

DIN EN 419212-1



ICS 35.240.15

Mit DIN EN 419212-3:2017-11
Ersatz für
DIN EN 419212-1:2015-03 und
DIN EN 419212-2:2015-03

**Anwendungsschnittstelle für sichere Elemente zur elektronischen
Identifikation, Authentisierung und für vertrauenswürdige Dienste –
Teil 1: Einführung und allgemeine Definitionen;
Englische Fassung EN 419212-1:2017**

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

Part 1: Introduction and common definitions;
English version EN 419212-1:2017

Interface applicative des éléments sécurisés utilisés comme dispositifs de création de
signature électronique qualifiée (cachet) –

Partie 1: Introduction et définitions communes;
Version anglaise EN 419212-1:2017

Gesamtumfang 73 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (EN 419212-1:2017) 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 Chipkarten“ 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 419212-2 soll die Implementierung des europäischen rechtlichen Rahmens für elektronische Signaturen unterstützen, indem sie die funktions- und sicherheitsbezogenen Anforderungen an sichere Elemente (SE) (z. B. Chipkarten) zur Verwendung als qualifizierte elektronische Signaturerstellungseinheit (QSCD, en: Qualified electronic Signature Creation Device) entsprechend den Bedingungen der Europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt [2] definiert.

Ein mit der Norm übereinstimmendes sicheres Element (SE) wird in der Lage sein, eine „qualifizierte elektronische Signatur“ zu erzeugen, die die Artikel der Verordnung zu elektronischen Signaturen erfüllt und daher als zu handschriftlichen Signaturen [2] äquivalent betrachtet werden kann.

Die Normenreihe DIN EN 419212 besteht aus fünf Teilen:

- *Teil 1: „Einführung und allgemeine Definitionen“ beschreibt Geschichte, Anwendungszusammenhang, Marktperspektive und eine Anleitung für das Grundverständnis von elektronischen Signaturen. Sie bietet außerdem allgemeine Begriffe und Verweisungen, die für die gesamte Reihe 419212 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, 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 von 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).

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 3166-1:2006 siehe DIN EN ISO 3166-1:2007-03

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) Begriffe zu elektronischen Siegeln wurden aufgenommen;
- c) allgemeine Signaturdienste wurden in Teil 2 verschoben und um Siegeldienste ergänzt;
- d) Festlegungen zur Geräteauthentisierung wurden in Teil 3 verschoben.

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

Nationaler Anhang NA (informativ)

Begriffe und Abkürzungen

3 Begriffe

Für die Anwendung der Teile 1 bis 5 dieser Normenreihe gelten die folgenden Begriffe.

ANMERKUNG Diese Begriffe stimmen mit den Begriffen in der überarbeiteten Fassung von ISO/IEC 7816-4 überein.

3.1

fortgeschrittenes elektronisches Siegel

elektronisches Siegel, das die folgenden Anforderungen erfüllt:

- a) es ist eindeutig dem Siegelersteller zugeordnet;
- b) es ermöglicht die Identifizierung des Siegelerstellers;
- c) es wird unter Verwendung von elektronischen Siegelerstellungsdaten erstellt, die der Siegelersteller mit einem hohen Maß an Vertrauen unter seiner Kontrolle zum Erstellen elektronischer Siegel verwenden kann; und
- d) es ist so mit den Daten, auf die es sich bezieht, verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann

3.2

fortgeschrittene elektronische Signatur

Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit Ihnen verbunden werden, um den Ursprung und die Unversehrtheit der verbundenen Daten sicherzustellen. Elektronische Signatur, die die folgenden Anforderungen erfüllt:

- a) sie ist eindeutig dem Unterzeichner zugeordnet;
- b) sie ermöglicht die Identifizierung des Unterzeichners;
- c) sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann;
- d) sie ist so mit den Daten, auf die sie sich bezieht, verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann

3.3

Anonymität

Zusicherung, dass ein Benutzer ein Betriebsmittel oder einen Dienst ohne Offenlegung seiner Benutzeridentität nutzen kann

3.4

Anonymisierung

Prozess, der die Zuordnung eines Kenndatensatzes zu einem Betroffenen löscht

3.5

anonymisierte Daten

ehemals mit einer Person verknüpfte Daten, die jetzt nicht mehr mit dieser Person in Verbindung gebracht werden können

3.6**anonyme Daten**

Daten, die nicht mit einer bestimmten Person verknüpft werden können

3.7**Answer-to-Reset-Datei**

Elementardatei, die die Betriebsmerkmale der Karte angibt

3.8**ohne Authentisierung vertrauenswürdig**

Betriebsumgebung, die ohne eine weitere Geräteauthentisierung der Definition nach vertrauenswürdig ist

BEISPIEL Ein Beispiel dafür ist die Anwendung innerhalb eines Unternehmens, in dem jeder vorhandene Zugangspunkt mit einem vertrauenswürdigen Netzwerk verbunden ist.

