SLOVENSKI STANDARD
oSIST prEN 14890-2:2012

01-maj-2012

Uporabniški vmesnik za pametne kartice, ki se uporabljajo kot naprave za izdelovanje varnega podpisa - 2. del: Dodatne storitve

Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

Anwendungsschnittstelle für Chip-Karten, die zur Erzeugung qualifizierter elektronischer Signaturen verwendet werden - Teil 2: Zusätzliche Dienste

Interface applicative des cartes à puces utilisées comme dispositifs de création de signature numérique sécurisés - Partie 2: Services complémentaires

Ta slovenski standard je istoveten z: **prEN 14890-2**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

oSIST prEN 14890-2:2012 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 14890-2

March 2012

ICS 35.240.15

Will supersede EN 14890-2:2008

English Version

Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

Interface applicative des cartes à puces utilisées comme dispositifs de création de signature numérique sécurisés - Partie 2: Services complémentaires

Anwendungsschnittstelle für Chip-Karten, die zur Erzeugung qualifizierter elektronischer Signaturen verwendet werden - Teil 2: Zusätzliche Dienste

This draft European Standard is submitted to CEN members for enquiry. 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, 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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. prEN 14890-2:2012: E

Contents

Foreword 3
1 Scope 4
2 Normative references 4
3 Terms and definitions 5
4 Abbreviations and notation 6
4.1 Abbreviations 6
5 Additional Service Selection 8
6 Client/Server Authentication 10
6.1 Client/Server protocols 10
6.2 Steps preceding the client/server authentication 10
6.3 Padding format 11
6.4 Client/Server protocol 13
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
7.4 Asymmetric external authentication 25
8 Symmetric key transmission between a remote server and the ICC 45
8.1 Steps preceding the key transport 45
8.2 Key encryption with RSA 45
8.3 Diffie-Hellman key exchange for key encipherment 49
9 Signature verification 53
9.1 Signature verification execution flow 53
10 Certificates for additional services 57
10.1 File structure 57
10.2 EF.C.CH.AUT 57
10.3 EF.C.CH.KE 58
10.4 Reading Certificates and the public key of CAs 58
11 Privacy Context functions 59
11.1 Introduction 59
11.2 Auxiliary Data Verification 59
11.3 Restricted Identification 64
11.4 mERA-based eServices with trusted third party protocol 69
12 APDU data structures 75
12.1 Algorithm Identifiers 75
12.2 CRTs 75
Annex A (normative) Security Service Descriptor Templates 78
Annex B (informative) Key and signature formats for elliptic curves over prime fields GF(p) 84
Annex C (informative) Security environments 86
Annex D (normative) Algorithm Identifiers — Coding and specification 99
Annex E (informative) Example of DF.CIA 105
Bibliography 109

Foreword

This document (prEN 14890-2:2012) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by AFNOR.

This document is currently submitted to the CEN Enquiry.

This document will supersede EN 14890-2:2008.

This standard supports services in the context of IAS **I**dentification, **A**uthentication and Electronic **S**ignature (IAS) services, as well as other services.

In EN 14890 Part 1, the standard allows to support the implementation of the European legal framework for electronic signatures, defining the functional and security features for a smart card intended to be used as a Secure Signature Creation Device according to the Terms of the European Directive on Electronic Signature 1999/93. A card compliant to the standard will be able to produce a "Qualified Electronic Signature (QES)" that fulfils the requirements of Article 5.1 of the Electronic Signature Directive and therefore can be considered equivalent to hand-written signatures.

In EN 14890 Part 2, the standard specifies mechanisms to support other services like generic Identification, Authentication, confidentiality, signature verification services and privacy features.

The standard defines a set of services that will enable the development of interoperable cards issued by any card industry sector. The standard will describe an application interface and behavior of the SSCD, i.e. it should be possible to implement it on native and interpreter based cards.

