

DIN EN 419212-5

ICS 35.240.15

Entwurf

Einsprüche bis 2016-12-21
Ersatzvermerk
siehe unten

**Anwendungsschnittstelle für sichere Elemente zur elektronischen
Identifikation, Authentisierung und für vertrauenswürdige Dienste –
Teil 5: Vertrauenswürdige elektronische Dienste;
Englische Fassung FprEN 419212-5:2016**

Application Interface for Secure Elements for Electronic Identification, Authentication and
Trusted Services –
Part 5: Trusted eService;
English version FprEN 419212-5:2016

Anwendungswarnvermerk

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

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

Stellungnahmen werden erbeten

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

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

Ersatzvermerk

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

Gesamtumfang 62 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (FprEN 419212-5:2016) 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 419212-5 soll die Implementierung des europäischen rechtlichen Rahmens für elektronische Signaturen unterstützen, indem Sie die funktions- und sicherheitsbezogenen Anforderungen an sichere Elemente (z.B. Chipkarten) zur Verwendung als qualifizierte elektronische Signaturerstellungseinheit (en: Qualified electronic Signature Creation Device, QSCD) entsprechend den Bedingungen der Europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt definiert.

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

Die Normenreihe DIN EN 419212 besteht aus fünf Teilen:

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

Das Präsidium des DIN hat mit seinem Beschluss 1/2004 festgelegt, dass von dem in den Regeln der europäischen Normungsarbeit von CEN/CENELEC verankerten Grundsatz, wonach Europäische Normen in den drei offiziellen Sprachen Deutsch, Englisch, Französisch veröffentlicht werden, in begründeten Ausnahmefällen abgewichen und auf die deutsche Sprachfassung verzichtet werden kann. Daher wurden von dieser Norm nur die Begriffe übersetzt (siehe Nationaler Anhang NA).

Änderungen

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

- a) Normenreihe wurde aufgrund der eIDAS Verordnung umstrukturiert;
- b) Die zusätzlichen Dienste aus dem früheren Teil 2 wurden in diesen neuen Teil 5 übernommen.

English Version

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 5: Trusted eService

Anwendungsschnittstelle für sichere Elemente, die als qualifizierte elektronische Signatur-/Siegelerstellungseinheiten verwendet werden - Teil 5: Vertrauenswürdige elektronische Dienste

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.....	5
Introduction	6
1 Scope	7
2 Normative references.....	7
3 Terms and definitions	7
4 Abbreviations and notation.....	7
5 Additional Service Selection.....	7
6 Client/Server Authentication	11
6.1 General.....	11
6.2 Client/Server protocols	11
6.3 Steps preceding the client/server authentication	12
6.4 Padding format	12
6.4.1 PKCS #1 v 1-5 Padding.....	12
6.4.2 PKCS #1 V 2.x (PSS) Padding.....	13
6.4.3 Building the DSI on ECDSA.....	14
6.5 Client/Server protocol	14
6.5.1 General.....	14
6.5.2 Step 1 — Read certificate	15
6.5.3 Step 2 — Set signing key for client/server internal authentication	16
6.5.4 Step 3 — Internal authentication	17
6.5.5 Client/Server authentication execution flow.....	19
6.5.6 Command data field for the client server authentication	20
7 Role Authentication.....	21
7.1 Role Authentication of the card	21
7.2 Role Authentication of the server	21
7.3 Symmetrical external authentication	21
7.3.1 Protocol	21
7.3.2 Description of the cryptographic mechanisms	25
7.3.3 Role description.....	26
7.4 Asymmetric external authentication	26
7.4.1 Protocol based on RSA.....	26
8 Symmetric key transmission between a remote server and the ICC.....	29
8.1 Steps preceding the key transport.....	29
8.2 Key encryption with RSA	29
8.2.1 PKCS#1 v1.5 padding.....	29
8.2.2 PKCS#1 v1.5 padding.....	31
8.2.3 OAEP padding	31
8.2.4 Execution flow	32
8.3 Diffie-Hellman key exchange for key encipherment.....	34
8.3.1 General.....	34
8.3.2 Execution flow	36
9 Signature verification	38