3.9**Authentisierung**

elektronischer Prozess, der die Bestätigung der elektronischen Identifizierung einer natürlichen oder juristischen Person; oder die Bestätigung des Ursprungs und der Unversehrtheit von elektronischen Daten ermöglicht

3.10**Zertifikat für elektronische Signaturen**

elektronische Bescheinigung, die elektronische Signaturprüfdaten mit einer natürlichen Person verknüpft und die mindestens den Namen oder das Pseudonym dieser Person bestätigt

3.11**Befehl-Antwort-Paar**

Satz zweier Nachrichten: ein Befehl gefolgt von einer Antwort

3.12**Vertraulichkeitsschutz**

Verhinderung der Offenlegung von Informationen für unberechtigte Personen, Instanzen oder Systeme [ISO 7498-2]

3.13**Siegelersteller**

juristische Person, die ein elektronisches Siegel erstellt

3.14**Dateneinheit**

kleinster Satz von Bits, der eindeutig referenziert werden kann

3.15**Datenelement**

Information, die an der Schnittstelle sichtbar ist und für die ein Name, eine Beschreibung des logischen Inhalts, ein Format und eine Kodierung definiert sind

3.16**Datenobjekt**

Information, die an der Schnittstelle sichtbar ist und die aus einem Tag, einer Länge und einem Wert besteht (d. h. ein Datenelement)

Anmerkung 1 zum Begriff: In dieser Spezifikation werden Datenobjekte als BER-TLV-Datenobjekte bezeichnet. Siehe ISO/IEC 7816-4.

3.17

zugeordnete Datei

Datei, die Dateisteuerungsinformationen und wahlweise Speicher zur Zuteilung enthält. Sie kann Halter weiterer EF und/oder DF sein

3.18

Geräteauthentisierung

Überprüfungsprozess der Anmeldeinformationen eines Gerätes

3.19

DF-Name

Byte-Strang, der eine zugeordnete Datei auf der Karte eindeutig kennzeichnet

3.20

digitale Signatur

an eine Dateneinheit angefügte Daten oder eine kryptographische Transformation einer Dateneinheit, mit der ein Empfänger der Dateneinheit die Möglichkeit der Überprüfung der Quelle und Integrität der Dateneinheit erhält und die einen Schutz gegen Fälschung z. B. durch den Empfänger bietet

3.21

elektronisches Siegel

Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit Ihnen verbunden werden, um den Ursprung und die Unversehrtheit der verbundenen Daten sicherzustellen

3.22

elektronische Siegelerstellungseinheit

konfigurierte Software oder Hardware, die zum Erstellen eines elektronischen Siegels verwendet wird

3.23

elektronische Signatur

Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit Ihnen verbunden werden und vom Unterzeichner zum Signieren verwendet werden

3.24

elektronische Signaturerstellungseinheit

konfigurierte Software oder Hardware, die zum Erstellen einer elektronischen Signatur verwendet wird

3.25

qualifiziertes elektronisches Siegel

fortgeschrittenes elektronisches Siegel, das von einer qualifizierten elektronischen Siegelerstellungseinheit erstellt wird und auf einem qualifizierten Zertifikat für elektronische Siegel beruht. Ein qualifiziertes Zertifikat ist in [eIDASReg#1] spezifiziert

3.26

qualifizierte elektronische Siegelerstellungseinheit

elektronische Siegelerstellungseinheit, die ein qualifiziertes elektronisches Siegel erstellt

3.27

qualifizierte elektronische Signaturerstellungseinheit

elektronische Signaturerstellungseinheit, die folgende Anforderungen erfüllt:

- 1) Sie muss durch geeignete Technik und Verfahren zumindest gewährleisten, dass
 - a) die Vertraulichkeit der zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten angemessen sichergestellt ist,
 - b) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten praktisch nur einmal vorkommen können,
 - c) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten mit hinreichender Sicherheit nicht abgeleitet werden können und die elektronische Signatur bei Verwendung der jeweils verfügbaren Technik verlässlich gegen Fälschung geschützt ist,

- d) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten vom rechtmäßigen Unterzeichner gegen eine Verwendung durch andere verlässlich geschützt werden können.
- 2) Qualifizierte elektronische Signaturerstellungseinheiten dürfen die zu unterzeichnenden Daten nicht verändern und nicht verhindern, dass dem Unterzeichner diese Daten vor dem Unterzeichnen angezeigt werden.
- 3) Das Erzeugen oder Verwalten von elektronischen Signaturerstellungsdaten im Namen des Unterzeichners darf nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt werden.
- 4) Unbeschadet des Punktes 1), Buchstabe d), dürfen qualifizierte Vertrauensdiensteanbieter, die elektronische Signaturerstellungsdaten im Namen des Unterzeichners verwalten, die elektronischen Signaturerstellungsdaten ausschließlich zu Sicherungszwecken kopieren, sofern folgende Anforderungen erfüllt sind:
 - a) die kopierten Datensätze müssen das gleiche Sicherheitsniveau wie die Original-Datensätze aufweisen;
 - b) es dürfen nicht mehr kopierte Datensätze vorhanden sein als zur Gewährleistung der Dienstleistungskontinuität unbedingt nötig

