PD CEN/TS 419221-6:2019

BSI Standards Publication

Conditions for use of EN 419221-5 as a qualified electronic signature or seal creation device

bsi.

National foreword

This Published Document is the UK implementation of CEN/TS 419221-6:2019.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and security devices for personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2019

ISBN 978 0 539 01820 2

ICS 35.040.01; 35.240.30

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2019.

Amendments/corrigenda issued since publication

Date	Text affected

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 419221-6

March 2019

ICS 35.040.01; 35.240.30

English Version

Conditions for use of EN 419221-5 as a qualified electronic signature or seal creation device

Conditions d'utilisation de l'EN 419221-5 en tant dispositif de création de signature ou cachet électronique qualifié

Bedingungen zu lokalen Verwendung von EN 419221-5 als qualifizierte elektronische Signatur- oder Siegelerstellungseinheit

This Technical Specification (CEN/TS) was approved by CEN on 11 February 2019 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, Serbia, 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: Rue de la Science 23, B-1040 Brussels

Ref. No. CEN/TS 419221-6:2019 E

Contents

Page

European foreword

This document (CEN/TS 419221-6:2019) 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 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.

According to the CEN/CENELEC Internal Regulations, the national standards organisations 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, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

EU Regulation N° 910/2014 (eIDAS) on electronic identification and trust services for electronic transactions in the internal market [1] builds on the concept and requirements defined in the earlier EU Directive 1999/93 on Electronic Signatures [i.3]. eIDAS defines an electronic signature which has legal equivalence to handwritten signature. eIDAS defines a variant of the electronic signature called electronic seal. An electronic seal authenticates the origin of data but created under control, as opposed to "sole control" for electronic signatures, of a legal person (e.g. organization), as opposed to natural person (i.e. individual). eIDAS recognizes a special level of qualified electronic signature and seal which is created using a qualified signature creation device (QSigCD) or qualified seal creation device (QSealCD) and supported by a qualified certificate. The requirements for a qualified seal creation device are described to be "mutatis mutandis" as for a qualified signature creation device.

The EN 419221-5 standard states that a conformant cryptographic module is intended to be used as a qualified electronic signatures and seal creation device under Regulation 910/2014 (see Clause 1.2.1) but the scope of the document is aimed at trust service providers. This document aims to give users, implementers and regulators a clear basis for acceptance of EN 419221-5 certified devices for use as a qualified signature creation device or a qualified electronic seal creation device under Regulation 910/2014 even if not operated by a qualified TSP.

Annex A of EN 419221-5:2018 describes how the requirements for a Qualified Signature Creation Device (as defined in Annex II of (EU) No 910/2014) are covered by the standard. The equivalent may also be applied "Mutatis Mutandis" to Qualified Seal Creation Device where the requirements for control are considered to be less stringent ("control" instead of "sole control").

1 Scope

This document specifies conditions for use of an EN 419221-5 certified device in the case the signatory or seal creator has direct local control of the cryptographic module with the aim of being recognized as a qualified seal and/or signature creation device as defined in Regulation EU 910/2014 [1].

This document is aimed at use by entities other than trust service providers. Trust service providers can use EN 419221-5 directly without the need to take into account specific conditions as specified in the present document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 419221-5:2018, *Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services*

3 Terms and definitions

3.1 Terminology

For the purposes of this document the terms and definitions given in EU Regulation N° 910/2014 [1] apply.

The term “seal” is used to denote “Electronic Seal”.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.2 Abbreviations

For the purposes of this document the following abbreviations apply.

QSealCD	Qualified Seal Creation Device
QSignCD	Qualfied Signature Creation Device
QTSP	Qualified Trust Service Provider
eIDAS	electronic Identification, Authentication and Signatures

NOTE This is the informal name used for Regulation 910/2014 [1].