Irish Standard Recommendation
S.R. CEN/TS 419241:2014

Security Requirements for Trustworthy Systems Supporting Server Signing

S.R. CEN/TS 419241:2014

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:	*Published:*
CEN/TS 419241:2014	2014-03-26

This document was published under the authority of the NSAI and comes into effect on:	ICS number:
2014-04-05	35.240.99
	NOTE: If blank see CEN/CENELEC cover page

NSAI	T +353 1 807 3800	Sales:
1 Swift Square,	F +353 1 807 3838	T +353 1 857 6730
Northwood, Santry	E standards@nsai.ie	F +353 1 857 6729
Dublin 9	W NSAI.ie	W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 419241

March 2014

ICS 35.240.99

English Version

Security Requirements for Trustworthy Systems Supporting Server Signing

Exigences de sécurité pour des systèmes fiables de serveur de signature électronique

Sicherheitsanforderungen für Vertrauenswürdige Systeme, die Serversignaturen unterstützen

This Technical Specification (CEN/TS) was approved by CEN on 14 October 2013 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TS 419241:2014 E

Contents

Page

Foreword

This document (CEN/TS 419241:2014) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by AFNOR.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

Successful implementation of European Directive 1999/93/EC on a community framework for electronic signatures 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 Standardization Initiative (EESSI).

Within this framework the Comité Européen de Normalisation / Information Society Standardization 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 Directive 1999/93/EC and the development of a European electronic signature infrastructure.

This document will describe security requirements for a server-side system using certificates in order to create advanced electronic signatures (AdES) in accordance with the requirements of the European Directive on Electronic Signature 1999/93. The signature is to be supported by a qualified certificate, or other public key certificate issued for the purposes of signing, issued by a Trust Services Provider (TSP) operating to recognized good practices (e.g. ETSI EN 319 411-3 (aka ETSI/TS 102 042) or ETSI EN 319 411-2 (aka ETSI/TS 101 456)). The document will include requirements for the use of the appropriate protection profiles for the Signature Creation Device (SCDev).

The purpose of the trustworthy system is to produce an advanced electronic signature created under sole control of a natural person, or a legal person (such advanced electronic signatures produced by legal persons are called electronic seals).

The Signature Generation Service Provider (SGSP) operates the trustworthy system in an environment with a security policy which incorporates general physical, personnel, procedural and documentation security requirements as defined in ETSI EN 319 411-2 / ETSI EN 319 411-3.

This document is identified as CEN/TS 419241 within the Rationalised Framework for Electronic Signature Standardization ETSI SR 001 604.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

The European Directive 1999/93/EC establishes a framework of requirements for the use of electronic signatures. This Directive also introduces the notion of advanced electronic signature which is defined as legally equivalent to a hand-written one if generated by a physical person using a qualified certificate stored in a Secure Signature Creation Device (SSCD).

Since the publication of the Directive, other forms of electronic signatures have appeared in order to meet market needs (e.g. e-Invoicing, e-Procurement). These other forms do not necessarily require the use by a natural or legal person of a secure signature creation device and/or qualified certificate.

One of these forms is an electronic signature created using a networked server. The Signature Creation Data (SCD) is under control of an individual user but held centrally within a shared server, instead on a secure signature creation device held by the signatory.

It is not the intent of this standard to limit the type of public key certificate, qualified or otherwise, used by the networked signing server.

The main objective of this standard is to define requirements and recommendations for a networked signing server which may process electronic certificates used by natural or legal persons for electronically signing documents.

This document specifies basic requirements for server signing. Additional specifications may be issued which provide more detailed requirements. For further details see ETSI SR 001 604.

1 Scope

1.1 General

This document specifies security requirements and recommendations for Trustworthy System Supporting Server Signing (TW4S) that generate advanced electronic signatures as defined in Directive 1999/93/EC. This document may also be applied to electronic signatures complying to Article 5(1) of Directive 1999/93/EC employing a Secure Signature Creation Device (SSCD) compliant with Annex III and supported by a qualified electronic signature.

The Server Signing Application (SSA) runs on a networked server supporting one or more signatories to remotely sign electronic documents using centralized signature keys held on the signing server under sole control of the signatory.

An SSA 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:

— provides commonly recognized functional models of TW4S;

— specifies overall requirements that apply across all of the services identified in the functional model;

— specifies security requirements for each of the services identified in the SSA.

— specifies security requirements for sensitive system components which may be used by the SSA (e.g. Signature Creation Device (SCDev)).

This document does not specify technologies and protocols, but rather identifies requirements on the security on technologies to be employed.

1.2 Out of scope

The following aspects are considered to be out of scope:

— other trusted services that may be used alongside this service such as signature validation service, time-stamping service and information preservation service,

— any application or system outside of the SSA,

— 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).

1.3 Audience

This document specifies security requirements that are intended to be followed by:

— providers of SSA systems.

— Trust Service Providers (TSP) offering signature generation service.