3.28

Elementardatei

Satz von Dateneinheiten oder Datensätzen, die denselben Identifikator aufweisen. Eine Elementardatei kann nicht Halter einer anderen Datei sein

3.29

Dateisteuerungsparameter

logische, aufbaubezogene und sicherheitsbezogene Attribute einer Datei

3.30

Identifikator

2-Byte-Binärwert zur Adressierung einer Datei

3.31

Folgenlosigkeit

Sicherheitseigenschaft eines Protokolls, die zusichert, dass die Offenlegung eines Langzeitschlüssels es einem Angreifer nicht ermöglicht, die Sicherheitseigenschaften für die Ausführung des Protokolls, die in der Vergangenheit festgelegt wurden, zum Beispiel durch Neuberechnung früherer abgeleiteter Schlüssel, zu gefährden

3.32

Identifizierung

eindeutige Zuordnung eines Satzes beschreibender Parameter zu einer Person innerhalb eines gegebenen Zusammenhangs

3.33

Integritätsschutz

Mechanismus zur Sicherstellung, dass Daten nicht unerkannt verändert werden können

3.34

Masterdatei

obligatorische eindeutige zugeordnete Datei, die die Wurzel der Dateistruktur darstellt

3.35

Nachricht

Byte-Strang, der vom Schnittstellengerät zur Karte oder umgekehrt gesendet wird, ausgenommen übertragungsorientierte Zeichen nach ISO/IEC 7816-3

3.36

gegenseitige Authentisierung

Authentisierung, bei der beide Beteiligten (ICC und IFD) gegenseitig authentisiert werden

3.37

Nichtbeweisbarkeit

siehe „nicht nachprüfbare Authentisierung“

3.38

übergeordnete Datei

zugeordnete Datei, die einer bestimmten Datei in der Hierarchie unmittelbar vorangeht

3.39

Passwort

Daten, die der Kartenbenutzer der Karte vorlegen muss, wenn von der Anwendung gefordert und die, im Sinne dieser Spezifikation, ein Strang von Zahlen und/oder ASCII-Zeichen ist

3.40

Pfad

Verkettung von Dateiidentifikatoren ohne Begrenzung. Wenn der Pfad mit dem Identifikator der Masterdatei beginnt, handelt es sich um einen absoluten Pfad

3.41

Schutz personenbezogener Daten

Anspruch von Personen, Gruppen oder Organisationen, selbst zu bestimmen, wann, wie und in welchem Umfang Informationen über sie anderen mitgeteilt werden [ISO 7498-2]

3.42

privater Schlüssel

Schlüssel eines asymmetrischen Schlüsselpaars einer Entität, der nur von dieser Entität benutzt werden sollte

3.43

Pseudonym

Identifikator mit ausreichend Informationen, um einem Prüfer das Herstellen einer eindeutigen Verbindung zu einer Entität zu ermöglichen

Anmerkung 1 zum Begriff: Ein Pseudonym kann zur Verringerung von Datenschutzrisiken bei der Verwendung von Identifikatoren mit festen oder bekannten Werten eingesetzt werden.

Anmerkung 2 zum Begriff: Ein Pseudonym kann ein Identifikator mit einem von einer Person gewählten oder zufällig zugewiesenen Wert sein.

3.44

Pseudonymisierung

spezielle Art der Anonymisierung, die sowohl die ursprünglichen Identifikationsdaten zu einer Person löscht als auch die Zuordnung eines speziellen Namens (Pseudonym) zu einer Person so ermöglicht, dass anhand des zugeordneten Namens (Pseudonym) kein Rückschluss auf die Identität der Person möglich ist

3.45**pseudonymisierte Daten**

Daten, die nur mit einer bestimmten Person verknüpft werden können, wenn jemand im Besitz einer entsprechenden Zuordnungstabelle ist

3.46**Pseudonymität**

Zusicherung, dass ein Benutzer ein Betriebsmittel oder einen Dienst ohne Offenlegung seiner Benutzeridentität nutzen darf, aber für die Benutzung nach wie vor zur Verantwortung gezogen werden kann

