SLOVENSKI STANDARD
SIST EN 419212-5:2018

01-julij-2018

Nadomešča:
SIST EN 419212-1:2015
SIST EN 419212-2:2015

Uporabniški vmesnik za varnostne elemente za elektronsko identifikacijo, avtentikacijo in zanesljivost storitev - 5. del: Zaupnost e-storitev

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

Interface applicative des éléments sécurités pour les services électroniques d'identification, d'authentification et de confiance - Partie 5 : Services électroniques de confiance

Ta slovenski standard je istoveten z: **EN 419212-5:2018**

ICS:

35.240.15	Identifikacijske kartice. Čipne kartice. Biometrija	Identification cards. Chip cards. Biometrics

SIST EN 419212-5:2018 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419212-5

April 2018

ICS 35.240.15

Supersedes EN 419212-1:2014, EN 419212-2:2014

English Version

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

Interface applicative des éléments sécurités pour les services électroniques d'identification, d'authentification et de confiance - Partie 5 : Services électroniques de confiance

Anwendungsschnittstelle für sichere Elemente zur elektronischen Identifikation, Authentisierung und für vertrauenswürdige Dienste - Teil 5: Vertrauenswürdige elektronische Dienste

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

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

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

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword ... 4
Introduction ... 5
1 Scope ... 6
2 Normative references ... 6
3 Terms and definitions ... 6
4 Abbreviations and notation ... 6
5 Additional Service Selection ... 6
6 Client/Server Authentication ... 10
6.1 General ... 10
6.2 Client/Server protocols ... 10
6.3 Steps preceding the client/server authentication ... 11
6.4 Padding format ... 11
6.4.1 PKCS #1 v 1-5 Padding ... 11
6.4.2 PKCS #1 V 2.x (PSS) Padding ... 12
6.4.3 Building the DSI on ECDSA ... 13
6.5 Client/Server protocol ... 13
6.5.1 General ... 13
6.5.2 Step 1 — Read certificate ... 14
6.5.3 Step 2 — Set signing key for client/server internal authentication ... 15
6.5.4 Step 3 — Internal authentication ... 16
6.5.5 Client/Server authentication execution flow ... 18
6.5.6 Command data field for the client server authentication ... 19
7 Role Authentication ... 20
7.1 Role Authentication of the card ... 20
7.2 Role Authentication of the server ... 20
7.3 Symmetrical external authentication ... 20
7.3.1 Protocol ... 20
7.3.2 Description of the cryptographic mechanisms ... 24
7.3.3 Role description ... 25
7.4 Asymmetric external authentication ... 25
7.4.1 Protocol based on RSA ... 25
8 Symmetric key transmission between a remote server and the ICC ... 28
8.1 Steps preceding the key transport ... 28
8.2 Key encryption with RSA ... 28
8.2.1 General ... 28
8.2.2 PKCS#1 v1.5 padding ... 30
8.2.3 OAEP padding ... 30
8.2.4 Execution flow ... 31
8.3 Diffie-Hellman key exchange for key encipherment ... 33
8.3.1 General ... 33
8.3.2 Execution flow ... 35
9 Signature verification ... 37
9.1 General ... 37
9.2 Signature verification execution flow ... 37

9.2.1 General 37
9.2.2 Step 1: Receive Hash 37
9.2.3 Step 2: Select verification key 39
9.2.4 Step 3: Verify digital signature 39

10 Certificates for additional services 40
10.1 File structure 40
10.2 File structure 41
10.3 EF.C_X509.CH.DS 41
10.4 EF.C.CH.AUT 41
10.5 EF.C.CH.KE 42
10.6 Reading Certificates and the public key of CAs 42

11 APDU data structures 42
11.1 Algorithm Identifiers 42
11.2 General 42
11.3 CRTs 43
11.3.1 General 43
11.3.2 CRT DST for selection of ICC's private client/server auth. key 43
11.3.3 CRT AT for selection of ICC's private client/server auth. key 43
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) 44

Annex A (informative) Security Service Descriptor Templates 45

Annex B (informative) Example of DF.CIA 51

Bibliography 58

European foreword

This document (EN 419212-5:2018) has been prepared by Technical Committee CEN/TC 224 “Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment”, the secretariat of which is held by AFNOR.

