CEN

WORKSHOP

AGREEMENT

CWA 14171

May 2004

ICS 03.160; 35.040

Supersedes CWA 14171:2001

English version

General guidelines for electronic signature verification

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 14171:2004 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 specify general guidelines and recommendations for Electronic Signature Verification. The CWA is intended for use by developers and evaluators of a Signature Verification Application and of its components.

This version of this CWA 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 to purchasers from the CEN Central Secretariat.

This document supersedes CWA 14171:2001.

Introduction

Although there are no formal requirements for signature verification specified in Dir.1999/93/EC[1], Annex IV (the text of which is reproduced in Annex A of this present CWA) recommends that:

"During the signature-verification process it should be ensured with reasonable certainty that:..."

Thus, in order to achieve this "*reasonable certainty",* there is a need for general guidelines on signature verification procedures, including both the products used for verification, and their management.

Signature verification is a process that can be performed in many ways, for example:

- by a natural person, using his workstation and accompanying software to request verification of a received signature,
- by a computer program, using an automated procedure.

Dir.1999/93/EC [1] mentions "data displayed to the verifier", which might be interpreted as verification by a natural person. However, the second case will be useful in electronic commerce, and guidelines are also needed for automated signature verification. Also, the term "displayed" should be interpreted in a more general sense as "presented", since the signed data may be any type of media (text, sound, video etc).The following are the major parties involved in a business transaction supported by electronic signatures:

- Signer,
- Verifier,
- Certification Service Provider,
- Arbitrator.

The **Signer** is the entity which creates the electronic signature.

The **Verifier** is the entity which verifies the electronic signature, it may be a single entity or multiple entities.

The **Certification Service Providers** (CSPs) are one or more service providers which help to build trust relationships between the signer and verifier. They may be used by the signer and verifier to assist them in performing their tasks.

The **Arbitrator** is an entity able to arbitrate disputes between a signer and a verifier.

The signer must provide at least a basic form of Electronic Signature. This basic form does not protect against all potential threats caused by signers' certificates revocation, certificate issuer signing key revocation, signing algorithms and/or keylength weakening, etc., which can undermine the signature reliability. An advantage of this basic form is that it can be created without accessing on-line ancillary services. Moreover, a basic electronic signature may be sufficient in the case of some short-lived transactions, i.e. a signature a party will rely upon within a few hours, before the next useful revocation information is made available. This form is however insufficient to settle disputes in the long term. In order to provide long term verification properties some additional information need to be captured after the electronic signature has been generated. In order to differentiate between these differing circumstances this CWA uses two distinct terms: Initial Verification, and Subsequent Verification.

An **Initial Verification** must be performed within a suitable time after an electronic signature has been generated, in order to capture additional information that will support later verification, potentially over long timescales. The information to be captured and held will relate to the signer's certificate status and validity at the time of the signature and additional information whose capture must be delayed to allow for the 'pipeline' effect of any system processes, e.g. for the promulgation of a revocation decision.

If such data are correctly collected, **Subsequent Verifications** may be successfully performed years after the electronic signature was produced. In order to be able to perform a Subsequent Verification there should be no need to capture more data than those captured at the time of the Initial Verification. Exceptions are, for example, the revocation status of a TSU certificate and additional data acquired for archiving purposes. For

an archive system more data may need to be subsequently captured if the cryptography that was used at the time of the signature is no longer considered to be strong enough to protect the archived data.

This document identifies those data that need to be captured and archived so that they can be later used for arbitration, should a dispute occur between the signer and a verifier. This document also identifies the security requirements for the various elements of a signature verification system.

In order to contribute to the interests of the consumers, i.e. consumer confidence and trust in electronic signatures, the signature verification interface should be as easy to perform and no more difficult to accomplish than is the verification of a hand written signature. It should reduce the probability of human errors and be accessible to most users. This document provides recommendations for the use of the interface and guidance on organisational measures to achieve this confidence.

The present document does not specify how the requirements identified may be assessed by an independent party, nor does it address the requirements for information to be made available to such independent assessors, or requirements upon such assessors. These are addressed in CWA 14172-4 "EESSI Conformity Assessment Guidance: Part 4 - Signature creation applications and general guidance for electronic signature verification".

1. Scope

This document sets out general guidelines on the recommended functionality and assurances for electronic signature verification, in the light of the recommendations in Annex IV from [Dir.1999/93/EC]and in the interest of the consumer.

Its primary purpose is to provide guidance on the way to verify qualified electronic signatures that are equivalent to handwritten signatures according to Article 5.1 of Dir.1999/93/EC [1] , and to complement them with additional data that may help in assessing their validity long after their signing time. Signatures with such additional data have been called “Enhanced Electronic Signatures”.

2. References

[1]. DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

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

[3]. ETSI TS 101 733: Electronic Signature formats

[4]. ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES)

[5]. ETSI TS 101 456: Policy requirements for Certification Authorities issuing qualified certificates

[6]. ETSI TS 101 862: Qualified Certificate Profile

[7]. ETSI TS 102 231: Requirements for Trust Service Provider status information

[8]. RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP

[9]. RFC 3280: PKIX Certificate and CRL Profile

[10]. RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

[11]. ISO/IEC 9594-8 – Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks