

DIN EN 419212-2



ICS 35.240.15

Einsprüche bis 2016-12-21
Ersatzvermerk
siehe unten

Entwurf

**Anwendungsschnittstelle für sichere Elemente zur elektronischen
Identifikation, Authentisierung und vertrauenswürdige Dienste –
Teil 2: Signatur- und Siegeldienste;
Englische Fassung FprEN 419212-2:2016**

Application Interface for Secure Elements for Electronic Identification, Authentication and
Trusted Services –
Part 2: Signature and Seal Services;
English version FprEN 419212-2:2016

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 419212-3:2016-11, E DIN EN 419212-4:2016-11 und
E DIN EN 419212-5:2016-11 als Ersatz für DIN EN 419212-2:2015-03 und DIN EN 419212-1:2015-03

Gesamtumfang 116 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (FprEN 419212-2:2016) 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 419212-2 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;
allgemeine Signaturdienste, welche vorher in Teil 1 waren, wurden in Teil 2 verschoben und um Siegeldienste ergänzt.

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 2: Signature and Seal Services

Anwendungsschnittstelle für sichere Elemente, die als
qualifizierte elektronische Signatur-
/Siegelerstellungseinheiten verwendet werden - Teil 2:
Signatur- und Siegeldienste

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.....	6
Introduction	7
1 Scope	8
2 Normative references	8
3 Terms and definitions	9
4 Symbols and abbreviations	9
5 Signature application.....	9
5.1 Application Flow.....	9
5.2 Trusted environment versus untrusted environment	11
5.3 Selection of ESIGN application.....	12
5.3.1 General	12
5.3.2 Exceptions for Secure Messaging.....	13
5.4 Selection of cryptographic information application	13
5.5 Concurrent usage of signature applications.....	13
5.5.1 General.....	13
5.5.2 Methods of channel selection	13
5.5.3 Security issues on multiple channels.....	13
5.6 Security environment selection	13
5.7 Key selection.....	14
5.8 Security Services.....	14
6 User verification	15
6.1 General.....	15
6.2 Knowledge based user verification	15
6.2.1 General	15
6.2.2 Explicit user verification	16
6.2.3 Password based mechanisms	17
6.2.4 Presentation formats.....	17
6.2.5 Retry and Usage counters	17
6.2.6 Password Change	18
6.2.7 Reset of RC and setting a new password.....	18
6.3 Biometric user verification.....	19
6.3.1 General	19
6.3.2 Retrieval of the Biometric Information Template	20
6.3.3 Performing the biometric user verification	21
6.3.4 Reset of RC	23
7 Digital Signature Service	23
7.1 General.....	23
7.2 Signature generation algorithms	24
7.3 Activation of digital signature service.....	24
7.4 General aspects.....	24

7.5	Signature Generation	26
7.5.1	General	26
7.5.2	No hashing in Card.....	26
7.5.3	Partial hashing.....	27
7.5.4	All hashing in ICC	28
7.6	Selection of different keys, algorithms and input formats	29
7.6.1	General	29
7.6.2	Restore an existing SE.....	29
7.6.3	Setting the Hash Template (HT) of a current Security Environment (SE)	30
7.6.4	Modify the Digital Signature Template (DST) of a current Security Environment (SE).....	31
7.7	Read certificates and certificate related information.....	31
7.7.1	General	31
7.7.2	Read certificate related CIOs	31
7.7.3	Read signer's certificate from ICC.....	32
7.7.4	Retrieval of the signer's certificate from a directory service	33
8	Password-based authentication protocols.....	33
8.1	General	33
8.2	Notation.....	34
8.3	Authentication steps.....	34
8.3.1	General	34
8.3.2	Step 1 — Reading the protocol relevant public parameters.....	36
8.3.3	Step 2 — Set PBM parameters and generate blinding point.....	37
8.3.4	Step 3 — Get encrypted nonce	38
8.3.5	Step 4.1 — Map nonce and compute generator point for generic mapping.....	38
8.3.6	Step 4.2 — Map nonce and compute generator point for integrated mapping.....	39
8.3.7	Step 5 — Generate session keys	41
8.3.8	Step 6 — Explicit key authentication.....	42
9	Secure Messaging.....	43
9.1	General	43
9.2	CLA byte.....	43
9.3	TLV coding of command and response message	43
9.4	Treatment of SM-Errors	44
9.5	Padding for checksum calculation.....	44
9.6	Send sequence counter (SSC)	44
9.7	Message structure of Secure Messaging APDUs.....	45
9.7.1	Cryptograms	45
9.7.2	Cryptographic Checksums.....	46
9.7.3	Final command APDU construction	49
9.8	Response APDU protection	50
9.9	Use of TDES and AES	54
9.9.1	TDES/AES encryption/decryption.....	54
9.9.2	CBC mode.....	55
9.9.3	Retail MAC with TDES.....	55
9.9.4	EMAC with AES.....	56
9.9.5	CMAC with AES.....	57
10	Key Generation	57
10.1	General	57
10.2	Signature key and certificate generation.....	58
11	Key identifiers and parameters.....	59
11.1	General	59
11.2	Key identifiers (KID)	60

11.2.1	General.....	60
11.2.2	Secret and private keys.....	60
11.3	Public Key parameters.....	60
11.3.1	General.....	60
11.3.2	RSA public key parameters.....	60
11.4	Diffie-Hellman key exchange parameters.....	60
11.5	Authentication tokens in the protocols mEACv2 and PCA	61
11.5.1	General.....	61
11.5.2	TDES.....	61
11.5.3	AES.....	61
11.5.4	Ephemeral Public Key Data Object	61
11.6	The compression function Comp()	61
11.7	DSA with ELC public key parameters.....	62
11.7.1	General.....	62
11.7.2	The plain format of a digital signature.....	62
11.7.3	The uncompressed encoding.....	63
11.8	ELC key exchange public parameters	63
12	AlgIDs, Hash- and DSI Formats.....	63
12.1	General.....	63
12.2	Algorithm Identifiers and OIDs.....	64
12.3	Hash Input-Formats	64
12.3.1	General.....	64
12.3.2	PSO:HASH without command chaining	65
12.3.3	PSO:HASH with command Chaining	65
12.4	Formats of the Digital Signature Input (DSI).....	66
12.4.1	General.....	66
12.4.2	DSI according to ISO/IEC 14888-2 (scheme 2)	66
12.4.3	Digest Info for SHA-X Hash:Digest Info SHA:Digest Info.....	68
12.4.4	DSI according to PKCS #1 V 2.x MGF function	70
12.4.5	DSA with DH key parameters.....	71
12.4.6	Elliptic Curve Digital Signature Algorithm - ECDSA.....	71
13	Files	71
13.1	General.....	71
13.2	File structure	71
13.3	File IDs.....	72
13.4	EF.DIR.....	72
13.5	EF.SN.ICC.....	73
13.6	EF.DH.....	73
13.7	EF.ELC.....	74
13.8	EF.C.ICC.AUT	74
13.9	EF.C.CA _{ICC} .CS-AUT.....	75
13.10	EF.C_X509.CH.DS.....	75
13.11	EF.C_X509.CA.CS (DF.ESIGN).....	75
13.12	EF.DM.....	76
14	Cryptographic Information Application	76
14.1	General.....	76
14.2	ESIGN cryptographic information layout example	79
14.2.1	General.....	79
14.2.2	EF.CIAInfo.....	79
14.2.3	EF.AOD.....	81
14.2.4	EF.PrKD.....	86
14.2.5	EF.PuKD	89