9.1	General	38
9.2	Signature verification execution flow	38
9.2.1	General	38
9.2.2	Step 1: Receive Hash	39
9.2.3	Step 2: Select verification key	40
9.2.4	Step 3: Verify digital signature	41
10	Certificates for additional services	41
10.1	File structure.....	41
10.2	File structure.....	42
10.3	EF.C_X509.CH.DS.....	42
10.4	EF.C.CH.AUT	42
10.5	EF.C.CH.KE.....	43
10.6	Reading Certificates and the public key of CAs.....	43
11	APDU data structures.....	43
11.1	Algorithm Identifiers.....	43
11.2	Algorithm Identifiers.....	43
11.3	CRTs.....	44
11.3.1	General	44
11.3.2	CRT DST for selection of ICC's private client/server auth. key	44
11.3.3	CRT AT for selection of ICC's private client/server auth. key.....	44
11.3.4	CRT CT for selection of ICC's private key.....	44
11.3.5	CRT DST for selection of IFD's public key (signature verification)	45
	Annex A (informative) Security Service Descriptor Templates.....	46
A.1	General	46
A.2	Security Service Descriptor Concept	46
A.3	SSD Data Objects	47
A.3.1	General	47
A.3.2	DO Extended Header List, tag '4D'	47
A.3.3	DO Instruction set mapping (ISM), tag '80'	47
A.3.4	DO Command to perform (CTP), tag '52' (refer to ISO/IEC 7816-6).....	47
A.3.5	DO Algorithm object identifier (OID), tag '06' (refer to ISO/IEC 7816-6)	48
A.3.6	DO Algorithm reference, tag '81'	48
A.3.7	DO Key reference, tag '82'	48
A.3.8	DO FID key file, tag '83'	48
A.3.9	DO Key group, tag '84'	48
A.3.10	DO FID base certificate file, tag '85'	48
A.3.11	DO FID adjoined certificate file, tag '86'	48
A.3.12	DO Certificate reference, tag '87'	48
A.3.13	DO Certificate qualifier, tag '88'	48
A.3.14	DO FID for file with public key of the certification authority PK(CA), tag '89'	49
A.3.15	DO PIN usage policy, tag '5F2F'	49
A.3.16	DO PIN reference, tag '8A'	49

A.3.17 DO Application identifier (AID), tag ‘4F’ (refer to ISO/IEC 7816-6).....	49
A.3.18 DO CLA coding, tag ‘8B’	49
A.3.19 DO Status information (SW1-SW2), tag ‘42’ (refer to ISO/IEC 7816-6)	49
A.3.20 DO Discretionary data, tag ‘53’ (refer to ISO/IEC 7816-6)	50
A.3.21 DO SE number, tag ‘7B’	50
A.3.22 DO SSD profile identifier, tag ‘8D’	50
A.3.23 DO FID mapping, tag ‘8E’	50
A.4 Location of the SSD templates	50
A.5 Examples for SSD templates	50
Annex B (informative) Example of DF.CIA.....	52
Bibliography	60

European foreword

This document (FprEN 419212-5:2016) 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” [22].

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 ” [22] and therefore can be considered equivalent to a hand-written signature.

This standard consists of five parts:

Part 1: “Introduction and common definitions” describes the history, application context, market perspective and a tutorial about the basic understanding of electronic signatures. It also provides common terms and references valid for the entire 419212 series. [NP1#1]

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

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

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

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

Introduction

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

The European Committee for Standardization (CEN) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning the mapping function given in [NP2#8.2.5] 8.2.5 “Step 4.2 - Map nonce and compute generator point for integrated mapping”.

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

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

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

Morpho
11, boulevard Galliéni
92445 Issy-les-Moulineaux Cedex

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

1 Scope

Part 5 of this series contains Identification, Authentication and Digital Signature (IAS) services in addition to the QSCD mechanisms already described in Part 2 to enable interoperability and usage for IAS services on a national or European level.

It also specifies additional mechanisms like key decipherment, Client Server authentication, identity management and privacy related services.

2 Normative references

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

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

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

ISO/IEC 9796-2:2010, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

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

3 Terms and definitions

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

4 Abbreviations and notation

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

5 Additional Service Selection

Additional services are typically used in the context of applications that use digital signatures.

A well known additional service is the **client/server authentication**. In this case, the ICC is used as a crypto toolbox, e.g. in order to encrypt a challenge with a private key, being stored in the ICC. This is particularly helpful in applications, where a tamper resistant device is required for client/server authentication. A secure ICC has the necessary tamper resistant quality and may therefore be used efficiently to support the application in this context.