3.47**öffentlicher Schlüssel**

öffentlicher Teil eines asymmetrischen Schlüsselpaars

3.48**qualifizierte elektronische Signatur**

fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht

3.49**Datensatz**

Byte-Strang, der von der Karte als Gesamtheit behandelt und durch eine Datensatznummer referenziert werden kann

3.50**Datensatznummer**

laufende Nummer, die jedem Datensatz zugewiesen wird und die den Datensatz innerhalb seiner Elementardatei eindeutig identifiziert

3.51**Wiederholungszähler**

Zähler, der verwendet wird, um die Anzahl fehlerhafter Verwendungen eines entsprechenden (Sicherheits-) Objekts zu zählen. Wenn das Objekt (z. B. Passworteingabe) korrekt verwendet wurde (korrektes Passwort eingegeben), wird der Wiederholungszähler auf seinen Ausgangswert zurückgesetzt. Ein typischer Wert eines Wiederholungszählers ist 3

3.52**geheimer Schlüssel**

in symmetrischen Algorithmen verwendeter Schlüssel

3.53**Sicherheitsumgebung**

Benutzungsbedingung von Objekten in der Karte einschließlich gespeicherter Daten und Datenbearbeitungsfunktionen, die als Datenelement mit einer oder mehreren Zugriffsregeln ausgedrückt wird

3.54**Unterzeichner**

natürliche Person, die eine elektronische Signatur erstellt

3.55**Signaturerstellungseinheit**

sichere Einheit, die in der Lage ist, aus ihren gespeicherten Daten und Funktionalitäten eine Signatur zu erstellen

3.56

nicht nachprüfbare Authentisierung

Authentisierung, die keinen beständigen kryptographischen Nachweis dafür gibt, dass die Authentisierung stattgefunden hat

3.57

vertrauenswürdige Umgebung

Betriebsumgebung, die durch Definition ihrer physikalischen Lage, ihres physikalischen Schutzes oder ihrer physikalischen Zugriffsbedingungen oder sonstige Maßnahmen die Verfälschung der an der Kommunikationsschnittstelle sichtbaren Daten verhindert

3.58

vertraute Umgebung

Umgebung, für die der Benutzer entschieden hat ihr zu vertrauen

Anmerkung 1 zum Begriff: In sehr wenigen Fällen kann der Benutzer entscheiden, ob einer Umgebung vertraut werden kann oder nicht. Falls ein Benutzer sich nicht sicher ist, ob eine Umgebung ohne Authentisierung vertrauenswürdig ist, wird sehr empfohlen keine PIN einzugeben, bis auf einer Anzeige der Nachweis für sichere Nachrichtenübertragung erscheint (was eine vertrauenswürdige Umgebung impliziert).

3.59

vertrauenswürdiger Kanal

Mittel, durch das eine TSF und ein vertrauenswürdiges abgesetztes IT-Produkt mit dem erforderlichen Vertrauen kommunizieren können, um die TSP zu unterstützen

3.60

vertrauenswürdiger Pfad

Mittel, durch das ein Benutzer und eine TSF mit dem erforderlichen Vertrauen kommunizieren können, um die TSP zu unterstützen

3.61

Unverknüpfbarkeit

Zusicherung, dass ein Benutzer Betriebsmittel oder Dienste mehrfach nutzen kann, ohne dass andere in der Lage sind, diese Nutzungen miteinander zu verknüpfen [ISO 7498-2]

3.62

nicht zuverlässige Umgebung

Betriebsumgebung, die Fälschung und Einschleusen von an der Kommunikationsschnittstelle vorliegenden Daten nicht verhindert. Eine Umgebung, die ohne Authentisierung nicht vertrauenswürdig ist und die ihre Vertrauenswürdigkeit nicht durch eine Geräteauthentisierung nachweisen kann, muss als nicht zuverlässig angesehen werden. In einer nicht zuverlässigen Umgebung sollten vom Karteninhaber keine weiteren Handlungen erfolgen

3.63

nicht vertrauenswürdige Umgebung

Betriebsumgebung, die nicht als zuverlässig vorausgesetzt werden kann. Bis ein Vertrauensnachweis erbracht worden ist (in der Regel durch eine Geräteauthentisierung), sollte die Umgebung vom Karteninhaber keine sensiblen Daten, vor allem keine PIN, gesendet bekommen

Anmerkung 1 zum Begriff: Nach einer erfolgreichen Geräteauthentisierung wird die nicht vertrauenswürdige Umgebung eine vertrauenswürdige Umgebung. Aus diesem Grund bezeichnet die Eigenschaft „nicht vertrauenswürdig“ nicht die Eigenschaft „nicht zuverlässig“, sondern beinhaltet die Forderung nach einem Vertrauensnachweis.