14.2.6 EF.CD.....	91
14.2.7 EF.DCOD.....	93
Annex A (normative) Security environments.....	98
A.1 General	98
A.2 Definition of CRTs (examples)	99
A.2.1 General	99
A.2.2 CRT for Authentication (AT)	99
A.2.3 CRT for Cryptographic Checksum (CCT)	101
A.2.4 CRT for Digital Signature (DST)	101
A.2.5 CRT for confidentiality (CT)	102
A.3 Security Environments (example).....	103
A.3.1 General	103
A.3.2 Security Environment #10	104
A.3.3 Security Environment #11	104
A.4 Coding of access conditions (example).....	104
A.4.1 General	104
A.4.2 Access Conditions	105
Annex B (informative) Seals and Signatures.....	106
B.1 General	106
B.2 Example of a seal creation/verification	106
B.3 Definition of a Seal versus signature	106
B.4 Verifying a seal vs. signature	107
B.5 Seal creation specifications.....	107
B.5.1 General	107
B.5.2 User verification.....	107
B.5.3 Automated sealing.....	107
B.5.4 Delegated sealing.....	107
B.5.5 Operating conditions.....	108
Annex C (informative) Remote Signatures	109
C.1 Introduction.....	109
C.2 Architecture.....	109
C.2.1 General	109
C.2.2 Static view.....	110
C.2.3 Dynamic View.....	110
Bibliography	112

European foreword

This document (FprEN 419212-2:2016) 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 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 ” [2] 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]

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

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 qualified signature creation devices covering

- Signature creation and mobile signature creation
- User verification
- Password based authentication

The specified mechanisms are suitable for other purposes like services in the context of [2].

The particular case of seal is also covered by the specification. The differences between seal and signature is exposed in Annex B. Annex B also explains how the mechanisms for SEs as qualified signature creation devices can be used for SEs as qualified seal creation devices.

Mobile signature is an alternative to the classical signature case which is performed by a secure element. Mobile signature is encouraged by the large widespread of mobile devices and the qualification authorized by the eIDAS Regulation [2]. The particular case of remote signature (or server signing) is covered by this specification in Annex C.

In the rest of this document, except Annex B, there will be no particular notion of a seal since it technically compares to the signature.

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, *Identification cards -- Integrated circuit cards -- Part 8: Commands for security operations*

ISO/IEC 7816-11:2004, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 7816-15, *Identification cards — Integrated circuit cards — Part 15: Cryptographic information application*

ISO/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO 11568-2:2012, *Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

ISO/IEC 14888-2:2008, *Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms*

ISO/IEC 19794-2:2005, *Information technology — Biometric data interchange formats — Part 2: Finger minutiae data*

ISO/IEC 15946-5, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation, 2009-12-15*

3 Terms and definitions

For the purposes of this document, terms and definitions apply as described in [NP1#2].

4 Symbols and abbreviations

For the purposes of this document, symbols and abbreviations apply as described in [NP1#3].

5 Signature application

5.1 Application Flow

Figure 1 shows an execution flow for a signature creation as it is mandated in [1].

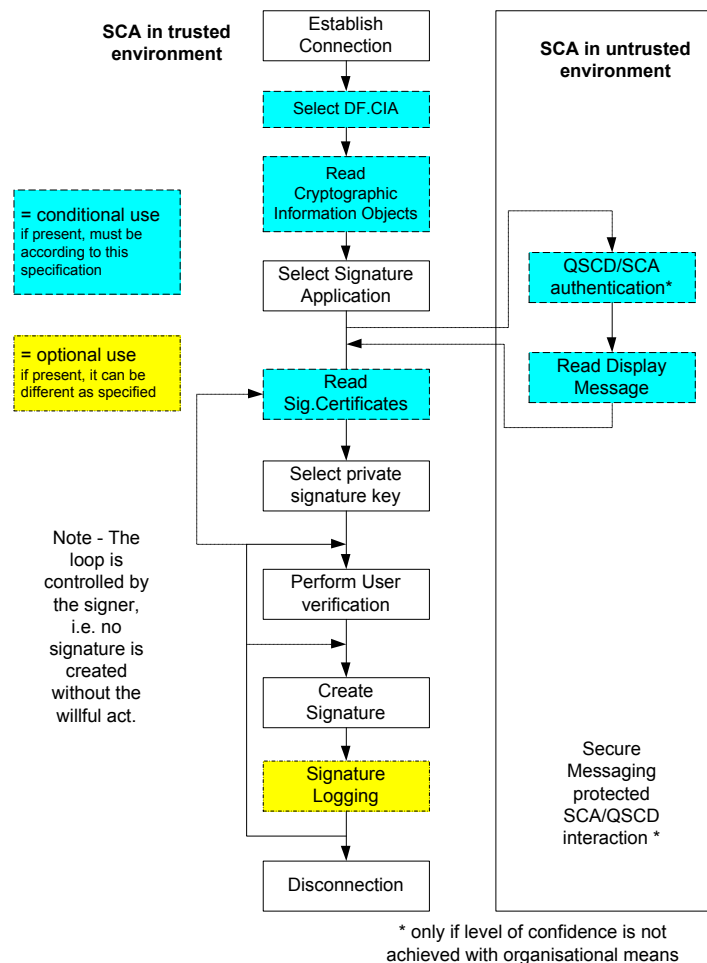


Figure 1 — Interaction sequences between SCA and QSCD in compliance with EU regulation

The corresponding technical implementation is given in this document and as various mechanisms are specified for device authentication and user verification with a number of resulting combinations, Figure 2 gives some example execution flows for typical signature cards. Each card implements a signature application and they differ in the combination of privacy and security features.

A card with a contact interface that is used in a trusted environment may not require any device authentication. In contrast, contactless cards are vulnerable to skimming and eavesdropping attacks and hence require protection.

Reading SN.ICC would be a possible start for a non-privacy protecting device authentication (e.g. [NP3#3.8]) whereas the card is addressed through contacts. For privacy protection (e.g. [NP3#3.5]/[NP3#3.6]) reading SN.ICC would not be desirable. Instead a password based mechanism may be involved which prevents the card being addressed unless a password, e.g. secret PIN or Card Access Number printed on the card is entered first. This is suitable for contactless cards which shall not allow communication without either the explicit act-of-will of the card holder or proof of legitimate physical possession of the card.

In multi-application environments device authentication may be performed on card (e.g. MF level) prior to application selection.

Whether for basic or additional services, a device authentication is always mandatory if the environment where the signature device is being used, is not known to be trustable. This is typical for public environment (e.g. airport, merchandise, POS). Only in trusted environments (e.g. company, campus) can device authentication be skipped.

The user can decide to abort the operation when (s)he is prompted to enter the PIN/password during user verification. Once the IFD has performed a device authentication, a display message (Personal Assurance Message – PAM) can be shown on the terminal screen to inform the cardholder that the environment is safe and s(he) may continue entering the PIN/password since the environment is safe. More information about this mechanism can be found in [NP3#3.13].