Document decryption is another known service which may be performed by the IFD. A terminal application receives a document, typically encrypted with a symmetric key. The symmetric key is also provided encrypted with a public key. The ICC contains the appropriate private key, deciphers the symmetric key and returns it to the terminal application.

While the typical usage of a signature card is the generation of a digital signature, an application might want to verify a signature with a public key, being stored in the ICC. In this case an additional service is invoked for **signature verification**.

ICCs used as national identification cards, travel documents or driving licences generally provide additional applications to enable **eServices** (e.g. eGovernment, eBusiness, ...) including an E-SIGN

application. In the eID card context new privacy issues are to be put into account, e.g. user tracking, data minimizing, unlinkability of transactions or domain specific identifiers. This standard specifies privacy preserving protocols and mechanisms as additional services.

Additional services provided in the ICC mandate the existence of an appropriate security environment. Associated security environments are described in the [NP2#A].

In addition to the descriptive information found in DF.CIA (refer to [NP2#14]) information might be required that can be presented in Security Service Descriptors. The concept of Security Service Descriptors is described in the Annex A.

A user verification may be required prior to the usage of additional services. The password for this user verification shall be different from the password used for the signature generation. This is to maintain the purpose of the signature generation password for the sole purpose of a 'declaration of will' in the case of a signature generation.

Figure 1 shows an execution flow for an additional service. The corresponding technical implementation is given in this document.