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

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

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

This standard supports services in the context of **e**lectronic **ID**entification, **A**uthentication and Trust **S**ervices (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.

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

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

Part 4: “Privacy specific Protocols” describes functions and services to provide privacy to identification services.

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

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

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

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

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

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

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

Morpho

11, boulevard Galliéni

92445 Issy-les-Moulineaux Cedex

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

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 7816-8:2016, *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*

PKCS #1 v2.1:2002, RSA Cryptography Standard, RSA Laboratories[1]

3 Terms and definitions

For the purposes of this document, the terms and definitions apply as described in EN 419212-1.

4 Abbreviations and notation

For the purposes of this document, the symbols and abbreviations apply as described in EN 419212-1.

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**.

[1] Available at www.rsasecurity.com/rsalabs/pkcs/pkcs-1/ http://www.rsa.com/rsalabs/node.asp?id=2125

ICCs used as national identification cards, travel documents or driving licences generally provide additional applications to enable **eServices** (e.g. eGovernment, eBusiness, …) including an ESIGN 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 EN 419212-2:2017, Annex A.

In addition to the descriptive information found in DF.CIA (refer to EN 419212-2, clause 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.

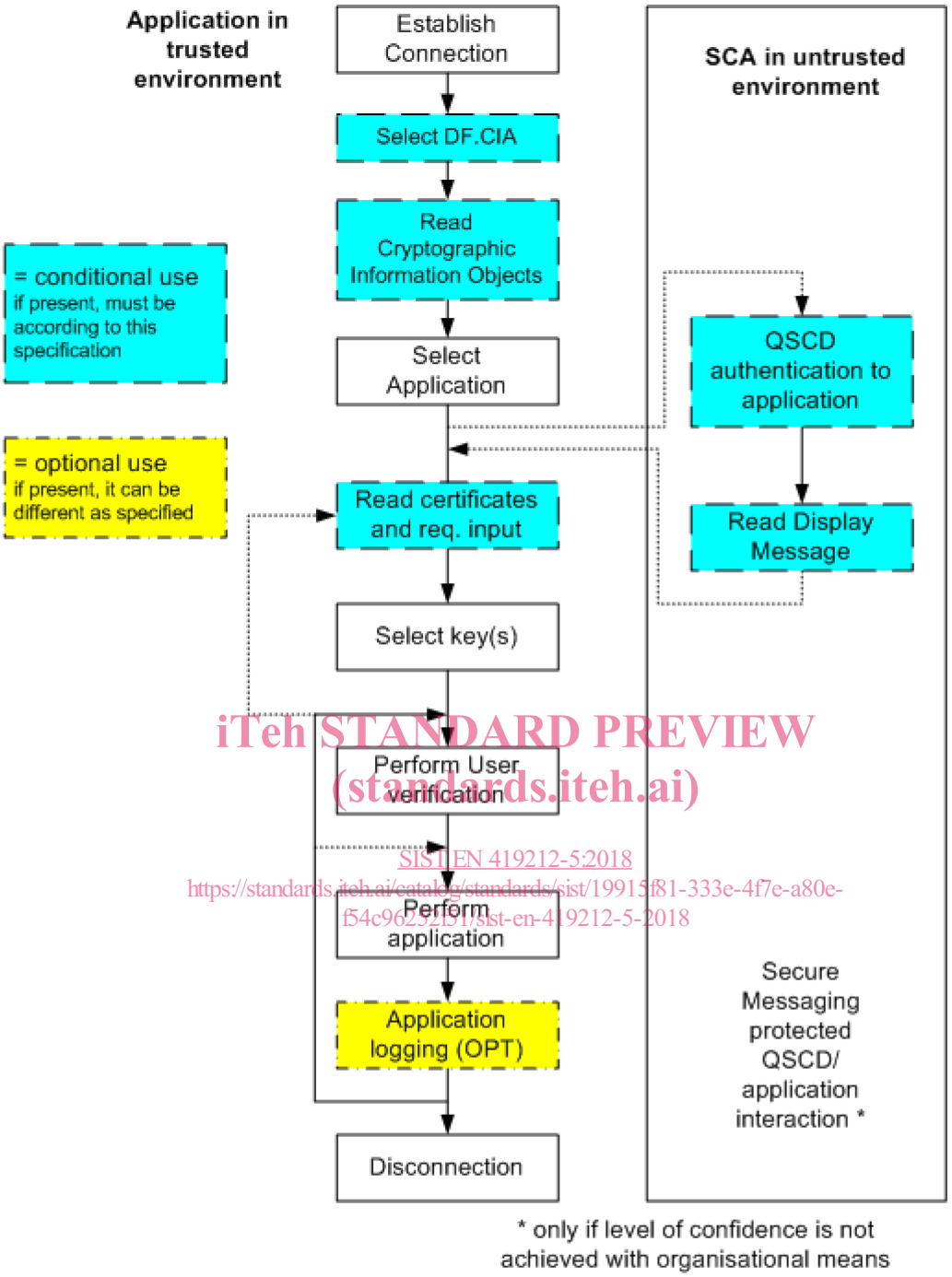

Figure 1 — Interaction sequences between application and QSCD

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.

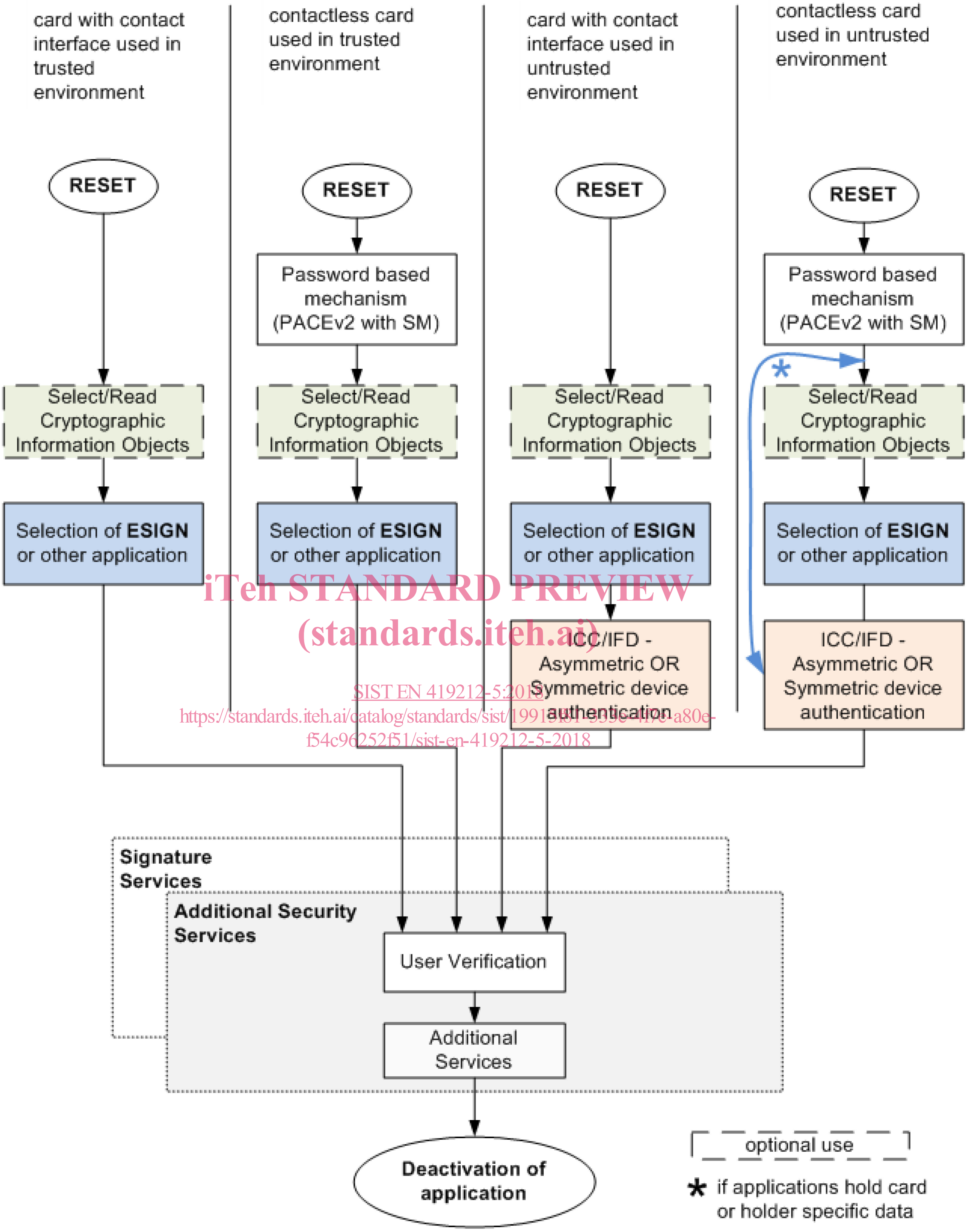

Figure 2 — Example of additional service selection

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.