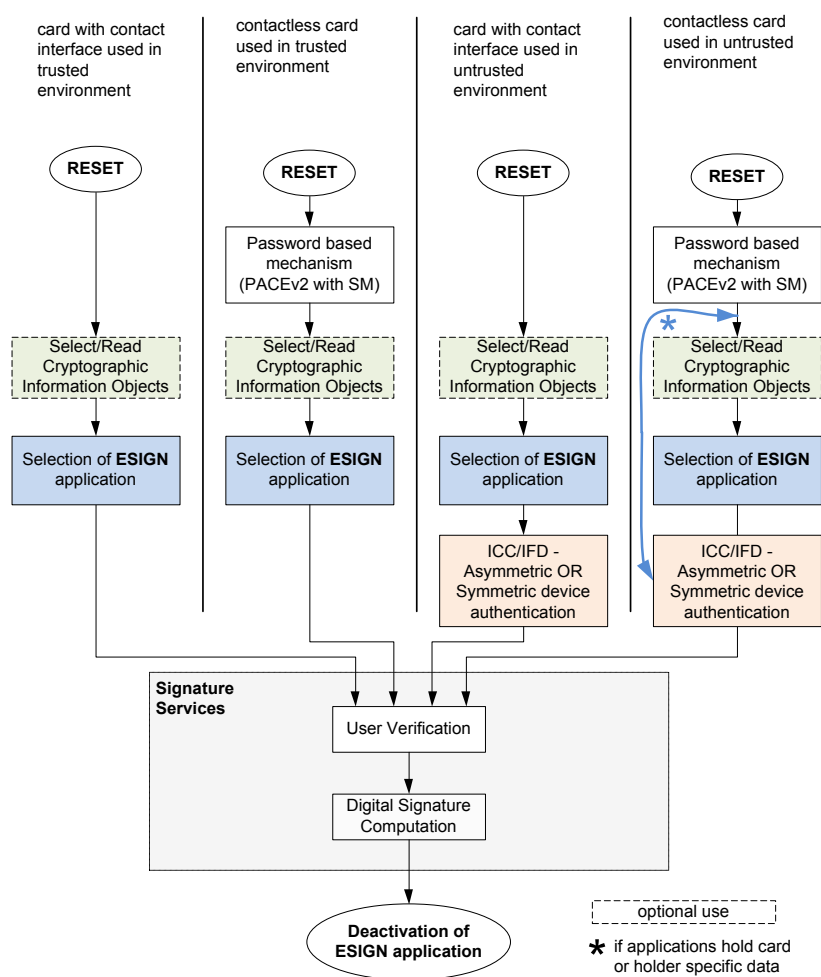


Figure 2 — Execute signature services

Figure 2 shows the selection of additional services in the context of the ESIGN application. User verification might be required for some of the additional services. The detailed access conditions are described in the appropriate security environments.

NOTE * For contactless case in untrusted environment, two choices are possible. Either the reading of CIA file (refer to 14) and the selection of application are done before device authentication, in conformity with Figure 1, or the device authentication is done first.

PKCS#15 takes into account privacy preserving measures involving EF.DIR so that to meet data minimizing property requirements (new component enhanced CIODDO under EF.DIR ensures that the IFD can access DF.CIA content only once security protocols i.e. PACE are fulfilled). This prevent the leakage of user information from CIA file and preserve privacy.

5.2 Trusted environment versus untrusted environment

According to the definitions in “trusted environment” [NP1#defTrustedEnvironment] and “untrusted environment” [NP1#defUntrustedEnvironment], this specification describes additional mechanisms in order to accomplish the required security as claimed in the protection profile [3]. The additional mechanisms according to this specification are:

- Device authentication
- Secure messaging

The following clause shows which authentication method is to be used for digital signatures in various privacy contexts, e.g. for contactless cards compared to contact cards.

Table 1 – Using authentication protocols in different context to secure signatures

Digital Signatures according to Chapter 7 can be performed after ...	Trusted Environment (private) to be secured by organisational means	Untrusted Environment (public) to be secured by cryptographical means
<i>Contact</i> communication channel has been established	As in generic case no authentication protocol necessary (see 5 “Signature application”)	Chip and Terminal Authentication, see device authentication protocols according [NP3#3].
<i>Contactless</i> communication channel has been established	Password Based authentication (PACEv2) with provision of secure channel by secure Messaging (restricted to specific types of passwords e.g. biometric passwords or passwords stored as keys inside the ICC (see 8 “Password-based authentication protocols”)	1. Password based authentication (PACEv2) with provision of secure channel by Secure Messaging 2. Chip and Terminal authentication e.g. see privacy and /or mEAC device authentication protocol according [NP3#3]. NOTE The RSA transport protocol [NP#3.8] is not suitable, unless the SN.ICC is set to a “dummy value” for privacy reasons.

5.3 Selection of ESIGN application

5.3.1 General

An ESIGN application is selected by its Application Identifier (AID) [see ISO/IEC 7816-5:2004]. The RID is registered by the ISO registration authority and has the following value:

A0 00 00 01 67.

The first 10 bytes of the AID have the following value

AID = A0 00 00 01 67 || “ESIGN” = A0 00 00 01 67 45 53 49 47 4E

with

Category = 'A.....' (international)

PIX = 'ESIGN' = 5 bytes

NOTE The maximum possible size of the PIX is 11 bytes (refer to ISO/IEC 7816-4, 12.2.3). The remaining 6 bytes may be used by CEN to distinguish between different implementations in the scope of this standard.

Table 2 — SELECT ESIGN application — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'A4' — SELECT
P1	'04' select by DF Name
P2	'00' or '02' return FCI info (see remark below)
Lc field	Length of command data field
Data field	AID.ESIGN — application identifier
Le field	'xx' expected response length

For the description of the SELECT command refer to ISO/IEC 7816-4 , 11.1.1.

Remarks

P2 It is left to the particular application to use other specified values from ISO/IEC 7816-4 , this specification does not mandate the retrieval of the file control information. JAVA cards, however, require P2 = '00' or P2 = '02'.

data field contains the AID.ESIGN as described above.

Table 3 — SELECT ESIGN application — response APDU

Response Parameter	Meaning
Data field	data according to P2. An FCI shall at least contain the DO '84' (DF Name)
SW1-SW2	Refer to ISO/IEC 7816-4

5.3.2 Exceptions for Secure Messaging

In case of an ICC without a MF, the SELECT by AID of an application shall always be issued by the terminal in clear, even if a secure messaging session is currently active. For such ICCs this SELECT by AID in clear shall not break the current secure messaging session (if any). For such ICCs this behaviour is necessary in order to allow the association of one applet instance to one application in a JAVA Card. Refer [NP3#3.12.2].

5.4 Selection of cryptographic information application

In compliance with ISO/IEC 7816-15 the cryptographic information application (CIA) belonging to the ESIGN application has the following AID:

AID.CIA_ESIGN = 'E8 28 BD 08 0F A0 00 00 01 67 || "ESIGN" (15 bytes)

The selection of the DF.CIA(ESIGN) is done with a DF Name as shown above.

5.5 Concurrent usage of signature applications

5.5.1 General

Concurrent usage of signature applications can be realized using the mechanisms of logical channel as defined in ISO/IEC 7816-4, 5.4.1

5.5.2 Methods of channel selection

The mechanism for channel selection is optional.

A channel may be selected by

- implicit selection with CLA byte of the SELECT command
- explicit selection with the MANAGE CHANNEL command

Both methods are described in ISO/IEC 7816-4 and will not be considered in this document.

5.5.3 Security issues on multiple channels

In order to access the resources of the ICC from another channel the 'shareable' bit shall be set in the FCI of the application DF.

Each invocation of an ESIGN-Application has its own security status.