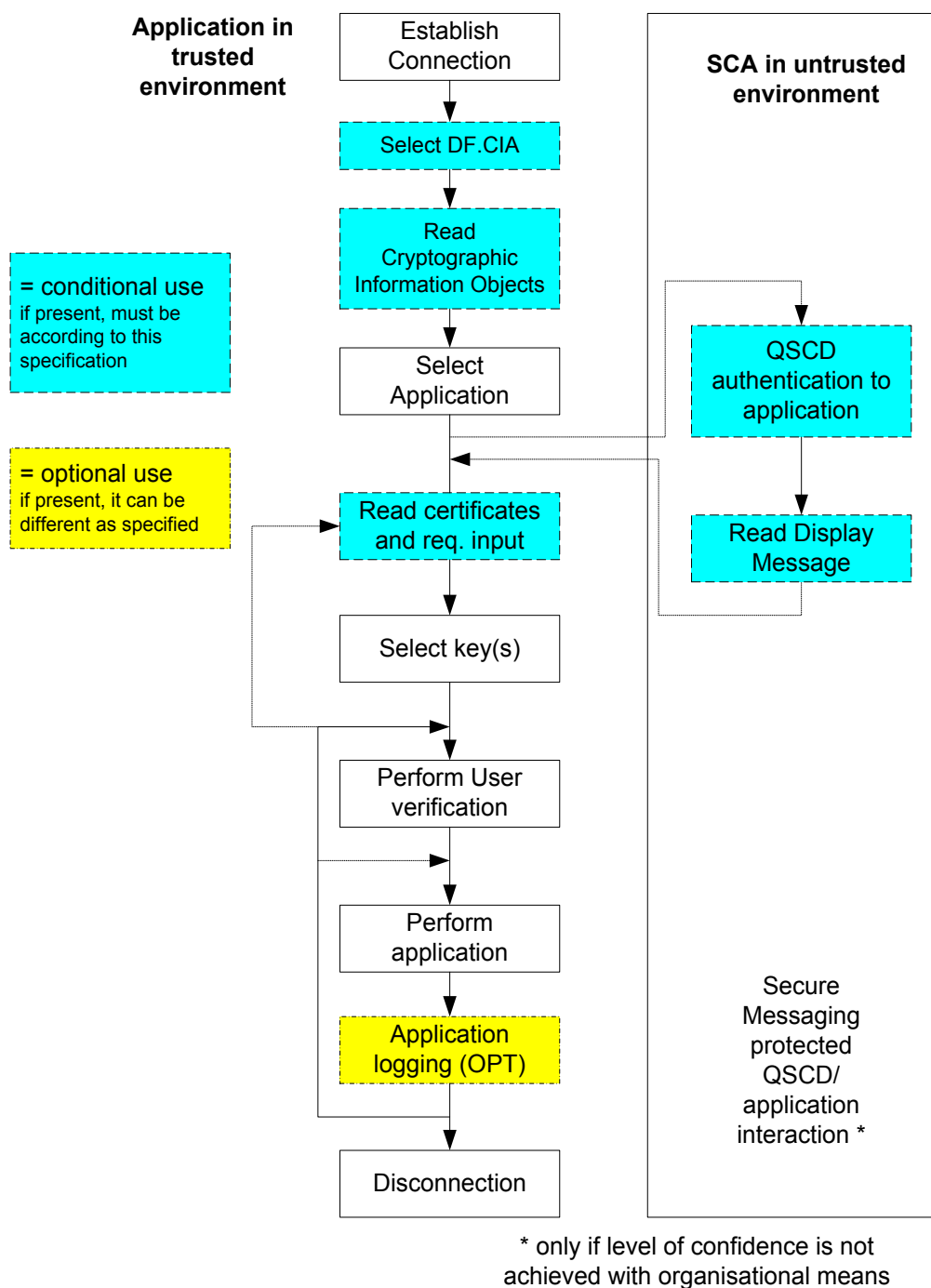


Figure 1 — Interaction sequences between application and QSCD

As the standard specifies various mechanisms for device and user authentication with a number of resulting combinations, Figure 2 shows execution flows for typical signature cards in different security and privacy context.

