile for Software Signature-Creation Devices

This version of this CWA Part was published 2004-03.

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.

1 Scope

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] – referred to as the Directive in the remainder of this document – established a legal framework for electronic signatures and certification-services in order to contribute to their legal recognition. It is laid down in article 5.1 that electronic signatures fulfilling certain quality metrics – so called qualified electronic signatures – satisfy the requirements of handwritten signatures. In article 5.2 a residual provision is given where electronic signatures are not denied legal effectiveness and admissibility as evidence in legal proceedings, even if the quality metrics of qualified electronic signatures are not met.

The scope of this document is on the latter –electronic signatures that do not fulfil all the requirements laid down for qualified electronic signatures in article 5.1 of the Directive. The document therefore analyses the differences between cryptographic mechanism of digital signatures, qualified electronic signatures (according to article 5.1 of the Directive), and electronic signatures (according to article 5.2 of the Directive). In addition, a set of use cases of electronic signatures which do not fulfil some of the requirements laid down in article 5.1 are discussed in order to point out its effectiveness in e-commerce environments or in various application fields asking for authentication measures.

In addition to the use cases, the evidence that is provided by electronic signatures is discussed. The electronic signatures and certification-services are broken up into its basic elements and the proof provided by each element is discussed from a legal perspective in order to establish the coherence between the technical elements and its legal effect.

Part 2 of this CWA contains a Protection Profile (PP) for a Software Signature Creation Device [SCDev-PP] suitable for such general electronic signatures. This Protection Profile follows the provision of the Common Criteria (CC) [ISO 15408]. It is based on the [SSCD PP] that has been developed as a standard for devices that are capable of creating qualified electronic signatures.

Although a CC PP has been chosen for highlighting the added value of independent evaluation of the security measures provided by the SCDev, other evaluation criteria may serve that purpose as well. Examples of such criteria are [FIPS 140-2] or [ITSEC].