3.64

Verwendungszähler

Zähler, der bei jeder Verwendung eines entsprechenden Objekts aktualisiert wird. Im Gegensatz zu Wiederholungszählern werden Verwendungszähler nicht auf ihren Ausgangswert zurückgesetzt, nachdem das Objekt erfolgreich verwendet wurde.

3.65

Zustimmung des Benutzers

Willenserklärung für einen kartenbezogenen Dienst

3.66

Gebrauch von Wendungen in der vorliegenden Norm

Schlüsselworte „MUSS“ (en: SHALL), „ERFORDERLICH“ (en: REQUIRED“), „DARF NICHT“ (en: SHALL NOT), „SOLLTE“ (en: SHOULD), „SOLLTE NICHT“ (en: SHOULD NOT), „EMPFOHLEN“ (en: RECOMMENDED), „DARF“ (en: MAY) und „WAHLWEISE“ (en: OPTIONAL) im vorliegenden Dokument sind nach der Beschreibung in [4] zu interpretieren

- MUSS:** Dieses Wort oder die Benennung „**ERFORDERLICH**“ oder „**MUSS**“ bedeutet, dass die Definition eine absolute Anforderung der Spezifikation darstellt.
- DARF NICHT:** Dieser Ausdruck bedeutet, dass die Definition ein absolutes Verbot der Spezifikation darstellt.
- SOLLTE:** Dieses Wort oder das Adjektiv „**EMPFOHLEN**“ bedeutet, dass unter bestimmten Umständen berechtigte Gründe dafür bestehen, ein bestimmtes Element zu vernachlässigen, aber die vollständigen Auswirkungen nachvollzogen und sorgfältig abgewogen werden müssen, bevor ein anderer Ablauf gewählt wird.
- SOLLTE NICHT:** Dieser Ausdruck oder das Adjektiv „**NICHT EMPFOHLEN**“ bedeutet, dass unter bestimmten Umständen berechtigte Gründe dafür bestehen, dass das jeweilige Verhalten zulässig oder sogar zweckdienlich ist, aber die vollständigen Auswirkungen sollten nachvollzogen und der Fall sorgfältig abgewogen werden, **bevor ein mit diesem Kennzeichen beschriebenes Verhalten implementiert wird.**
- DARF:** Dieses Wort oder das Adjektiv „**WAHLWEISE**“ bedeutet, dass ein Element wahlweise benutzt werden kann. Ein Hersteller kann sich für die Aufnahme des Elements entscheiden, weil es von einem bestimmten Marktsegment gefordert wird oder der Hersteller meint, dass es sein Produkt verbessert, während ein anderer Hersteller das gleiche Element weglassen kann. Eine Implementierung, die eine bestimmte Wahlmöglichkeit nicht enthält, MUSS so vorbereitet sein, dass sie mit einer anderen Implementierung zusammenarbeiten kann, die die Wahlmöglichkeit enthält, wenn auch unter Umständen mit einer verringerten Funktionalität.
- [...]** Eckige Klammern zeigen eine Wahlfreiheit an. Das kann entweder sein:
- eine *Auswahl von Werten* in einem vorgegebenen Bereich [„00‘ .. ,03‘] — typisch für Felder mit fester Länge,
 - oder eine Auswahl, ob ein Wert angegeben wird oder nicht — ... || ,80‘ L80 AlgID || [,83‘ L83 KeyID] ..., wobei der Datensatz in eckigen Klammern den *wahlweisen* Teil (= im Ermessen der Implementierung) angibt oder *bedingt* ist (= abhängig von einer in der Norm angegebenen Bedingung).
- BEDINGUNG:** Die Anwendung einer Ausprägung hängt von einer oder mehreren Bedingungen ab und darf nur vorgenommen werden, wenn die Bedingung(en) erfüllt werden. Die zugehörige(n) Bedingung(en) wird/werden immer beschrieben, wenn ein *bedingtes* Attribut durch eine Spezifikation erstellt wurde. Die Spezifikation darf, abhängig vom Kontext in dem sie erstellt wurde, *normativ* oder *informativ* sein, wenn die Bedingungen erfüllt sind.

4 Abkürzungen

Für die Anwendung der Teile 1 bis 5 dieser Normenreihe gelten die folgenden Abkürzungen.

ANMERKUNG Diese Begriffe stimmen mit den Begriffen in der überarbeiteten Fassung von ISO/IEC 7816-4 überein.