5.6 Security environment selection

A signature card may contain more than one authentication- or signature key and one or more user reference data respectively. In this case the IFD needs to select the appropriate keys to be involved in authentication or signature operations and/or user verification (e.g. PIN, Password or biometric data) respectively. The MANAGE SECURITY ENVIRONMENT (SET) command (refer to ISO/IEC 7816-4, 11.5.11.) is used in order to specify the desired keys to be involved in the next operation.

A security environment selection by means of an MSE: RESTORE command, is applicable in the context of the following operations:

- User verification (PIN, Password or biometric).
- Signature creation as described in chapter 7 "Digital Signature Service".
- Device authentication as described in chapter [NP3#3].

- Key Generation as described in chapter 10 “Key Generation”.
- Verification of card verifiable certificates as described in chapter “CV_Certificates and Key Management” [NP3#5].
- Authentication services as described in “Client/Server Authentication” [NP5#6].
- Authentication services as described in chapter “Role Authentication” [NP5#7].
- Key decipherment as described in chapter “Symmetric key transmission between a remote server and the ICC” [NP5#10]
- Signature verification as described in chapter “Signature verification” [NP5#11]

The actual application of the MANAGE SECURITY ENVIRONMENT is discussed in the appropriate chapters.

5.7 Key selection

The selection of keys is performed by the MSE:SET command if not specified otherwise (e.g. in the parameters of the command header). An appropriate keyID is submitted and stored in the ICC in order to specify the key to be used with the next command(s). Key selection shall be done prior to a security operation unless the key was previously implicitly, or explicitly, selected.

A keyID is typically a number represented by one or more bytes describing a non-standardized value which is application- or operating system specific. The IFD may retrieve the link between a certificate and a corresponding KeyID from the DF.CIA application data as described in [34] “Cryptographic Information Application”.

5.8 Security Services

A security service is a set of QSCD functions that serve the purpose of signature generation, verification, authentication or key en-/decipherment.

Extended security services comprise the installation of data and keys, card life cycle management and other functionalities that extend the scope described in the EU regulation [1]. Extended services are out of the scope of this standard.

The two volumes of this document specify the following security services.

- **User verification** service, refer to chapter 6 “User verification”
- **Key generation**, refer to chapter 10 “Key Generation”
- **Device authentication** service including secure messaging, refer to chapter [NP3#3]
- **Digital signature service** for the advanced electronic signatures services of the cardholder, refer to chapter 7 “Digital Signature Service”
- **Authentication service** as required for specific authentication procedure, refer to [NP5#6]
- **Role authentication**, refer to chapter [NP5#7]
- **Encryption key decipherment** service, refer to [NP5#10]
- **Signature verification** service, refer to [NP5#11].

- **Auxiliary data** comparison, refer to [NP4#3.2]
- **Pseudonymity and Anonymity services** refer [NP4#4]

6 User verification

6.1 General

User verification is part of the application flow as described in Figure 2.

Two general methods of user verification are available:

- *Knowledge based*
- *Biometric based*

Each method provides the following verification mechanisms

- *Explicit* user verification
- *Implicit* user verification (Password Based Mechanisms (PBM))

Verification data, dedicated to protect the use of the private key for signature generation shall be applied in the ICC. If several private keys for signature generation are in the ICC, their use may optionally be protected by different verification data.

The protection of the client/server authentication function and the protection of the key decipherment function shall use separate (global or local according to the security policy) verification data.

The following commands, as defined in ISO/IEC 7816-4 are referenced:

- VERIFY
- CHANGE REFERENCE DATA
- RESET RETRY COUNTER
- GENERAL AUTHENTICATE

Regardless of the usage of these commands, at no time shall the signature key be used, unless it is protected by a preceding user verification

If knowledge based or biometric user verification is part of a Common Criteria evaluation a vulnerability analysis (AVA_VAN) shall be performed. The assessment of a knowledge based mechanism is a relatively simple and well established probabilistic analysis. For biometric authentication mechanisms the analysis is more complex for example proof that a claimed False Acceptance Rate (FAR) is met might need analysis of comprehensive fingerprint databases.

6.2 Knowledge based user verification

6.2.1 General

Knowledge based user verification requires a password to be entered by the user. The explicit verification is done with the VERIFY command in contrast to Password based mechanisms

To avoid brute-force attacks by an exhaustive search attack on the password the guessing probability should be bounded. The guessing probability depends on the minimal password length, the coding of the password (numerical or alpha-numerical password) and any retry counter that may be assigned to the password.

Choosing a retry count of 3 for a password of 6 numerical digits guarantees a guessing probability of $3/10^6$ if the numerical password is selected randomly. Selecting a so called trivial password dramatically lowers the security of the user verification.

Using a longer or a randomly chosen alpha-numerical password is more secure and can allow a larger retry counter for the same (or smaller) $3/10^6$ guessing probability. This depends on the range where the password is selected from, e.g. for randomly chosen alpha-numerical passwords of length 4 the key space contains $1,5 \times 10^7$ elements (refer to [42] chapter 8.1). For such a password a retry count of 10 is comparable with a 6 digit numerical password.

6.2.2 Explicit user verification

Applications in the European domain frequently restrict passwords to numbers only sometimes known as 'PIN'. This standard does not restrict passwords to numbers – specifications using this standard have the freedom to restrict the range of possible input characters to “numbers only” on their own.

Execution Flow 1 of 1

Table 4 — VERIFY command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'20' VERIFY
P1	'00'
P2	< KeyRef > password reference
Lc field	Length of command data field
Data field	< verification data >

The structure and coding of the VERIFY command refer to ISO/IEC 7816-4, 11.5.6.). The parameter P2 codes the reference value of the password.

If a password is referenced the reference is called “reference data qualifier” (refer to ISO/IEC 7816-4, 11.5.1).

This standard specifies the following KIDs.

KID = '8x' Key reference to local reference data for protection of the use of a private signature key (min. 6 digits or characters); the value of the KID and the purpose of the signature password shall be indicated in the cryptographic information objects.

Also other passwords may be of the type “local”.

KID = '0x' Key reference to global reference data; the value of the KID and the purpose of the password shall be indicated in the cryptographic information objects.

In order to allow the co-existence of EMV-applications and ESIGN-applications on the same ICC, only the three least significant bits should be used to differentiate keys. Refer to 6.5.12.2 – Table 23 of [23].

Password Based Mechanisms should implement PIN error- or usage counters in order to avoid exhaustive retries with the PIN or password.

Table 5 — VERIFY — response APDU

Response Parameter	Meaning
Data field	absent
SW1-SW2	Refer to ISO/IEC 7816-4

6.2.3 Password based mechanisms

Password based mechanisms provide an implicit user verification by performing a multi-step authentication protocol, see PACEv2 in Clause 8 “Password-based authentication protocols”. In contrast to the application as device authentication protocol the corresponding password is not printed on the card but known by the user only. A reset counter is recommended to be assigned to the password. A password change and a reset of the Reset Counter shall be done applying the RESET RETRY COUNTER command, see 6.2.6 “Reset of RC and setting a new password”.

6.2.4 Presentation formats

The data field codes the verification data in one of the following formats.