This standard consists of two parts:

Part 1: “Basic Services for Electronic Signatures” describes the specifications for IAS based services on smart cards to be used in compliance to requirements of Article 5.1 of the Electronic Signature Directive,

Part 2: “Other Services” describes other services that may be used in conjunction with all, some or none of the services described in Part 1.

Changes from the 1st published 2008-Version.

The scope of the standard was enhanced through new mechanisms in the field of password based mechanisms and privacy.

Part 1:

- New algorithms added to device authentication protocols (e.g. AES, ELC)
- Added AES to secure messaging
- Introduced password based mechanisms (PACEv2)
- Updating references to their latest releases.
- Algorithm Identifier coding
- Recommendation for making best use of device authentication protocol

Part 2:

- Added anonymity and pseudonymity services
- Added Auxiliary data transmission e.g. for Age verification

1 Scope

Part 2 of this series contains Identification, Authentication and Digital Signature (IAS) services in addition to the SSCD mechanisms already described in Part 1 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 referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[1] ISO/IEC 7816-4:2005, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*
< UNDER REVISION>

[2] ISO/IEC 7816-8:2004, *Identification cards — Integrated circuit cards — Part 8: Commands for security operations*

[3] ISO/IEC 7816-9:2004, *Identification cards — Integrated circuit cards — Part 9: Commands for card management*

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

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply. These definitions are in compliance with those given in the revision of ISO/IEC 7816-4.

3.1
Anonymization
The process that removes the association between an identifying data set and a data subject.

3.2
Anonymized data
Data that once were linked to such an individual but can now no longer be related to that person

3.3
Anonymous data
Data that cannot be linked to a specific individual

3.4
C/S external authentication
The authentication of the server by the client. The client is regarded as the combination of the PC and the ICC. This external authentication is out of the scope of this specification

3.5
C/S internal authentication
The authentication of the client by the server. The client is regarded as the combination of the PC and the ICC

3.6
Forward secrecy
Forward secrecy is a quality of a security protocol, that guarantees the confidentiality of a transaction even if all longterm keys are compromised in the future.

3.7
identification
Identification is the unique association of a set of descriptive parameters to an individuum within a given context.

3.8
IFD
Device or entity that belongs to the external world (outside the ICC)

3.9
privacy
Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

3.10
pseudonymity
Pseudonymity is the ensurance that a user may use a resource or service without disclosing its user identity.

In contrast to anonymity the user creates and uses an ambiguous parameter – the pseudonym – (e.g. a phantasy name) which is not sufficient for user identification but is useful to partially recognize and address the user for dedicated communication purpose (e.g. chat room, forum).

3.11
secured channel
A communication link between the ICC and a security module (possibly also an ICC) that provides authenticity and/or integrity and/or secrecy

3.12
unlinkability
Unlinkability is the ensurance that a user may make multiple uses of resources or services without others being able to link these uses together [15].

4 Abbreviations and notation

The abbreviations and notation is in accordance with those given in [5].

4.1 Abbreviations

APDU	Application Protocol Data Unit
ARR	Access Rule Record
AT	CRT for Authentication
C/S	Client-Server
CA	Certification Authority
CC	Cryptographic Checksum
CCT	Cryptographic Checksum Template
CIA	Cryptographic Information Application
CMS	Card Management System
CRT	Control Reference Template
CT	Confidentiality Template
D[key](msg)	Decipherment of <msg> with <key>
DF	Dedicated File
DH	Diffie-Hellman
DO	Data Object
DS[key](msg)	Digital Signature of <msg> with <key>
DSI	Digital Signature Input
DST	CRT for Digital Signature
E[key](msg)	Encipherment of <msg> with <key>
EF	Elementary File
FCI	File Control Information
FCP	File Control Parameters
H_<id>	Hash function using <id> algorithm
ICC	Integrated Circuit(s) Card
ID	Identifier
IFD	Interface Device
INS	Instruction byte
KE	Key Encipherment
KEI	Key Encipherment Input Format