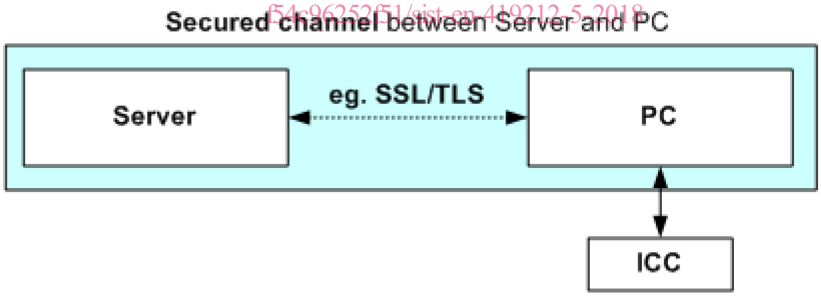

Figure 3 — Example of client/server authentication

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 EN 419212-2:2017 Annex 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 PKCS #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 PKCS #1, Version 2.1, Chapter 9.2 “EMSA-PKCS1-v1-5”. For particular Authentication input T refer to 6.4.5.

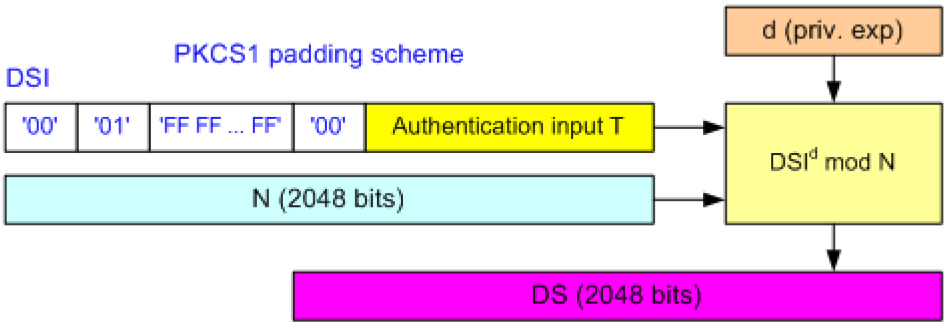

Figure 4 — Example for 2048 bit DSI according to PKCS #1 V1.5

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 EN 419212-2:2017, clause 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 PKCS #1 V 2.1, section 9.1. There are two modes of operation, each indicated by a separate set of algorithm IDs see EN 419212-1:2017, Table A.17.