AES	Erweiterter Verschlüsselungsstandard (en: Advanced Encryption Standard)
AID	Anwendungsbezeichner (en: Application Identifier)
APDU	Anwendungsprotokoll-Dateneinheit (en: Application protocol data unit)
AKI	Instanzschlüsselbezeichner (en: Authority Key Identifier)
AT	Authentisierungstemplate (en: Authentication Template), CRT für Authentisierung
AUT	Authentisierung (en: Authentication)
BCD	Binärcode für Dezimalziffern (en: Binary Coded Decimal)
BER	Basic Encoding Rules
C	Zertifikat (en: Certificate)
CA	Zertifizierungsinstanz (en: Certification Authority)
CAR	CA-Referenz (en: CA Reference)
CC	Kryptographische Prüfsumme (en: Cryptographic Checksum)
CDA	Kartengeräteauthentisierung (en: Card Device Authentication)
CG	Kryptogramm (en: Cryptogram)
CH	Karteninhaber (en: Cardholder)
CHA	Berechtigung des Zertifikatinhabers (en: Certificate Holder Authorization)
CHN	Karteninhabername (en: Cardholder Name)
CHR	Zertifikatinhaberreferenz (en: Certificate Holder Reference)
CIA	Kryptographische Informationsanwendung (en: Cryptographic Information Application)
CIO	Kryptographisches Informationsobjekt (en: Cryptographic Information Object)
CLA	Klassenbyte (en: Class byte)
Comp()	Die Komprimierungsfunktion des öffentlichen Schlüssels <i>Comp(...)</i> ist in EN 419212-2, 11.6, definiert
CPI	Zertifikatprofilbezeichner (en: Certificate Profile Identifier)
CRT	Control Reference Template
CS	CertSign, Zertifikat, das den öffentlichen Teil eines Signaturschlüsselpaars enthält
CT	CRT für Vertraulichkeit
CV	Kartenverifizierbar (en: Card Verifiable)
CWA	CEN Workshop Agreement
C/S	Client/Server
D[key](msg)	Dechiffrierung (en: Decipherment) von <msg> mit <key>
DE	Datenelement (en: Data Element)
DES	Datenverschlüsselungsstandard (en: Data Encryption Standard)
DF	Zugeordnete Datei (en: Dedicated File)
DH	Diffie-Hellman
DH.P	DH-Parameter (en: DH parameters), $DH.P = g p q$
DIR	Verzeichnis (en: Directory)

DO	Datenobjekt (en: Data Object)
DS[key](msg)	Digitale Signatur (en: Digital Signature) von <msg> mit <key>
DSA	Digitaler Signaturalgorithmus (en: Digital Signature Algorithm)
DSI	Digitale Signatureingabe (en: Digital Signature Input)
DST	Template für digitale Signatur (en: Digital Signature Template), CRT für DS
DTBS	Zu signierende Daten (en: Data to be signed)
DTBS/R	Entfernt zu signierende Daten (en: Data to be signed remotely)
E[key](msg)	Verschlüsselung (en: Encipherment) von <msg> mit <key>
ECC	Europäische Bürgerkarte (European Citizen Card)
ECDH	DH Schlüsselvereinbarung auf Basis von Kryptographie mit elliptischen Kurven (ELC)
ECDH.P	ECDH Parameter auf Basis von Kryptographie mit elliptischen Kurven. $ECDH.P = p a b G n$
ECDSA	Signaturschema auf Basis von Kryptographie mit elliptischen Kurven (ELC)
ELC	Kryptographie mit elliptischen Kurven (en: Elliptic Curve Cryptography)
EDFB	Encrypted Data Formatted Block
eIDAS	Elektronische Identifizierungs- und Authentisierungsdienste (en: E lectronic I dentification and A uthentication S ervices)
FCI	Dateisteuerungsinformation (en: File Control Information)
FID	Dateiidentifikator (en: File Identifier)
h(msg)	Hash-Code von <msg>
HT	CRT für Hash-Code
ICC	Karte mit integrierten Schaltkreisen, Chipkarte (en: Integrated Circuit(s) Card)
ICV	Initial Chaining Value
ID	Bezeichner (en: Identifier)
IFD	Schnittstellengerät (en: Interface Device)
INS	Befehlsbyte (en: Instruction byte)
KE	Schlüsselchiffrierung (en: Key Encipherment)
KID	Schlüsselbezeichner (en: Key Identifier)
L.F	Länge der elliptischen Kurvenparameter
MAC[key](msg)	Nachrichtenauthentisierungscode (en: Message Authentication Code) von <msg>, erstellt mit <key>
MF	Masterdatei (en: Master File)
MSE	MANAGE SECURITY ENVIRONMENT
OAEP	Optimales asymmetrisches Verschlüsselungs-Padding (en: Optimal Asymmetric Encryption Padding)
OID	Objektbezeichner (en: Object Identifier)
P1-P2	Parameterbytes (en: Parameter bytes)
PBM	Passwortbasierter Mechanismus (en: Password based mechanism)
PCA	Datenschutzbasierte Chipauthentisierung (en: Privacy based Chip Authentication)
PrK	Privater Schlüssel (en: Private Key)
PuK	Öffentlicher Schlüssel (en: Public Key)
PKI	Public-Key-Infrastruktur (en: Public Key Infrastructure)

