TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 419261

March 2015

ICS 03.120.20; 35.040; 35.240.30

English Version

Security requirements for trustworthy systems managing certificates and time-stamps

Exigences de sécurité pour systèmes de confiance gérant des certificats et des horodatages

Sicherheitsanforderungen für vertrauenswürdige Systeme zur Verwaltung von Zertifikaten für elektronische Signaturen und Zeitstempel

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 419261:2015 E

Contents

Page

2

Foreword

This document (CEN/TS 419261:2015) 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.

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 [Dir.1999/93/EC] and of REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [Reg.910/2014/EU] 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.

NOTE   According to Article 50 of Reg.910/2014/EU Directive 1999/93/EC is repealed with effect from 1 July 2016 and references to the repealed Directive shall be construed as references to the Regulation.

In 1999 the European Information and Communications Technologies 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 Normalization / 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 [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.

In 2011 the European Commission (EC) with the support of the European Free Trade Association has signed a specific grant agreement with the European Committee for Standardization (CEN) regarding the update of the existing European e-Signature CEN Workshop Agreements (CWAs) in the framework of Phase 1 of the mandate M/460. The present document is such a CEN Workshop Agreement that was first created as a CWA and then updated into a Technical Specification (TS).

The purpose of this TS is to describe the security requirements for trustworthy systems managing certificates for electronic signatures and to define overall system security requirements, whereas EN 419221 specifies security requirements for cryptographic devices. The requirements were partly inspired by Common Criteria [CC] Part 2, but the TS is not compliant to [CC], as e.g. EN 419221. In consequence, this TS cannot be used to perform Common Criteria certifications of products.

The TS is intended for use by designers and developers of systems managing certificates and time-stamps, as well as customers of such systems.

Executive Summary

This Technical Specification specifies security requirements on products and technology components, used by Trust Service Providers (TSPs) for issuing and managing certificates as well as electronic time-stamps in the sense of the REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [Reg.910/2014/EU].

The term TSP includes certification service providers (CSPs) issuing qualified certificates as defined in the Directive *"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]. These certificates are used in conjunction with electronic signatures and advanced electronic signatures in accordance with Directive 1999/93/EC [Dir.1999/93/EC]. Additionally, electronic time-stamps issued by a TSP provide evidence that the stamped data existed at a given time.

This Technical Specification contains the same requirements for TWS used by CSPs according to [Dir.1999/93/EC] and for TWS used by TSPs according to [Reg.910/2014/EU]. However, [Reg.910/2014/EU] allows TSPs to manage electronic time-stamps without managing certificates. This is not allowed for CSPs according to [Dir.1999/93/EC]. Therefore, this Technical Specification distinguishes between CSPs and TSPs with respect to the provided services where necessary.

TSPs need to use Trustworthy Systems (TWSs) for securely providing the following services, which are defined in this TS:

a) Registration Service - to verify the identity and, if applicable, any specific attributes of a subject;

b) Certificate Generation Service - to create certificates;

c) Dissemination Service - to provide certificates and policy information to subjects and relying parties;

d) Revocation Management Service - to allow the processing of revocation requests;

e) Revocation Status Service - to provide certificate revocation status information to relying parties;

f) Subject Device Provision Service – to prepare and provide a Signature Creation Device (SCDev) to subjects. This includes Qualifed electronic Signature and Seal Creation Device (QSCD) provision;

g) Time-stamping Service – provides a Time-stamping Service which may be needed for signature verification purposes.

TSP shall follow:

h) "General Security Requirements" specified in 5.2 that are applicable to all previously mentioned services;

i) Security requirements specified in 5.3, 5.4 and 5.5 that are specific to some of the previously mentioned services.

In accordance with Directive1999/93/EC, CSPs need to establish and maintain the first five core services relevant for the issuance and management of qualified certificates (Registration Service, Certificate Generation Service, Dissemination Service, Revocation Management Service, and Revocation Status Service). The other two services (Subject Device Provision Service and Time-stamping Service) are optional ones and are not required to be established and maintained by CSPs, because of having not being specifically addressed in Directive1999/93/EC.