The password to be coded is '**12345**'

BCD coding

12	34	5F
-----------	-----------	-----------

ASCII coding

31	32	33	34	35
-----------	-----------	-----------	-----------	-----------

UTF8

31	32	33	34	35
-----------	-----------	-----------	-----------	-----------

special (e.g. language specific) characters will be different from ASCII coding

Half nibble bcd

F1	F2	F3	F4	F5
-----------	-----------	-----------	-----------	-----------

PIN in Format 2
PIN Block (see
ISO 9564-1

25	12	34	5F	FF	FF	FF	FF
-----------	-----------	-----------	-----------	-----------	-----------	-----------	-----------

Figure 3 — Example of coding '12345' in different presentation formats

Figure 3 demonstrates the coding when the different presentation formats are used. The actual presentation format may be retrieved from information presented in DF.CIA (refer to 14 “Cryptographic Information Application”), unless implicitly known.

National regulations may specify additional security requirements.

6.2.5 Retry and Usage counters

In order to avoid exhaustive search (brute force) attacks, the password should be protected by an appropriate retry or usage counter. For a password of 6 numerical digits the retry counter is typically 3 to achieve a guessing probability of $3/10^6$. For longer or randomly chosen alpha-numerical passwords a greater value of the retry counter can be selected with a similar or smaller guessing probability.

This depends on the range where the password is selected from, e.g. if the password is a randomly chosen string of 32 bytes, then a retry counter may even be not necessary. Passwords protecting the usage of signature keys shall consist, unless otherwise specified, of at least 6 digits or characters.

In order to avoid an exhaustive search attack on the password under a known resetting code, the resetting code should be protected by an appropriate usage counter with a usage counter limit with a low value (typically $U = 3$ for a resetting code of numerical digits).

After successful presentation, the appropriate retry counter is automatically reset to its initial value.

For the definition of the counter types refer to Clause 3.

6.2.6 Password Change

The CHANGE REFERENCE DATA command for changing the global password may be used under the same access conditions defined for the VERIFY command.

The change of DF-specific (local) password can only be performed after selection of the appropriate DF.

Execution Flow 1 of 1

Table 6 — Password Change — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'24' CHANGE REFERENCE DATA
P1	'00' no algorithm specified
P2	['0x' '8x'] KID of referenced password
Lc field	Length of command data field
Data field	< password > < new password >

For the description of the command refer to ISO/IEC 7816-4, 11.5.7.

The length of the existing Reference Data are known in the ICC, so that neither a delimiter nor padding for filling up fixed formats is necessary. The length of the new password therefore computes $L_{\text{new}} = L_c - L_{\text{old}}$.

Table 7 — Password Change — response APDU

Response Parameter	Meaning
Data field	absent
SW1-SW2	Refer to ISO/IEC 7816-4

6.2.7 Reset of RC and setting a new password

After N (N as specified by application) subsequent false presentations of the password, the password is locked and does not allow further usage of the protected functions.

With the ISO/IEC 7816-4 command RESET RETRY COUNTER, the cardholder can initiate the reset of the RC to its initial value N. The Resetting Code shall have a minimum length of 6 digits¹⁾.

¹⁾ 'digit' can also be a character as part of a password.

It is also possible to define a new password with the RESET RC command.

The reset of DF-specific (local) retry counter can only be performed after selection of the appropriate DF.

Table 8 — RESET RETRY COUNTER — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'2C' RESET RETRY COUNTER
P1	['00' .. '03']
P2	['0x' '8x'] KID of referenced password
Lc field	Length of command data field
Data field	see below

For the coding of the RESET RETRY COUNTER command refer to ISO/IEC 7816-4, 11.5.10.

The content of the data field depends on the value of P1. The RESET RETRY COUNTER shall not change the security status, i.e. for using the signature creation key a VERIFY command is still required.

P1 = '00' Resetting code followed without delimitation by new reference data

P1 = '01' Resetting code

P1 = '02' New reference data

P1 = '03' Data field absent

Table 9 — RESET RETRY COUNTER — response APDU

Response Parameter	Meaning
Data field	absent
SW1-SW2	See ISO/IEC 7816-4

After successful presentation of the Resetting Code, the retry counter of the referenced password is automatically reset to its initial value (typically $N = 3$) for a 6 numerical digit password.

6.3 Biometric user verification

6.3.1 General

The support of a biometric user verification (on-card matching) is optional. User verification shall always be done with a password. If biometric user verification is available in the IFD and ICC then the biometric user verification can be performed instead of password verification.

The following general methods of biometric user verification are available:

1. The **sensor is off-card**, whereas the following cases apply:
 - a. The biometric verification data are sent from the interface device to the ICC and is compared by a match on card mechanism.
 - b. The biometric **verification and reference data are transformed** by a suitable application specific mechanism as e.g. Fuzzy Vault [39] to password / PIN format.

The verification mechanism is then performed as used for passwords / PINs by means of the VERIFY command or a password based mechanism

2. The **sensor is on-card**, so there is no need to transmit the biometric verification data from the interface device to the ICC.

Transforming biometric data to a unique value (b.) has the consequence that the biometric algorithm is performed completely in the offcard application and the ICC only has to perform a user verification by means of direct comparison with yes / no response.

The users have the benefit that they do not have to remember their password because it is linked to their biometrics and usually to an additional randomizer. The security of this mechanism is, however, only as sound as the underlying biometric algorithm i.e. it is in general weaker than a password / PIN Comparison based on random passwords.

If biometric user verification is supported and the sensor is off-card, the Finger Minutiae Matcher compliant to ISO/IEC 19794-2 shall be used. The On-Card Biometric Comparison Format identified by the CBEFF format type '0005' shall be applied as encoding format for finger minutiae.

The ICC shall provide the IFD with information about the supported biometric verification service using a Biometric Information Template (BIT) compliant to ISO/IEC 7816-11 that shall be encoded as presented in Table 15. The BIT shall not contain a data object for minutiae order referenced by tag '82', i.e. the ICC shall not rely on an ordering procedure performed by the IFD.

6.3.2 Retrieval of the Biometric Information Template

Prior to the verification, the SCA may need information about:

- AlgID of the matching algorithm and key reference of the biometric reference data;
- biometric type (e.g. fingerprint);
- biometric type instance (e.g. left pointer finger enrolled);
- format owner of the biometric data;
- format type of the biometric data;
- on-/off-card sensor.

This information may be found in the DF.CIA description (refer to 14 “Cryptographic Information Application”).

Alternatively this information may be provided in the Biometric Information Template (BIT), refer to ISO/IEC 7816-11. The BIT may be present in the DF.CIA or be retrieved with the GET DATA command.

The enrolment process is out of the scope of this standard.

Table 10 — Retrieve Biometric Information Template(s) — command APDU (optional)

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'CA' GET DATA
P1-P2	'7F60' Example: Biometric Information Template
Le field	'00'

For the coding of the command GET DATA refer to ISO/IEC 7816-4, 11.4.3.

Table 11 — Retrieve Biometric Information Template(s) — response APDU (optional)

Response Parameter	Meaning
Data field	BIT (Value field of Biometric Information Template(s))
SW1-SW2	Refer to ISO/IEC 7816-4

For the format of the biometric information template refer to 6.3.3.3 “Biometric Templates”.

6.3.3 Performing the biometric user verification

6.3.3.1 General

Two situations have to be distinguished:

- Sensor **off**-card;
- Sensor **on**-card.

Secure messaging (refer to 9.7 “Message structure of Secure Messaging APDUs” is required when executing commands on biometric user verification with Sensor off-card.

6.3.3.2 Sensor off-card

The sensor is outside the ICC, i.e. the captured biometric data needs to be sent to the ICC for on-card matching.

The IFD retrieves the Biometric Information Template by means of a GET DATA command according to 6.3..The corresponding path attribute in the Cryptographic Information Application denotes the DF that shall be selected prior to this GET DATA command.