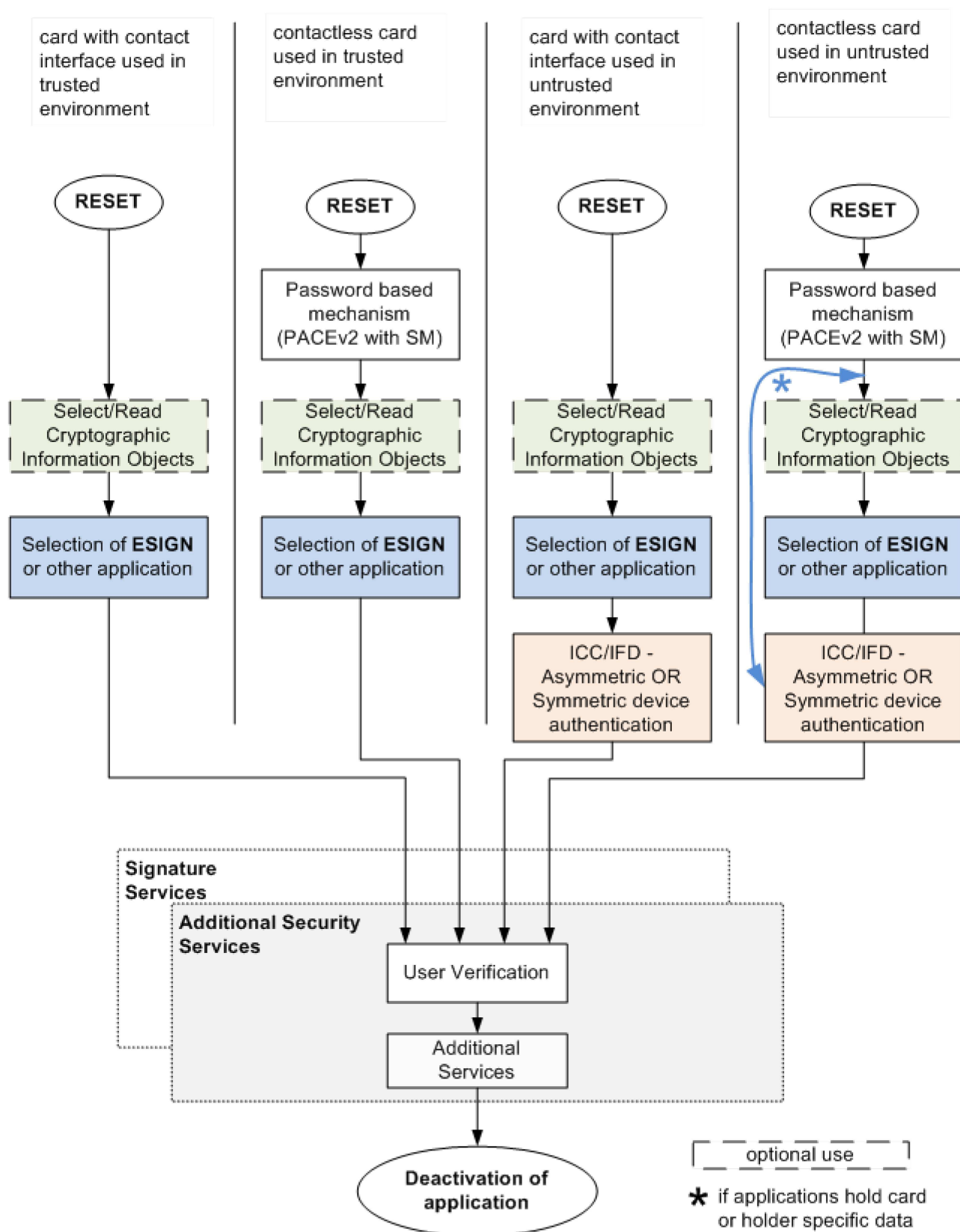


Figure 2 — Example of additional service selection

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.

For security reasons the cryptographic information objects shall not reveal any information which could be used to associated the ICC to the password. If this cannot be guaranteed, the device authentication shall be done prior to reading the cryptographic information objects to avoid that an unauthorized IFD may later reuse that association for further attacks.

Alternatively other measures shall be taken to avoid such an attack. 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 prevents the leakage of user information from CIA file and preserves privacy..

6 Client/Server Authentication

6.1 General

For proving access rights to components such as servers, a PK based authentication procedure has to be performed. Such client/server Authentication (refer to “C/S internal authentication”) is a process, independent from the requirement of device authentication.

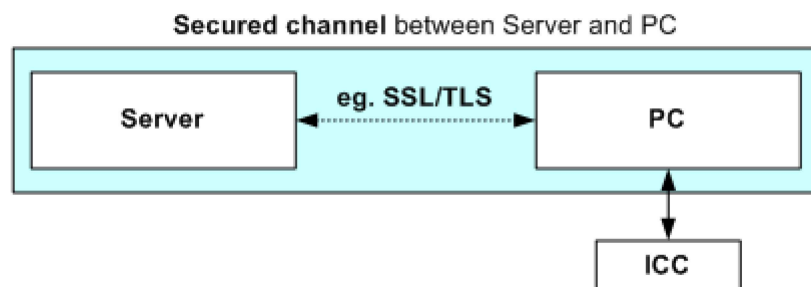


Figure 3 — Example of client/server authentication

In the above example client/server authentication establishes a secured channel between a remote server and a PC. The ICC will be used as a cryptographic toolbox in order to provide the cryptographic functionality to the PC.

This specification does not support the authentication of the server (“C/S external authentication”). The server’s certificate as well as the server protocol is application specific and therefore out of the scope of this document.

6.2 Client/Server protocols

This specification only covers the case, where the ICC performs a digital signature computation on the authentication input contained in the data field of an INTERNAL AUTHENTICATE (COMPUTE DIGITAL SIGNATURE) command. The input is formatted before the private key for authentication is used to form the signature.

The key pair used for client/server authentication shall be different from the device authentication keys and signature generation keys respectively. The public part of this key pair, stored with the distinguished name of the cardholder, is certified by a certificate (typically X.509 [8]). Such a certificate is not interpreted by the ICC.

Relevant authentication procedures are e.g.:

- the PK Kerberos protocol (for logon authentication)
- the SSL/TLS protocol
- the SSH protocol

All the above protocols are based on the same cryptographic algorithms. In particular they all use PKCS #1 padding format in the case of RSA. This specification describes the PKCS #1 padding and C/S authentication based on ECDSA.

6.3 Steps preceding the client/server authentication

The steps preceding a client/server authentication are application specific. Hence this specification does not mandate the existence of those steps.

The access conditions proposed in [NP2#A] specify a user verification as a mandatory step prior to client/server authentication.

The reference to the password to be used for user verification in the context of client/server authentication is described in the information of DF.CIA.

6.4 Padding format

6.4.1 PKCS #1 v 1-5 Padding

The DSI generation according to PKCS #1 v1.5 uses the padding scheme defined for the EMSA-PKCS-v1_5 encoding defined in [1] Section 9.2 (starting with step 3 of the encoding method). The padding is applied directly to the Authentication Input T.

Figure 4 shows an example for DSI generation according to PKCS #1 V1.5. In case of RSA, the authentication input T is formatted according to [1] PKCS #1, Version 2.1, Chapter 9.2 “EMSA-PKCS1-v1-5”. For particular Authentication input T refer to 6.4.5.