KID	Key Identifier
MD5	Message Digest 5 (hash algorithm)
MF	Master File
OAEP	Optimal Asymmetric Encryption Padding
P1-P2	Parameter bytes
PI	Padding Indicator
PrK	Private Key
PuK	Public Key
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standards
PBM	Password based mechanism
PSO	PERFORM SEC. OPERATION
PSS	Probabilistic Signature Scheme
RCA	RootCA
RFU	Reserved for Future Use
RND	Random Number
SE	Security Environment
SFI	Short File Identifier
SHA	Secure Hash Algorithm
SK	Secret Key
SN	Serial Number
SM	Secure Messaging
SSCD	Secure Signature Creation Device
SSD	Secure Service Descriptor
TDES	Triple-DES
UQB	Usage Qualifier

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**.

Additional services provided in the ICC mandate the existence of an appropriate security environment. Associated security environments are described in the Annex C “(informative) Security environments” on page 86.

In addition to the descriptive information found in DF.CIA (refer to 16 “Cryptographic Information Application” in Part 1) information might be required that can be presented in Security Service Descriptors. The concept of Security Service Descriptors is described in the Annex A on page 78.

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.

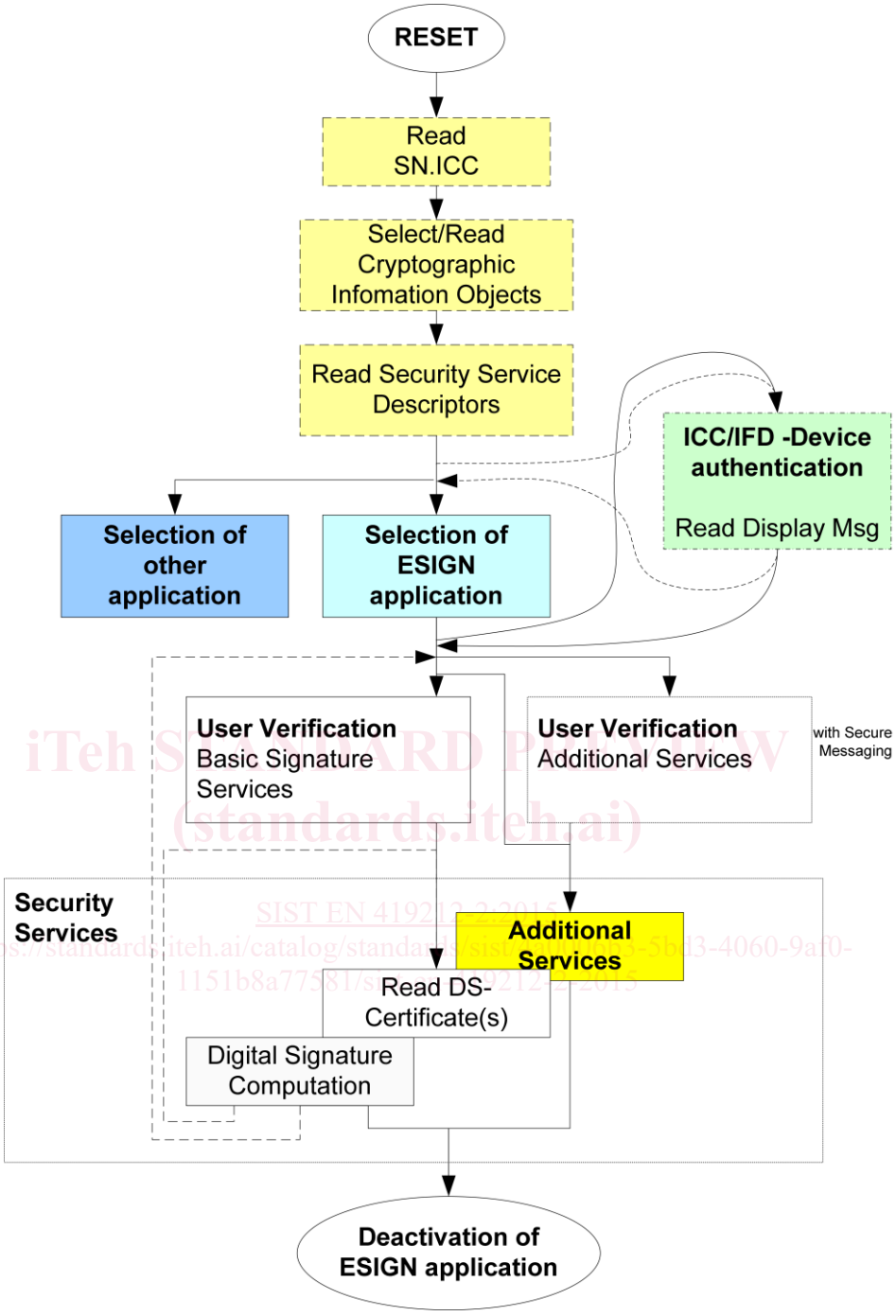

Figure 1 — Example of additional service selection

Figure 1 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.