Then the IFD uses a VERIFY command to process the biometric data structured according to the biometric template.

Table 12 — Biometric user verification — command APDU (Biometric verification)

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'21' VERIFY
P1	'00'
P2	'xx' reference data qualifier according to 6.1.1.
Lc field	Length of command data field
Data field	< biometric data template > refer to Table 14

For the structure and content of the APDU refer to ISO/IEC 7816-4, 11.5.6.

Table 13 — Biometric user verification 2 of 2- response APDU

Response Parameter	Meaning
Data field	absent
SW1-SW2	Refer to ISO/IEC 7816-4

6.3.3.3 Biometric Templates

Table 14 — Biometric data template

Tag	Length	Value		
'7F 2E'	Var.	Biometric Data Template		
		Tag	Length	
		'81'	Var.	Biometric data with standardized format (primitive encoding)

Table 15 — Biometric Information Template

Tag	Length	Value					Presence				
'7F 60'	Var.	Biometric Information Template (BIT)									
		Tag	Length	Value							
		'83'	'01'	Reference data qualifier according to 6.1.1.					Mandatory		
		'A1'	Var.	Biometric Header Template (BHT) in compliance with CBEFF					Mandatory		
				Tag	Length	Value					
				'81'	'01'	'08' (fingerprint)			Mandatory		
				'82'	'01'	Biometric subtype (refer to ISO/IEC 7816-11:2004, Table C.3)			Mandatory		
				'87'	'02'	'0101' (ISO/IEC JTC 1/SC37)			Mandatory		
				'88'	'02'	'00 05'			Mandatory		
				'B1'	Var.	Biometric matching algorithm parameters					Optional
						Tag	Length	Value			
		'81'	'02'			Minimum number of minutiae required (1 byte, binary coding) Maximum number of minutiae accepted (1 byte, binary coding)					

6.3.3.4 Sensor on-card

For the on-card verification, the VERIFY command selects the biometric data reference through P2.

Execution Flow

Table 16 — Biometric verification — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'21' VERIFY
P1	'00' no algorithm specified
P2	['0x' '8'x] reference data qualifier acc. to 6.1.1.
Lc field	Length of command data field
Data field	'5F2E' '00' '4D' '00' empty verification DO and extended. header list DO

For the description of the command refer to ISO/IEC 7816-4, 11.5.6.

The length of the existing reference data are known in the ICC, so that neither a delimiter, nor padding for filling up fixed formats is necessary.

Table 17 — Biometric verification — response APDU

Response Parameter	Meaning
Data field	absent
SW1-SW2	Refer to ISO/IEC 7816-4 [2]

For the structure and content of the APDU refer to ISO/IEC 7816-4, 11.5.6.

6.3.4 Reset of RC

For resetting the RC refer to 6.1.5 "Reset of RC and setting a new password".

With respect to biometric reference data only the RESET RETRY COUNTER command variants that make use of P1 = '01' and P1 = '03' are specified in this document. The usage of the command variants with P1 = '00' and P1 = '02' is outside the scope of the document as the enrolment process is not defined in this document.

7 Digital Signature Service

7.1 General

This chapter is related to technical aspects of electronic signatures according section 3 "Electronic signature" of the EU Regulation [1].

NOTE For QES additional organizational aspects need to be considered like evaluation, certification, CA accreditation.

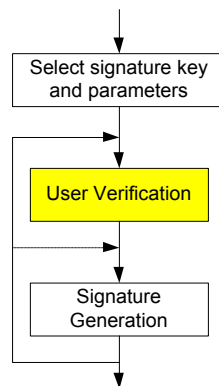
The technical requirements are fulfilled by the specifications of this standard.

7.2 Signature generation algorithms

For signature generation, algorithms as referenced in the current European and national algorithm catalogues shall be applied. Examples of existing documents are given in [4] [5] [6] [7].

7.3 Activation of digital signature service

In order to enable the digital signature service a user verification shall be applied prior to signature generation.



NOTE The loop is controlled by the signer, i.e. no signature is created without a willful act.

Figure 4 — User Verification of the Signer

Refer to Figure 1 for the overview of the signature generation flow.

A knowledge based interaction always expresses the explicit will of the card holder to sign a document whereas a biometric identification does not necessarily imply the intention to sign.

For the description of the user verification refer to 6 “User verification”.

7.4 General aspects

A digital signature process consists of several steps. Some of them are done outside the ICC, some of them are done inside the ICC, and some could be done on either side.

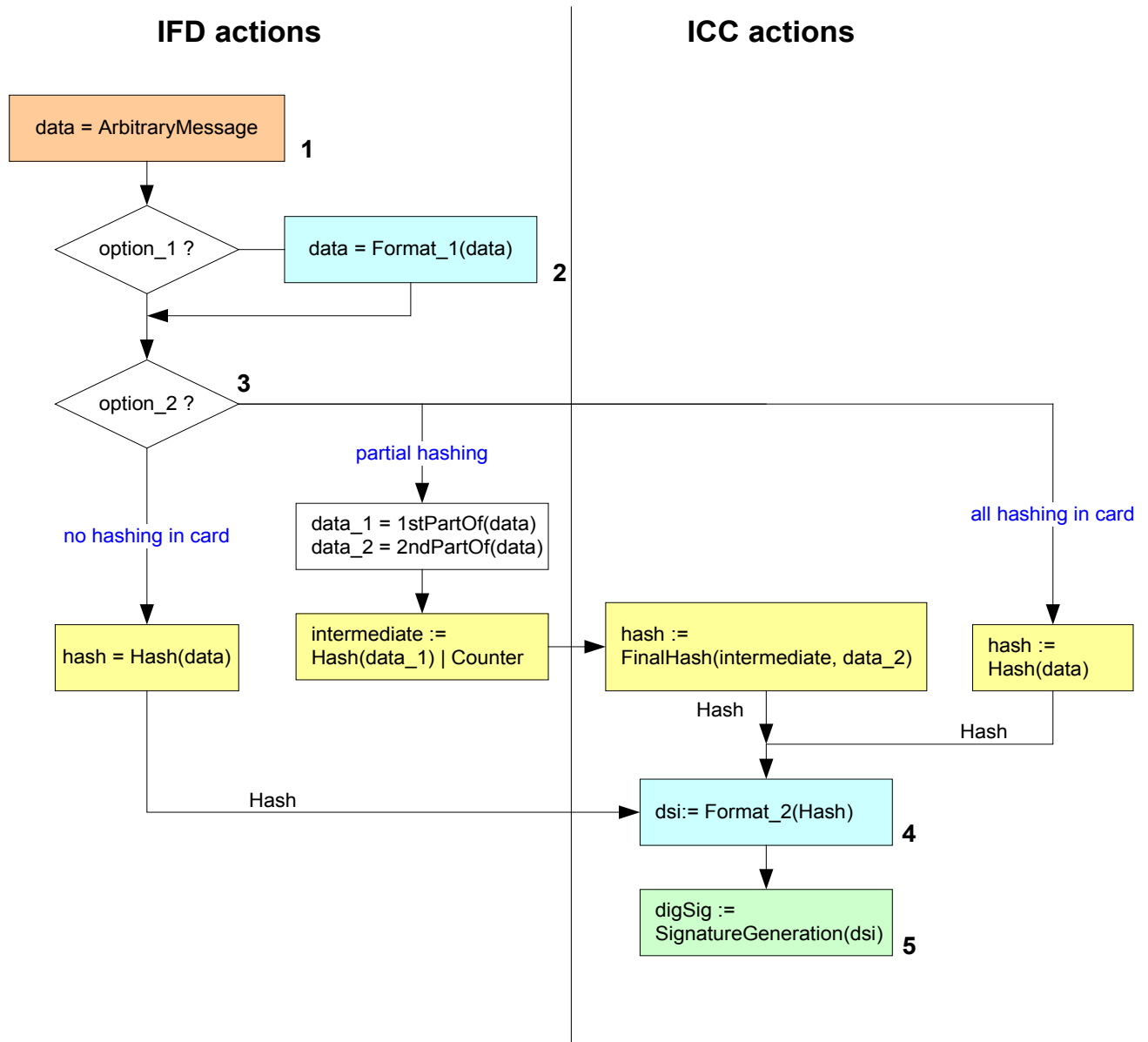


Figure 5 — Data-Flow chart for signature generation process (RSA Example)