TSPs managing certificates and operating in accordance with Regulation (EU) No 910/2014 [Reg.910/2014/EU] will need to establish and maintain the first five core services relevant for the issuance and management of qualified certificates (Registration Service, Certificate Generation Service, Dissemination Service, Revocation Management Service, and Revocation Status Service). The Subject Device Provision Service is an optional service for such a TSP. TSP managing electronic time-stamps need to establish and maintain the Time-stamping Service relevant for the issuance and management of electronic time-stamps.

TSPs issuing:

j) Certificates according to ETSI/TS 119 411-1 or TS 119 411-2 (or equivalent ENs to be subsequently published) and/or

k)   Time-stamps according to ETSI/TS 119 421 (or equivalent EN to be subsequently published)

may use TWSs that have been independently assessed against the relevant security requirements defined in this Technical Specification and declared as being compliant to these requirements. In this case, TSP may reduce their burden to establish conformance of their policy to the relevant standards and in meeting the requirements of Dir.1999/93/EC and/or [Reg.910/2014/EU].

Guidance for conformity assessment to the security requirements defined in this TS can be found in CWA 14172-3.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement 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 and the Regulation (EU) No 910/2014 [Reg.910/2014/EU] establish a framework of requirements for the use of electronic signatures which are legally equivalent to hand-written signatures. This is the case for "advanced electronic signatures" which are based on a "qualified certificate" and which are created by a "secure-signature-creation device" according to Article 5.1 of 1999/93/EC and qualified signatures according to Article 25.2 of [Reg.910/2014/EU].

In particular, Annex II of Dir. 1999/93/EC and Article 24.2 (e) of [Reg.910/2014/EU] provide the requirements to be followed by TSP when issuing qualified certificates (QCs) and qualified TSP providing qualified trust services. More specifically, they shall

- use trustworthy systems and products which are protected against modification and ensure the technical security of the processes supported by them.

This Technical Specification defines security requirements for TWSs within the scope of the services a TSP needs to provide. It is assumed that TWSs being compliant to relevant security requirements of this TS may be adopted by TSPs to reduce their effort in deploying systems meeting Dir.1999/93/EC and/or [Reg.910/2014/EU]. This approach should support industry in developing systems which meet the requirements laid down in Annex II (f) of Dir.1999/93/EC and in Article 24.2 (e) of [Reg.910/2014/EU].

ETSI TS 119 411-1, 119 411-2, and 119 421 have been taken into account as reference. As a consequence, TWSs already compliant to relevant security requirements of this TS will require minimal configuration by TSPs using them, to meet the security requirements for TWS defined in ETSI TS 119 411-1, 119 411-2, and 119 421 (or equivalent ENs to be subsequently published). In addition, compliant TWS may be used by different TSPs without the need to repeat the conformity assessment.

TWSs for TSPs managing certificates shall comply with the security requirements defined in 5.2 and 5.3 to support TSPs in providing the following core services:

a) Registration of subject information (Registration Service);

b) Certificate generation (Certificate Generation Service);

c) Certificate dissemination (Dissemination Service);

d) Certificate revocation management (Revocation Management Service);

e) Certificate revocation status provision (Revocation Status Service).

TWS for TSPs managing certificates may comply with the other security requirements defined in 5.4 and 5.5 to support TSPs in providing the following supplementary services:

f) SCDev / QSCD production (Subject Device Provision Service);

g) Time-stamping functions (Time-Stamping Service).

TWS for TSPs managing electronic time-stamps shall comply with requirements defined in 5.5 to provide the Time-Stamping Service and may provide the other services, either a) – e) or a) – f) and comply with the corresponding requirements, defined in 5.2 and 5.3 or 5.2, 5.3, and 5.4, respectively.

All security requirements defined in this TS are either:

h) mandatory (indicated by SHALL (NOT) or SHALL (NOT));

i) recommended (indicated by SHOULD (NOT) or (NOT) RECOMMENDED); or

j) optional (MAY or MAY (NOT)).