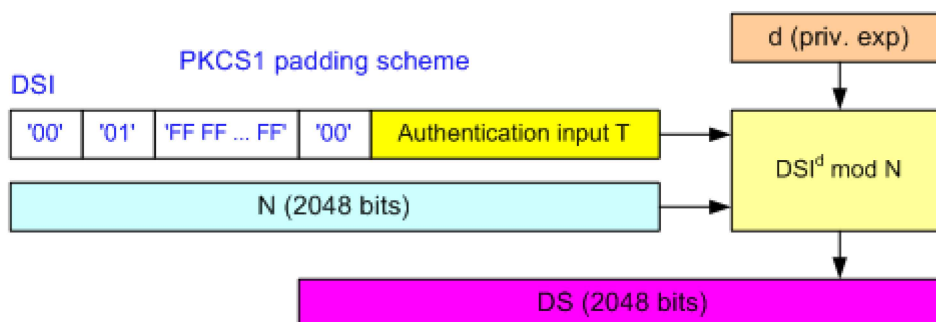


Figure 4 — Example for 2048 bit DSI according to PKCS #1 V1.5

The padding is realized through an octet string consisting of octets with value 'FF' (length ≥ 8). Due to security reasons the authentication input shall be smaller or equal to 33 % of the length of the modulus. The formatted octet string shall consist of k octets where k is the length in octets of the modulus of the private key for authentication.

The digest info is described in [NP2#12.3.3].

6.4.2 PKCS #1 V 2.x (PSS) Padding

The DSI generation according to PKCS1-PSS uses the padding scheme defined for the EMSA-PSS encoding defined in [1] section 9.1. There are two modes of operation, each indicated by a separate set of algorithm IDs see [NP1#TblA.17].

The DSI format according to PKCS #1 V 2.1 has the following structure. The message M represents the authentication input T.