Figure 5 shows an example of the alternatives to process a hash data signing. Signature input formatting aspects are not covered by Figure 5. The numbers 1..5 refer to the steps described below. The intermediate hash-code is the digest of preceding hash rounds followed by the big endian bit count. Only fully hashed blocks are transmitted, therefore the length of *data_1* (on partial hashing) is always a multiple of the digest size, related to the applied algorithm.

In principle, the signature generation process works as follows:

1. The signature generation process starts with an arbitrary message.
2. Optionally the original message is formatted in an application specific way. Typically, signature attributes and other format information besides the actual document to be signed, are added to the arbitrary message. The process of pre-formatting the data to be hashed is expressed as **Format_1** mechanism. The specification of the optional format mechanism **Format_1** is outside the scope of this document. It may require, e.g. also additional data flow from or to the ICC.

3. The data shall be hashed by applying a hash function which is on the list of the applicable hash functions. The hash-code could be considered as a check value of the data to be signed. Depending on *option_2* the hashing will be done either
 - completely outside the ICC,
 - partly outside and partly inside the ICC, thus data are split into two parts,
 - completely inside the ICC depending on the card functionality and the software organization.
4. Depending on the signature algorithm the *hash-code* shall be formatted by a format mechanism **Format_2**. Typically this is a *padding mechanism* as described in 12.4 “Formats of the Digital Signature Input (DSI)”. The result of this formatting is a *Digital Signature Input (dsi)*. Several format mechanisms have been defined, some of them are evaluated as “weak” and should not be used. The algorithm catalogues cover these aspects and propose formatting schemes which are approved until a specified date.
5. The final *dsi* (Digital Signature Input) is the string to be transformed by the signature algorithm. The result is the Digital Signature DS[<key >](*dsi*).

7.5 Signature Generation

7.5.1 General

Based on the example provided by Figure 5 different processes may be used to compute the hash value to be signed. The selection of the process may be based on security reasons, especially in case of RSA. If the ECDSA algorithm is used the typical flow will be “no hashing in card”.

7.5.2 No hashing in Card

The data to be signed is completely hashed outside the ICC. Depending on the algorithm the *hash-code* is transferred to and signed by the ICC using the PSO:COMPUTE DIGITAL SIGNATURE command.

Execution Flow 1 of 1

Table 18 — Signature computation (no hashing in ICC) — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'9E' COMPUTE DIGITAL SIGNATURE
P2	'9A' 'data to be signed'
Lc field	Length of command data field
Data field	data to be signed
Le field	'00'

For the structure and content of the APDU refer to ISO/IEC 7816-8, 5.2.

The response data field contains the *plain signature* without further TLV coding.

Table 19 — Signature computation (no hashing in ICC) — response APDU

Response Parameter	Meaning
Data field	plain signature without further TLV coding
SW1-SW2	Refer to ISO/IEC 7816-4

7.5.3 Partial hashing

The first part of the data to be signed is hashed outside the ICC. The intermediate hash-code is transferred to the ICC by the PSO:HASH command together with the remaining part of the data. Afterwards the signature is generated by the PSO:COMPUTE DIGITAL SIGNATURE command.

Execution Flow 1 of 2

Table 20 — Signature computation 1 of 2 (transfer intermediate hash-code) — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'90' hash
P2	'A0' input template for hash computation
Lc field	Length of command data field
Data field	'90' L ₉₀ < intermediate hash-code followed by big endian bit counter > '80' L ₈₀ < data to be hashed >

For the structure and content of the APDU refer to ISO/IEC 7816-8, 5.2.

For the content of the command data field or DO 'A0' refer to 12.3 "Hash Input-Formats".

The response data field is absent.

Table 21 — PSO-Hash response

Response Parameter	Meaning
Data field	absent
SW1-SW2	Refer to ISO/IEC 7816-4

Execution Flow 2 of 2

The second command performs a digital signature on the hashed value.

Table 22 — Signature computation 2 of 2 (compute signature) — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'9E' COMPUTE DIGITAL SIGNATURE
P2	'9A' data to be signed
Le field	'xx'

For the structure and content of the APDU refer to ISO/IEC 7816-8, 5.2.

The response data field contains the plain signature without further TLV coding.

Table 23 — PSO-COMPUTE DIGITAL SIGNATURE response

Response Parameter	Meaning
Data field	plain signature
SW1-SW2	Refer to ISO/IEC 7816-4

7.5.4 All hashing in ICC

The data to be signed is hashed inside the ICC. This is done by the PSO:HASH command. Finally the signature is generated by the PSO:COMPUTE DIGITAL SIGNATURE command.

Execution Flow 1 of 2

Table 24 — Signature computation 1 of 2 (all hashing in ICC) — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'2A' PSO:HASH
P1	'90' hash operation
P2	'80' plain value
Lc field	'xx'
Data field	plain data to be hashed

For the structure and content of the APDU refer to ISO/IEC 7816-8, 5.2.

The response data field is absent.

Table 25 — Signature computation 1 of 2 (all hashing in ICC) — response APDU

Response Parameter	Meaning
Data field	absent
SW1-SW2	Refer to ISO/IEC 7816-4

Execution Flow 2 of 2

The second command computes the digital signature.

Table 26 — Signature computation 2 of 2 (compute signature) — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'9E' COMPUTE DIGITAL SIGNATURE
P2	'9A' data to be signed
Le field	'00'

For the structure and content of the APDU refer to ISO/IEC 7816-8, 5.2.

The response data field contains the plain signature without further TLV coding.

Table 27 — PSO-COMPUTE DIGITAL SIGNATURE response

Response Parameter	Meaning
Data field	plain signature
SW1-SW2	Refer to ISO/IEC 7816-4
^a In the case of ECDSA the digital signature is calculated according to ISO/IEC 15946-5, for the format refer to [27] chapter A.7.4.1	

7.6 Selection of different keys, algorithms and input formats

7.6.1 General

If the ICC supports more than one key and an implicit selection is not available, then the private signature key needs to be selected.

If the ICC supports several digital signature algorithms or different Digital Signature Input formats (refer to 12 “AlgIDs, Hash- and DSI Formats” 69), then the algorithm or the DSI format respectively shall be selectable. However, it is possible that either (e.g. an algorithm), is implicitly specified if a key is selected.

It is further possible that an algorithm, a key or a signature input format is not implicitly known, nor uniquely specified.

In all of the above cases the appropriate parameter shall be selected explicitly with a MANAGE SECURITY ENVIRONMENT command as described in ISO/IEC 7816-4, 11.5.11.

