

DIN EN 419212-4

ICS 35.240.15

Ersatzvermerk
siehe unten

Anwendungsschnittstelle für sichere Elemente zur elektronischen Identifikation, Authentisierung und für vertrauenswürdige Dienste – Teil 4: Datenschutzspezifische Protokolle; Englische Fassung EN 419212-4:2018

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services –

Part 4: Privacy specific Protocols;

English version EN 419212-4:2018

Interface applicative des éléments sécurisés pour les services électroniques d'identification, d'authentification et de confiance –

Partie 4: Protocoles spécifiques à la protection de la vie privée;

Version anglaise EN 419212-4:2018

Ersatzvermerk

Mit DIN EN 419212-1:2017-11, DIN EN 419212-3:2017-11 und DIN EN 419212-5:2018-06 Ersatz für die 2017-11 zurückgezogene Norm DIN EN 419212-1:2015-03 und die 2017-11 zurückgezogene Norm DIN EN 419212-2:2015-03

Gesamtumfang 26 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (EN 419212-4:2018) wurde vom Technischen Komitee CEN/TC 224 „Persönliche Identifikation, elektronische Signatur, maschinenlesbare Karten sowie zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat von AFNOR (Frankreich) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Unterausschuss NA 043-01-17-04 UA „Austauschprotokolle bei Chip-Karten“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Dieses Dokument ersetzt DIN EN 419212-1:2015-03 und DIN EN 419212-2:2015-03.

Diese Norm unterstützt Dienste im Zusammenhang mit elektronischer Identifikation, Authentifizierung und Vertrauensdiensten (eIDAS), einschließlich Signaturen.

DIN EN 419212-4 soll die Implementierung des europäischen rechtlichen Rahmens für elektronische Signaturen unterstützen, indem sie die funktions- und sicherheitsbezogenen Anforderungen an sichere Elemente (z. B. Chipkarten) zur Verwendung als qualifizierte elektronische Signaturerstellungseinheit (en: Qualified electronic Signature Creation Device, QSCD) entsprechend den Bedingungen der Europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt definiert.

Ein mit der Norm übereinstimmendes sicheres Element wird in der Lage sein, eine „qualifizierte elektronische Signatur“ (QES) zu erzeugen, die die Artikel der Verordnung zu elektronischen Signaturen erfüllt und daher als zu handschriftlichen Signaturen äquivalent betrachtet werden kann.

Die Normenreihe DIN EN 419212 besteht aus fünf Teilen:

- *Teil 1: Einführung und allgemeine Definitionen* beschreibt die Geschichte, Anwendungszusammenhang, Marktperspektive und eine Anleitung für das Grundverständnis von elektronischen Signaturen. Sie bietet außerdem allgemeine Begriffe und Verweisungen, die für die gesamte 419212 Reihe gültig sind.
- *Teil 2: Signatur- und Siegeldienste* beschreibt Festlegungen für die Signaturerzeugung in Übereinstimmung mit der eIDAS-Verordnung.
- *Teil 3: Geräteauthentisierungsprotokolle* beschreibt die Geräteauthentisierungsprotokolle und die dazugehörigen Schlüsselverwaltungsdienste zur Einrichtung eines sicheren Kanals.
- *Teil 4: Datenschutzspezifische Protokolle* beschreibt Funktionen und Dienste für die Gewährleistung des Datenschutzes bei Identifikationsdiensten.
- *Teil 5: Vertrauenswürdige elektronische Dienste* beschreibt Dienste, die in Verbindung mit den in Teil 2 beschriebenen Signaturdiensten verwendet werden können.

Das Präsidium des DIN hat mit seinem Beschluss 1/2004 festgelegt, dass von dem in den Regeln der europäischen Normungsarbeit von CEN/CENELEC verankerten Grundsatz, wonach Europäische Normen in den drei offiziellen Sprachen Deutsch, Englisch, Französisch veröffentlicht werden, in begründeten Ausnahmefällen abgewichen und auf die deutsche Sprachfassung verzichtet werden kann.

Die Genehmigung dafür hat die DIN-Geschäftsleitung entsprechend den festgelegten Kriterien für die vorliegende Norm auf Antrag des Normenausschusses Informationstechnik und Anwendungen (NIA) erteilt.

Änderungen

Gegenüber DIN EN 419212-1:2015-03 und DIN EN 419212-2:2015-03 wurden folgende Änderungen vorgenommen:

- a) Normenreihe wurde aufgrund der eIDAS-Verordnung umstrukturiert;
- b) in Teil 4 wurden alle datenschutzspezifischen Protokolle aus den Vorgängerdokumenten aufgenommen.