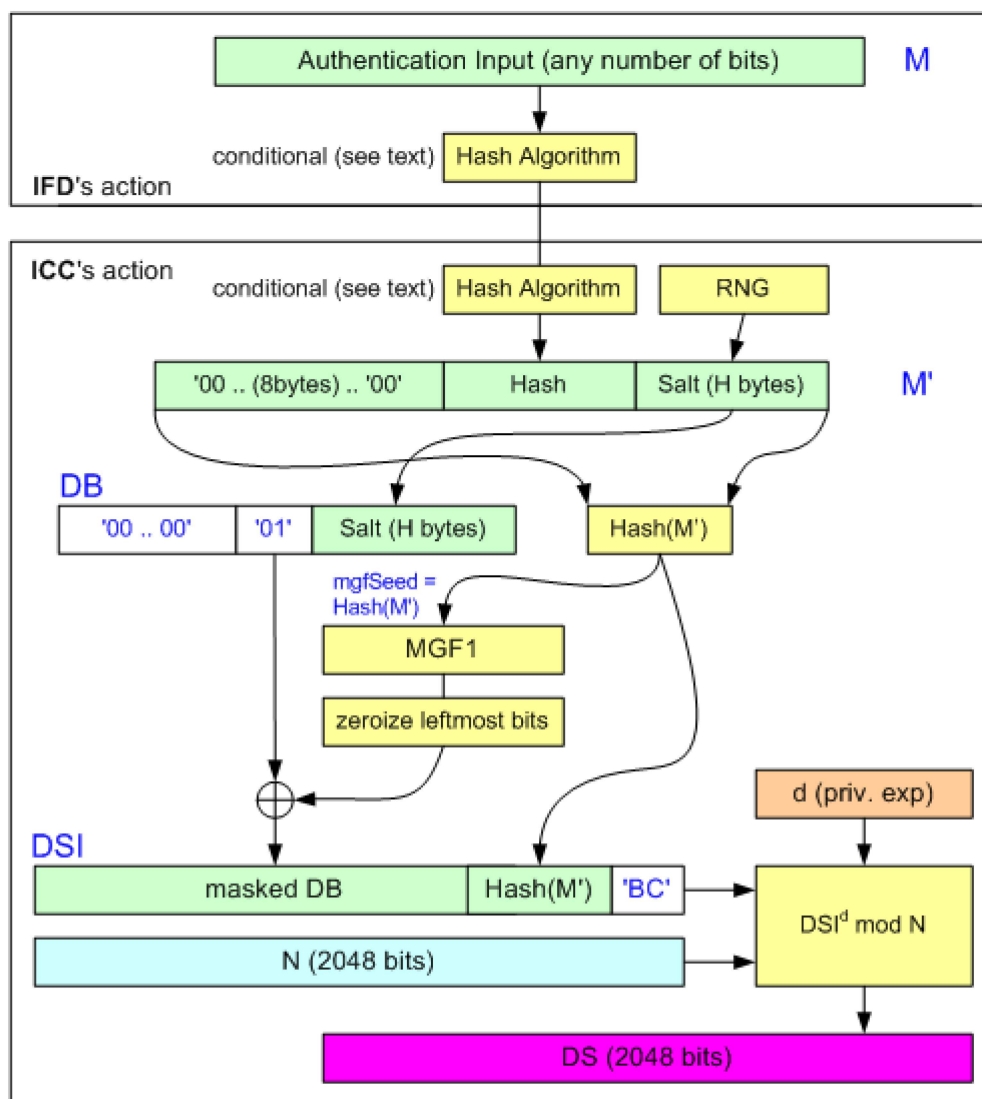


Figure 5 — Example for 2048 bit DSI according to PKCS #1 V2.1

Figure 5 shows an example for the DSI computation according to PKCS #1 V2.1. Building the first hash in the IFD is an optional step and appropriate, if the message M is large and the transmission of this large message M would required exhaustive data transmission to the ICC.

The hashing function used in MGF1 is the same as the one used to hash the authentication input. The $[8 \times \text{Key.ModulusByteLength} - (\text{Key.ModulusBitLength} - 1)]$ leftmost bits of the output of the MGF1 function are set to zero to provide a DSI input being arithmetically smaller than the modulus N. The MGF1 function is described in [1] [PKCS 1 — V.2.1, Chapter B.2.1].

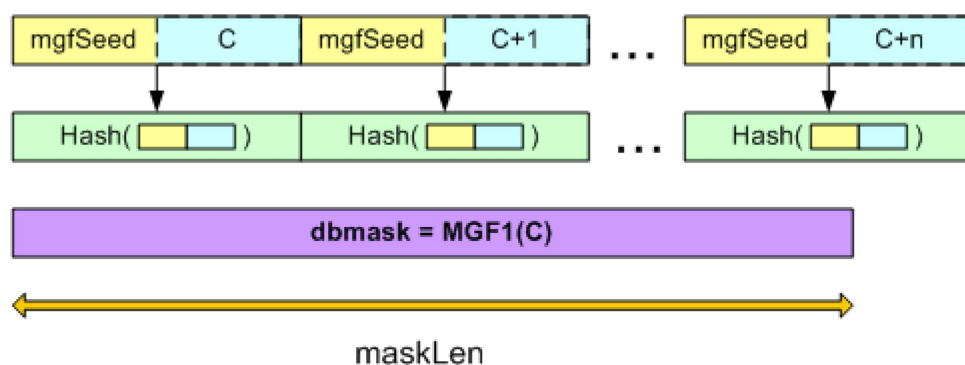


Figure 6 — Example for the mask generating function MGF1

Figure 6 shows an example for the mask generating function MGF1. The length of the salt is identical to the Digest Length H of the hash algorithm. The length of DB computes from

$$\text{Length}(DB) = N - H - 1 = \text{maskLen}.$$

where N is the byte length of the modulus and H is the digest length of the hash algorithm.

The length of the *mgfSeed* is identical to H , the length of C is 4 bytes as specified [1]. The initial value of C is zero. The concatenation of [*mgfSeed* || C] pairs is right truncated at the length of *maskLen* to build *dbmask*.

The $[8 \times \text{Key.ModulusByteLength} - (\text{Key.ModulusBitLength} - 1)]$ leftmost bits of *dbmask* are set to zero to provide a DSI input being arithmetically smaller than the modulus N .

The hashing function used in MGF1 is the same as the one used to hash the authentication input. The $[8 \times \text{Key.ModulusByteLength} - (\text{Key.ModulusBitLength} - 1)]$ leftmost bits of the output of the MGF1 function are set to zero to provide a DSI input being arithmetically smaller than the modulus N .

Table 1 — Digital Signature Input (DSI) — Format acc. to PKCS #1 V 2.x

T	L	V
—	—	masked DB = $DB \oplus \text{MGF1}(\text{Hash}(M'), \text{Key.ByteLength} - H - 1)$ Hash (M') 'BC' = Padding according to ISO/IEC 9796-2 (option 1)

6.4.3 Building the DSI on ECDSA

No hash shall be internally computed by the ICC. The size of the DSI shall not be greater than the size of the order of the base point (this point is relevant in particular for elliptic curves whose prime length is not a multiple of eight bits – e.g. P-521).