This can be achieved by

- restoring an existing SE (refer to 7.6.2)
- modifying a KeyID/[AlgID] in a template (refer to 7.6.4)

7.6.2 Restore an existing SE

Execution Flow 1 of 1

Table 28 — MANAGE SECURITY ENVIRONMENT — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'22' MANAGE SECURITY ENVIRONMENT
P1	'F3' RESTORE
P2	SE# security environment number

For the structure and content of the APDU refer to ISO/IEC 7816-4, 11.5.11.

The response data field is absent.

Table 29 — MANAGE SECURITY ENVIRONMENT response

Response Parameter	Meaning
Data field	absent
SW1-SW2	Refer to ISO/IEC 7816-4

NOTE The actual SE# is described in Part 5 of this specification.

7.6.3 Setting the Hash Template (HT) of a current Security Environment (SE)

If a hash algorithm is not implicitly known by the ICC, it shall be selected with the MANAGE SECURITY ENVIRONMENT command.

Execution Flow 1 of 1

Table 30 — Set hash template — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'22' MANAGE SECURITY ENVIRONMENT
P1	'41' SET (hash template acc. to p2)
P2	'AA' CRT for HT (hash template)
Lc field	'xx' length of the following data
Data field	'80' L80 yy AlgID

For the structure and content of the APDU refer to ISO/IEC 7816-4, 11.5.11.

The response data field is absent.

Table 31 — Set hash template — response

Response Parameter	Meaning
Data field	absent
SW1-SW2	Refer to ISO/IEC 7816-4

7.6.4 Modify the Digital Signature Template (DST) of a current Security Environment (SE)

If a signing key is not implicitly known by the ICC, it shall be selected with the MANAGE SECURITY ENVIRONMENT command. Optionally an algorithm identifier can be supplied in order to specify variations of the algorithm (e.g. for padding formats).

Execution Flow 1 of 1

Table 32 — Selection of signature key — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'22' MANAGE SECURITY ENVIRONMENT
P1	'41' SET for signature creation
P2	'B6' CRT for DST
Lc field	'xx' length of the following data
Data field	'84' L84 xx ['80' L80 yy] KeyID [AlgID]

For the structure and content of the APDU refer to ISO/IEC 7816-4, 11.5.11.

For the algorithm ID refer to [NP1#A].

The response data field is absent.

Table 33 — Selection of signature key — response

Response Parameter	Meaning
Data field	absent
SW1-SW2	Refer to ISO/IEC 7816-4

7.7 Read certificates and certificate related information

7.7.1 General

If more than one signature key is present in the ICC, the user may need to select the signature key for a certain signature creation. In the user certificates are fields indicating whether it is a private or professional certificate. Therefore the user may want to evaluate these fields in order to select the proper certificate and with it the associated private key. In the CIOs there is a link between a certificate and the associated private key and an indication where the certificates are to be found (in the ICC or on a server), in the latter case the ICC will provide an URL and optionally the certificate serial number.

7.7.2 Read certificate related CIOs

CIOs related to certificates denote which certificates are present in the ICC or are to be found on a server and which private key corresponds to the public key present in the certificate (refer to Clause 16).

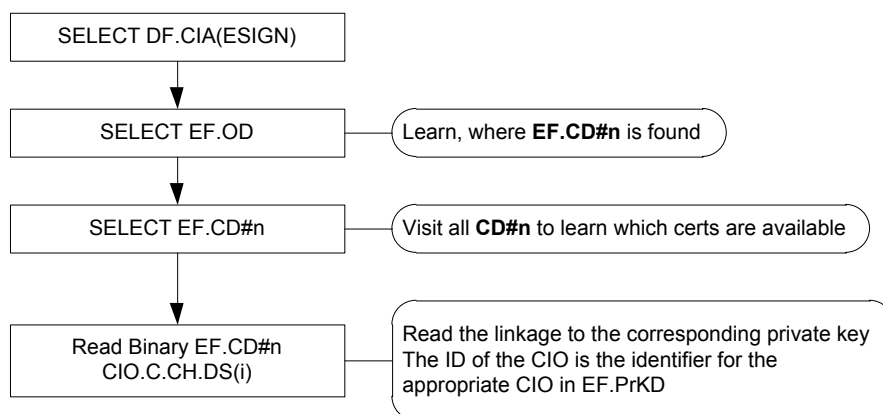


Figure 6 — Reading certificate related information (certificate is present in the ICC)

The certificate related information contains the ID of the appropriate CIO in EF.PrKD which contains the KeyID of the private key in question.

7.7.3 Read signer's certificate from ICC

If present, the corresponding certificate file(s) may be read from the ICC. Prior to reading the appropriate file needs to be selected. The location (e.g. path or (short) EF identifier) is denoted in the corresponding CIO in EF.CD#n.

Certificate related information is stored in EF.C.CH.DS(i). After selection of EF.C.CH.DS(i) according to the path information found in the CIO.C.CH.DS(i), either the certificate or related information may be read from the EF.C.CH.DS(i).

The actual content to be expected in EF.C.CH.DS(i) is described in DF.CIA. If no other description is available, then EF.C.CH.DS(i) contains the certificate.

Execution Flow 1 of 1

Table 34 — Read signer's certificate — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'B0' READ BINARY
P1-P2	'xxxx' Offset
Le field	'00' read all data

The response data field codes the data content of EF.C.CH.DS(i).

Table 35 — Read signer's certificate — response APDU

Response Parameter	Meaning
Data field	Data.EF.C.CH.DS(i)
SW1-SW2	Refer to ISO/IEC 7816-4

The command and response APDUs are described in ISO/IEC 7816-4, 11.2.3.

The structure and coding of EF.C.CH.DS(i) will typically be an X.509 certificate format, but it could also be some other format. The actual format is application specific and out of the scope of this standard.

NOTE If the expected length exceeds the length of the APDU response data field then the READ BINARY might have to be called several times with an appropriate offset.

7.7.4 Retrieval of the signer's certificate from a directory service

In order to retrieve the signer's certificate through a directory service the card holder shall identify the certificate uniquely. This reference value information may be retrieved by reading the appropriate CIO.C.CH.DS from the DF.CIA(ESIGN) according to Figure 6.

According to ISO/IEC 7816-15 "8.7.2 X.509 certificate attributes" the appropriate data object CIO.C.CH.DS contains the following fields.

X509CertificateAttributes:: = SEQUENCE

```
{  
  
    value ObjectValue { Certificate },  
  
    subject Name OPTIONAL,  
  
    issuer [0] Name OPTIONAL,  
  
    serialNumber CertificateSerialNumber OPTIONAL,  
  
    ... – For future extensions  
  
}
```

The interpretation of the components shall be as follows:

X509CertificateAttributes.value: The value shall be a *Referenced Value* either identifying a file containing a DER encoded certificate at the given location, or a URL pointing to some location where the certificate can be found in ISO/IEC 7816-15.

8 Password-based authentication protocols

8.1 General

Protocols of the password-based authentication family (PBM) aim at providing a confidential communication and a password-based authentication of an ICC and an IFD. The ICC may be either a contact or contact-less ICC and the IFD could be a remote server interacting with the ICC through a local reader. Both parties share a common weak low entropy password. The protocols basically follow four steps:

1. Getting an (encrypted) nonce
2. Mapping the nonce (onto the point of an elliptic curve)
3. Performing a Diffie-Hellman key agreement
4. Explicit mutual authentication