PKCS	Standards zur Verschlüsselung mit öffentlichem Schlüssel (en: Public Key Cryptography Standards)
PI	Padding-Indikator (en: Padding Indicator)
PIN	Persönliche Identifikationsnummer (en: Personal Identification Number)
PP	Schutzprofil (en: Protection Profile)
PRND	Zufallspaddingzahl (en: Padding Random Number)
PSO	PERFORM SECURITY OPERATION
PSS	Probabilistisches Signatursystem (en: Probabilistic Signature Scheme)
QES	Qualifizierte elektronische Signatur (en: Qualified Electronic Signature)
QSCD	Qualifizierte Signaturerstellungseinheit (en: Qualified Signature Creation Device)
RC	Wiederholungszähler (en: Retry Counter)
RCA	RootCA
RD	Referenzdaten (en: Reference Data)
RFU	Für zukünftige Verwendung reserviert (en: Reserved for Future Use)
RID	Registrierter Bezeichner des Anwendungsanbieters (en: Registered application provider identifier)
RND	Zufallszahl (en: Random number)
RSA	Signatur-Algorithmus nach Ronald Rivest, Adi Shamir, Leonard Adleman
SCA	Signaturerstellungsanwendung (en: Signature-Creation Application)
SHA	Sicherer Hash-Algorithmus (en: Secure Hash Algorithm)
SE	Sicherheitsumgebung (en: Security Environment)
SIG()	Signatur von
SK	Geheimer Schlüssel (en: Secret Key)
SN	Laufende Nummer (en: Serial Number)
SM	Sichere Nachrichtenübermittlung (en: Secure Messaging)
SSC	Sendefolgezähler (en: Send Sequence Counter)
SSCD	Sichere Signaturerstellungseinheit (en: Secure Signature Creation Device)
SW1-SW2	Statusbytes (en: Status bytes)
TDA	Terminalgeräuthentication (en: Terminal Device Authentication)
TDES	Triple-DES, diese Norm berücksichtigt nur die 2-Schlüssel-Variante
TOE	Evaluierungsgegenstand (en: Target of Evaluation)
TPDU	Dateneinheit des Übertragungsprotokolls (en: Transmission Protocol Data Unit)
TLS	Transportschichtsicherheit (en: Transport Layer Security)
TLV	Tag, Länge, Wert (en: Tag, Length, Value)
TSF	TOE-Sicherheitsfunktionen (en: TOE Security Functions)
TSP	TOE-Sicherheitsrichtlinien (en: TOE Security Policy)
x_p	x-Koordinate des elliptischen Kurvenpunkts P
y_p	y-Koordinate des elliptischen Kurvenpunkts P

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN ISO 3166-1:2007-03; *Codes für die Namen von Ländern und deren Untereinheiten — Teil 1: Codes für Ländernamen (ISO 3166-1:2006); Deutsche Fassung EN ISO 3166-1:2006*

— Leerseite —

English Version

Application Interface for Secure Elements for Electronic
Identification, Authentication and Trusted Services —
Part 1: Introduction and common definitions

Interface applicative des éléments sécurisés utilisés
comme dispositifs de création de signature
électronique qualifiée (cachet) —
Partie 1: Introduction et définitions communes

Anwendungsschnittstelle für sichere Elemente zur
elektronischen Identifikation, Authentisierung und
für vertrauenswürdige Dienste —
Teil 1: Einführung und allgemeine Definitionen

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: Avenue Marnix 17, B-1000 Brussels

Contents

Page

European foreword.....	5
Introduction	6
1 Scope	7
2 Normative references	7
3 Terms and definitions	7
4 Symbols and abbreviations	15
5 Management Summary	18
5.1 Motivation.....	18
5.2 What is in behind?.....	19
5.3 Use Cases	20
5.4 Privacy and Security.....	21
5.5 Overview - EU Directive and Regulation.....	21
5.6 Facts and Figures.....	22
Annex A (normative) Algorithm Identifiers — Coding and specification	23
Table A.1 — AlgIDs.....	24
Table A.2 — Coding of byte 3 and 4 (for hash calculation - byte 2 = '01' to '0F')	24
Table A.3 — Coding of byte 3 (for digital signature computation - byte 2 = '1x')	25
Table A.4 — Coding of byte 4 (for digital signature computation - byte 2 = '1x')	25
Table A.5 — Coding of byte 3 (for C/S authentication - byte 2 = '2x').....	25
Table A.6 — Coding of byte 4 (for C/S authentication - byte 2 = '2x').....	25
Table A.7 — Coding of byte 3 (for key decipherment - byte 2 = '3x').....	26
Table A.8 — Coding of byte 4 (for key decipherment - byte 2 = '3x').....	26
Table A.9 — Coding of byte 3 (for authentication protocol - byte 2 = '4x').....	26
Table A.10 — Coding of byte 4 (for authentication protocol - byte 2 = '4x')	28
Table A.11 — Coding of byte 3 (for digital signature verification - byte 2 = '9x').....	28
Table A.12 — Coding of byte 4 (for digital signature verification - byte 2 = '9x').....	28
Table A.13 — Coding of byte 3 (for role authentication - byte 2 = 'Ax').....	29
Table A.14 — Coding of byte 3 (for privacy features - byte 2 = 'Cx')	29
Table A.15 — Coding of byte 4 (for role authentication - byte 2 = 'Ax').....	29
Table A.16 — Coding of byte 4 (for privacy feature - byte 2 = 'Cx')	29
Table A.17 — 1-byte Algorithm-ID coding.....	30
Annex B (informative) OID values.....	32
B.1 OIDs for certificate signatures.....	32
Table B.1 — Object identifier values related to a public key in a certificate.....	32
B.2 OIDs for key transport protocol.....	32