6.5 Client/Server protocol

6.5.1 General

Table 2 shows the execution flow of the RSA client/server authentication. This specification covers only the internal authentication.

Table 2 — Client/Server authentication flow

Stage	Step	IFD	Transmission	ICC
1	—	... preceding steps(e.g. user verification) that are application specific for client/server authentication		application specific protocol flow
INTERNAL AUTHENTICATION — server (IFD) authenticates client (ICC)				
2	1	READ BINARY of certificate (typically X.509)		certificate
	2	MSE:SET PrK.CH.AUT		
	3	INTERNAL AUTHENTICATE or COMPUTE DIGITAL SIGNATURE		
Client (ICC) is authenticated to server (IFD)				
3	—	... subsequent steps that are application specific to present client/server authentication		not specified in this document

6.5.2 Step 1 — Read certificate

If the IFD does not already have the client's (ICC) authentication certificate, it may read it from a global data file EF.C.CH.AUT. The client's certificate C.CH.AUT may contain public algorithm quantities which depend on the client/server authentication algorithm.

Execution Flow

Table 3 — Read EF.C.CH.AUT — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'B0' READ BINARY
P1	'85' Example: SFI = 05
P2	'00' offset = 0
Le field	'00'

For the structure and content of the APDU refer to ISO/IEC 7816-4:2013, 11.2.3.

The structure and coding of C.CA_{ICC}.CS_{AUT} may be as described in section [NP3#5.13log], but it could also be some other certificate format unknown to the ESIGN application. The actual format is application specific and out of the scope of this standard.

Table 4 — Read EF.C.CH.AUT — response

Response Parameter	Meaning
Data field	EF.C.CH.AUT plain data as stored in EF
SW1-SW2	Refer to ISO/IEC 7816-4

Unless the READ BINARY selects the file using a short EF Identifier (SFI), an appropriate SELECT(EF) command shall be executed prior to reading the file.

6.5.3 Step 2 — Set signing key for client/server internal authentication

The MSE command sets the keyID of the ICC's client/server private authentication key to be used for the following computation of the digital signature.

Execution Flow

Table 5 — Select key reference for internal authentication - command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'22' MANAGE SECURITY ENVIRONMENT
P1	'41' SET for internal authentication
P2	'A4'
Lc field	'xx'
Data field	CRT data field with AlgID (PrK.CH.AUT) and KeyRef(PrK.CH.AUT)

For the structure and content of the APDU refer to ISO/IEC 7816-4:2013, 11.5.11.

The structure and coding of the key reference data are specified in 11.2.2.

In order to avoid ambiguity the hashing function MGF1 shall be indicated in the AlgID.

The response data field is empty.

Table 6 — Select key reference for internal authentication — response

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

Alternatively the COMPUTE DIGITAL SIGNATURE command can be used.

Alternative Execution Flow

Table 7 — Select key reference for internal authentication — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'22' MANAGE SECURITY ENVIRONMENT
P1	'41' SET for internal authentication
P2	'B6' digital signature DST
Lc field	'xx'
Data field	CRT data field with AlgID (PrK.CH.AUT) and KeyRef(PrK.CH.AUT)

For the structure and content of the APDU refer to ISO/IEC 7816-4:2013, 11.5.11.

The structure and coding of the key reference data are specified in 11.3.2.

The response data field is empty.

Table 8 — Select key reference for internal authentication — response

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

6.5.4 Step 3 — Internal authentication

The IFD sends a challenge in the data field of the INTERNAL AUTHENTICATE command. The ICC computes a signature over the challenge by using its private key, that was selected in the preceding step.

Execution Flow

Table 9 — INTERNAL AUTHENTICATE — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	'88' INTERNAL AUTHENTICATE
P1	'00' no algorithm information
P2	'00' key reference — none
Lc field	'xx'
Data field	data authentication input see below (Table 13 to Table 17)
Le field	'00'

For the structure and content of the APDU refer to ISO/IEC 7816-4:2013, 11.5.2.

The digital signature input format is described in 6.4.5 .

The algorithms usable for client server authentication are described in 11.2.

The response data contains the signature.