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

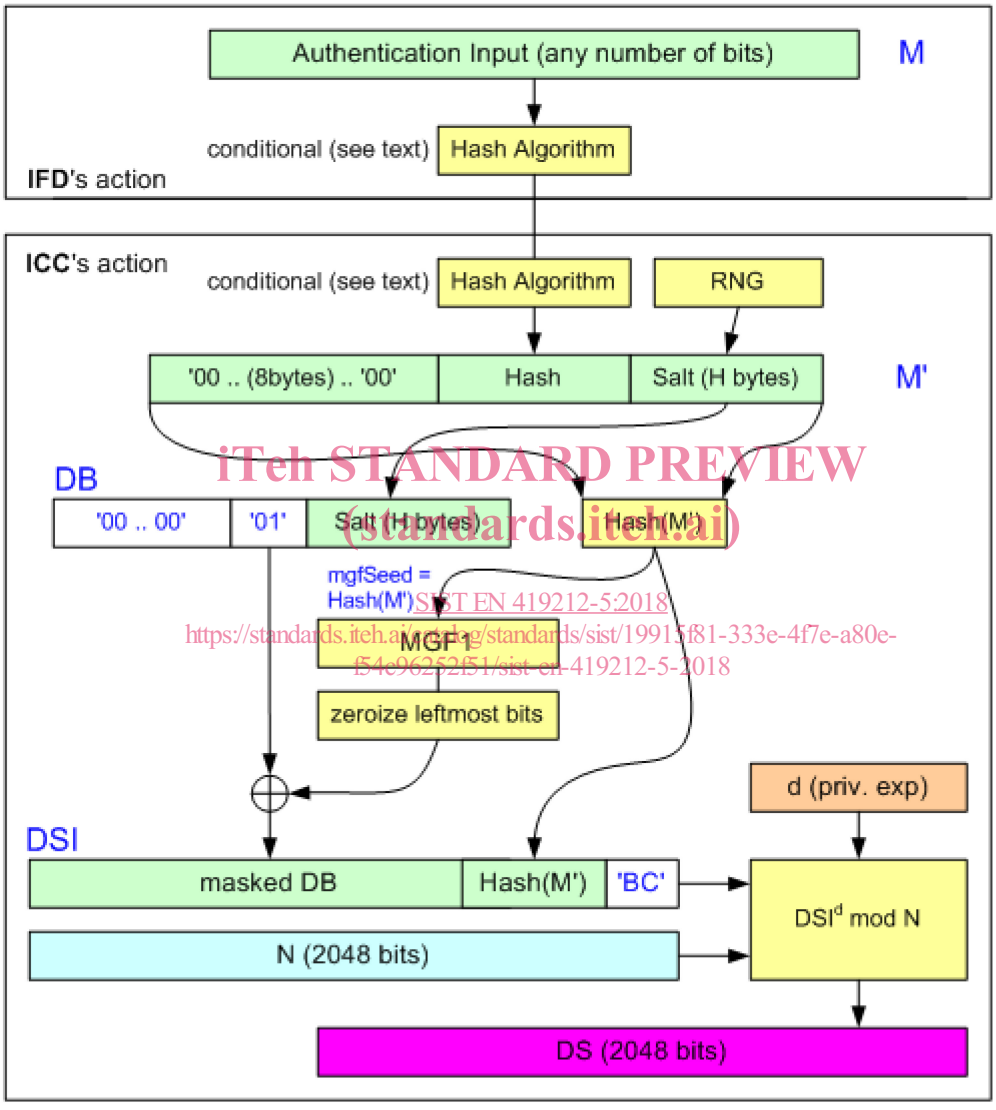

Figure 5 — Example for 2048 bit DSI according to PKCS #1 V2.1

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 require 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 x Key.ModulusByteLength — (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 PKCS #1 V2.1.

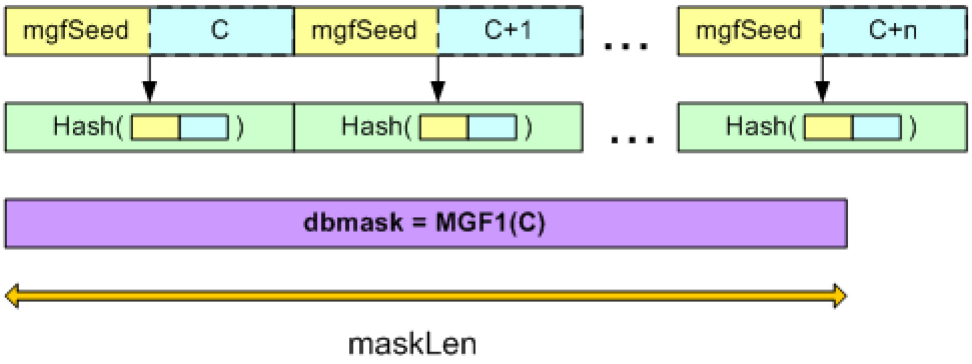

Figure 6 — Example for the mask generating function MGF1

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

Length(***DB***) = *N* – *H* – 1 = ***maskLen***.

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

The length of the *mfgSeed* is identical to H, the length of C is 4 bytes as specified in PKCS #1 V 2 . The initial value of C is zero. The concatenation of [*mfgSeed* || *C*] pairs is right truncated at the length of *maskLen* to build *dbmask*.

The [8 x Key.ModulusByteLength - (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 x Key.ModulusByteLength — (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 ⊕ MGF1(Hash(M'), 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.