Table B.2 — Object identifier values for the key transport protocol.....	33
B.3 OIDs for device authentication with privacy	33
Table B.3 — Object identifier values for device authentication with privacy	33
B.4 OIDs for password based mechanisms	34
Table B.4 — PACE OIDs	34
B.5 OIDs for mEAC protocol.....	34
B.5.1 OIDs for Chip Device Authentication	34
Table B.5 — Chip Device Authentication (DES/AES).....	34
B.5.2 OIDs for Terminal Device Authentication.....	35
Table B.6 — Terminal Authentication (RSA/ECDSA).....	35
B.6 OIDs for privacy protocols.....	36
B.6.1 OIDs for Restricted Identification.....	36
Table B.7 — OIDs for Restricted Identification.....	36
Table B.8 — OIDs for use in certificate extension.....	36
B.6.2 OIDs for Restricted Identification.....	36
Table B.9 — OIDs for use in auxiliary data verification.....	36
B.7 OIDs for mEAC based eServices - OIDs for Terminal Device Authentication in mEAC-based eServices	36
Table B.10 — OID values for the mEAC Terminal Authentication.....	36
B.8 OIDs for the PCA mechanism	37
Table B.11 — OID for the PCA mechanism.....	37
Annex C (informative) Build scheme for object identifiers defined by EN 419212	38
Figure C.1 — Build scheme for mEAC OIDs	39
Annex D (informative) Tutorial on Signature Technology	40
D.1 General	40
D.2 Signatures and keys	41
Table D.1 — Generating RSA keys.....	42
D.3 Signing documents	42
D.4 About certificates.....	43
D.5 The “chain of trust”	44
D.6 Multi step signature generation.....	44
D.6.1 General	44
D.6.2 Device authentication protocols	44
D.6.3 Secure Messaging.....	45
D.6.4 Password based device authentication	45
D.6.5 PIN entry	45
D.7 Signing the document.....	46

Annex E (informative) Guide to the EN 419212	47
E.1 From EN 14890 to EN 419212.....	47
E.2 The EU Regulation 910/2014 and the Directive 1999/93/EU.....	48
E.3 Secure Elements (SE)	48
E.4 Specific protection required for contactless integrated circuits	49
E.4.1 General.....	49
E.4.2 Eavesdropping attacks.....	49
E.4.3 Skimming attack.....	49
E.4.4 Relay attack.....	49
E.4.5 Denial of Service (DoS) attack	49
E.4.6 Countermeasures.....	50
E.5 The Human-Machine Interface.....	50
E.6 Communications with the ICC and with the user	50
E.7 Information that should be initially communicated by the ICC to the IFD	51
E.8 User agreement using PINs.....	51
E.9 PIN unlocking.....	52
E.10 PIN change	52
E.11 User agreement using biometric information	52
E.12 User control using a local display and a local keyboard	52
E.13 Card applications	53
E.13.1 General.....	53
E.13.2 eSign card application	53
E.13.3 Device authentication mechanisms.....	53
E.13.4 Document Decryption mechanisms	53
E.14 Signature-/Seal functions.....	53
E.14.1 General.....	53
E.14.2 Digital signature/seal creation	54
E.14.3 Digital signature verification.....	54
E.14.4 Identification and authentication service	54
Bibliography.....	56

European foreword

This document (EN 419212-1:2017) has been prepared by Technical Committee CEN/TC 224 “Furniture”, 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 March 2018, and conflicting national standards shall be withdrawn at the latest by March 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 419212-2, 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 electronic 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” [2].

A Secure Element (SE) compliant to the standard will be able to produce a “qualified electronic signature” that fulfils the requirements of Article of the Electronic Signature Regulation and therefore can be considered equivalent to a hand-written signature [2].

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.

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 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, clause 8.3.6 “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.