

DIN EN 419212-4

ICS 35.240.15

Entwurf

Einsprüche bis 2016-12-21
Ersatzvermerk
siehe unten

**Anwendungsschnittstelle für sichere Elemente zur elektronischen
Identifikation, Authentisierung und für vertrauenswürdige Dienste –
Teil 4: Datenschutzspezifische Protokolle;
Englische Fassung FprEN 419212-4:2016**

Application Interface for Secure Elements for Electronic Identification, Authentication and
Trusted Services –
Part 4: Privacy specific Protocols;
English version FprEN 419212-4:2016

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2016-10-21 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs
besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.din.de/go/entwuerfe bzw. für Norm-
Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de,
sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im
Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-
Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA),
10772 Berlin, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Ersatzvermerk

Vorgesehen mit E DIN EN 419212-1:2016-11, E DIN EN 419212-2:2016-11, E DIN EN 419212-3:2016-11 und
E DIN EN 419212-5:2016-11 als Ersatz für DIN EN 419212-1:2015-03 und DIN EN 419212-2:2015-03

Gesamtumfang 25 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (FprEN 419212-4:2016) wurde vom Technischen Komitee CEN/TC 224 „Persönliche Identifikation, elektronische Signatur, maschinenlesbare Karten sowie zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat vom AFNOR (Frankreich) gehalten wird.

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

Dieses Dokument ist derzeit zum einstimmigen Annahmeverfahren (UAP) vorgelegt.

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

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: „Geräteauthentifizierung“ beschreibt die Geräteauthentifizierungsprotokolle und die dazugehörigen Schlüsselverwaltungsdienste zur Einrichtung eines sicheren Kanals.*
- *Teil 4: „Datenschutzspezifische Protokolle“ beschreibt Funktionen und Dienste, um den Datenschutz bei Identifikationsdiensten zu gewährleisten.*
- *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. Daher wurden von dieser Norm nur die Begriffe übersetzt (siehe Nationaler Anhang NA).

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.

October 2016

ICS 35.240.15

Will supersede EN 419212-1:2014, EN 419212-2:2014

English Version

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

Anwendungsschnittstelle für sichere Elemente, die als
qualifizierte elektronische Signatur-
/Siegelerstellungseinheiten verwendet werden - Teil 4:
Datenschutzspezifische Protokolle

This draft European Standard is submitted to CEN members for unique acceptance procedure. It has been drawn up by the Technical Committee CEN/TC 224.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN 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, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

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.

Warning: This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.



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

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

Contents

European foreword.....	4
Introduction	5
1 Scope.....	6
2 Normative references.....	6
3 Privacy Context functions	6
3.1 Introduction	6
3.2 Auxiliary Data Comparison.....	7
3.2.1 General.....	7
3.2.2 Presentation of the auxiliary data	7
Table 1 — Reference device authentication scheme mEAC	8
3.2.3 Age Verification	10
Table 2 — COMPARE operation — command APDU	10
Table 3 — COMPARE operation — response	10
3.2.4 Document Validation	10
Table 4 — COMPARE operation — command APDU	11
Table 5 — COMPARE operation — response	11
3.3 Restricted Identification.....	11
3.3.1 General.....	11
Table 6 — General command sequence for Restricted Identification	13
3.3.2 Command APDU for Step RI:1	15
Table 7 — Step RI:1 of Restricted Identification — command APDU	15
Table 8 — Step RI:1 of Restricted Identification — response APDU.....	15
3.3.3 Command APDU for Step RI:2	16
Table 9 — Step RI:2 of Restricted Identification — command APDU	16
Table 10 — Coding of CAPDU Tag 'AX'	16
Table 11 — Step RI:2 of Restricted Identification — response APDU	16
4 e-Services with trusted third party protocol	17
4.1 General.....	17
4.2 Architecture	17
Figure 1 — eServices with trusted third party - Architecture	18
4.3 Enhanced Role Authentication (ERA) protocol.....	18
Figure 2 — eServices with trusted third party - Protocol flow [TR03110P2#2.3.6]	19
4.4 Authentication flow steps	20
4.4.1 General.....	20
Table 12 — Privacy preserving scheme	20
4.4.2 Step 1: Service selection	21

4.4.3	Step 2: User consent.....	22
4.4.4	Step 3 User authentication to the SP.....	22
4.4.5	Step 4 Access to the service (or go to next steps).....	22
4.4.6	Step 5 Request for attributes (OPT).....	22
4.4.7	Step 6 Restoration of security context (OPT).....	22
4.4.8	Step 7 User authentication to the AP (OPT).....	22
4.4.9	Step 8 Reading and providing attribute requested (OPT).....	22
4.4.10	Step 9 Restoration of security context (OPT).....	22
4.4.11	Step 10 Ask access to the service (OPT).....	22
4.4.12	Step 11 Verification of attributes by the SP (OPT).....	22
4.4.13	Step 12 Grant access to the service (OPT).....	22
	Bibliography	23

European foreword

This document (FprEN 419212-4:2016) has been prepared by Technical Committee CEN/TC 207 “Furniture”, the secretariat of which is held by AFNOR.

This document is currently submitted to the Unique acceptance procedure.

This document will supersede 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. [NP1#1]

Part 2: “Signature and Seal Services” describes the specifications for signature generation according to the eIDAS regulation. [NP2#1]

Part 3: “Device Authentication” describes the device authentication protocols and the related key management services to establish a secure channel. [NP3#1]

Part 4: “Privacy specific Protocols” describes functions and services to provide privacy to identification services. [NP4#1]

Part 5: “Trusted eServices” describes services that may be used in conjunction with signature services described in Part 2. [NP5#1]

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 [NP2#8.2.5] 8.2.5 “Step 4.2 - Map nonce and compute generator point for integrated mapping”.

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.

1 Scope

This part specifies mechanisms for SEs to be used as privacy-enabled devices in the context of IAS, and fulfill the requirements of Article 5 of the so-called eIDAS Regulation about data processing and protection.

It covers:

- Age verification
- Document validation
- Restricted identification
- eServices with trusted third party based on ERA protocol

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 7816-8:2004, *Integrated circuit(s) cards with contacts — Part 8: Commands and mechanisms for security operations*

3 Privacy Context functions

3.1 Introduction

Privacy Context is an environment to be considered whereas a card holder may be exposed to an environment that might read privacy parameters from the card ahead of any device authentication. Such privacy parameters can be the unique Card ID or other personalized parameters that allow a tracking and profiling of the card holder.

For instance, if the nationality of a card holder can be identified by the nature of the card description parameters (e.g. algorithm ID), then a card holder of certain nationality could be exposed to observation. Privacy context describes the requirement to allow a card holder to be confident that privacy parameters will not be exposed to unauthorized environment.

ICC Cards used for eID functionality may need as well privacy features e.g. to conceal the identity or the specific profile of the ICC owner in open networks or for Machine to Machine (M2M) services.

One popular functionality represents the well known use of pseudonyms here implemented by the restricted identification or 4.3 “Enhanced Role Authentication (ERA) protocol” with the purpose that these pseudonyms are used for certain services (e.g. payment sector) and cannot be linked to a global profile of the owner.

Another application lies in the validation of the ICC for authorization to web services, (e.g. voting) where only as much information is to be revealed as necessary for the actual service. Another popular use is the age verification with information provided only to the extent that a person is older than a particular age but without revealing the actual age of the card holder.

Different privacy oriented protocols are described in the following sections.