Frühere Ausgaben

DIN EN 14890-1: 2009-03
DIN EN 14890-2: 2009-03
DIN EN 419212-1: 2015-03
DIN EN 419212-2: 2015-03

— Leerseite —

English Version

Application Interface for Secure Elements for Electronic
Identification, Authentication and Trusted Services -
Part 4: Privacy specific Protocols

Interface applicative des éléments sécurisés pour les
services électroniques d'identification,
d'authentification et de confiance - Partie 4 : Protocoles
spécifiques à la protection de la vie privée

Anwendungsschnittstelle für sichere Elemente zur
elektronischen Identifikation, Authentisierung und für
vertrauenswürdige Dienste - Teil 4:
Datenschutzspezifische Protokolle

This European Standard was approved by CEN on 6 February 2017.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

Contents

Page

European foreword.....	3
Introduction	4
1 Scope.....	5
2 Normative references.....	5
3 Introduction	5
3.1 General.....	5
3.2 Auxiliary Data Comparison.....	6
3.2.1 General.....	6
3.2.2 Presentation of the auxiliary data	6
3.2.3 Age Verification	9
3.2.4 Document Validation	10
3.3 Restricted Identification.....	10
3.3.1 General.....	10
3.3.2 Command APDU for Step RI:1	14
3.3.3 Command APDU for Step RI:2	15
4 e-Services with trusted third party protocol	16
4.1 General.....	16
4.2 Architecture	16
4.3 Enhanced Role Authentication (ERA) protocol	18
4.4 Authentication flow steps	19
4.4.1 General.....	19
4.4.2 Step 1: Service selection	21
4.4.3 Step 2: User consent.....	21
4.4.4 Step 3 User authentication to the SP	21
4.4.5 Step 4 Access to the service (or go to next steps)	21
4.4.6 Step 5 Request for attributes (OPT)	21
4.4.7 Step 6 Restoration of security context (OPT).....	21
4.4.8 Step 7 User authentication to the AP (OPT).....	21
4.4.9 Step 8 Reading and providing attribute requested (OPT)	21
4.4.10 Step 9 Restoration of security context (OPT).....	21
4.4.11 Step 10 Ask access to the service (OPT).....	21
4.4.12 Step 11 Verification of attributes by the SP (OPT).....	21
4.4.13 Step 12 Grant access to the service (OPT).....	21
Bibliography.....	22

European foreword

This document (EN 419212-4:2018) has been prepared by Technical Committee CEN/TC 224 “Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment”, the secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by October 2018, and conflicting national standards shall be withdrawn at the latest by October 2018.

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 supersedes EN 419212-1:2014 and EN 419212-2:2014.

This standard supports services in the context of **electronic IDentification, Authentication and Trust Services (eIDAS)** including signatures.

In EN 419212 Part 2, the standard allows support of implementations of the European legal framework for electronic signatures, defining the functional and security features for a Secure Elements (SE) (e.g. smart cards) intended to be used as a Qualified Signature Creation Device (QSCD) according to the Terms of the “European Regulation on Electronic Identification and Trust Services for electronic transactions in the internal market”.

A Secure Element (SE) compliant to the standard will be able to produce a “qualified electronic signature” that fulfils the requirements of section 4, in particular Articles 26 (requirements for advanced electronic signatures) and 29 (requirements for qualified electronic signature creation devices) of the so-called eIDAS Regulation and therefore can be considered equivalent to a hand-written signature.

This standard consists of five parts:

- Part 1: “Introduction and common definitions” describes the history, application context, market perspective and a tutorial about the basic understanding of electronic signatures. It also provides common terms and references valid for the entire 419212 series.
- Part 2: “Signature and Seal Services” describes the specifications for signature generation according to the eIDAS regulation.
- Part 3: “Device Authentication” describes the device authentication protocols and the related key management services to establish a secure channel.
- Part 4: “Privacy specific Protocols” describes functions and services to provide privacy to identification services.
- Part 5: “Trusted eServices” describes services that may be used in conjunction with signature services described in Part 2.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: 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

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

The European Committee for Standardization (CEN) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning the mapping function given in EN 419212-2:2017 8.2.

The patent relates to “Sagem, MorphoMapping Patents FR09-54043 and FR09-54053, 2009”.

CEN takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has ensured CEN that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with CEN. Information may be obtained from:

Morpho

11, boulevard Galliéni

92445 Issy-les-Moulineaux Cedex

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. CEN shall not be held responsible for identifying any or all such patent rights.