6 Client/Server Authentication

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” on page 5) is a process, independent from the requirement of device authentication.

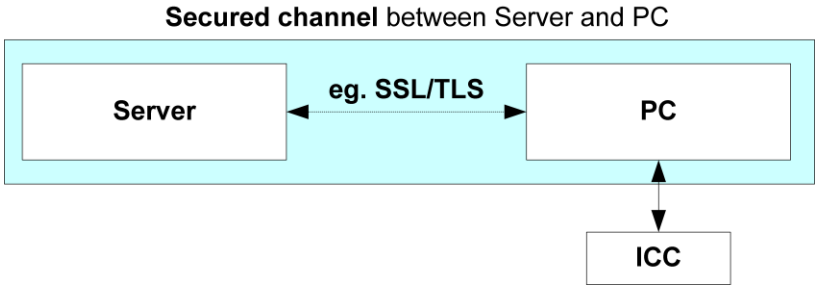

Figure 2 — Example of client/server authentication

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” on page 5). The server’s certificate as well as the server protocol is application specific and therefore out of the scope of this document.

6.1 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 [11]. 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 WTLS 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.

6.2 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 Annex C “(informative) Security environments” on page 86 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.

6.3 Padding format

6.3.1 PKCS #1 v 1-5

In case of RSA, the authentication input *T* is formatted according to [7] PKCS #1, Version 2.1, Chapter 9.2 “EMSA-PKCS1-v1-5”. For particular algorithms refer to 6.4.5 "Command data field for the client server authentication" on page 19.

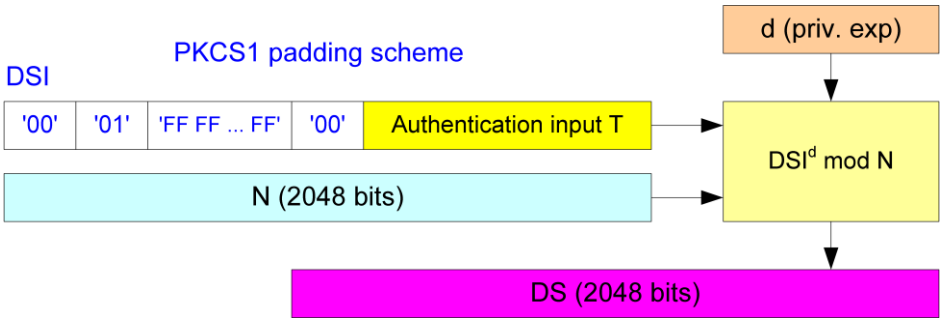

Figure 3 — Example for 2048 bit DSI according to PKCS #1 V1.5

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 13.3.3 “Digest Info for SHA-X” in Part 1.

6.3.2 DSI according to PKCS #1 V 2.x (PSS)

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

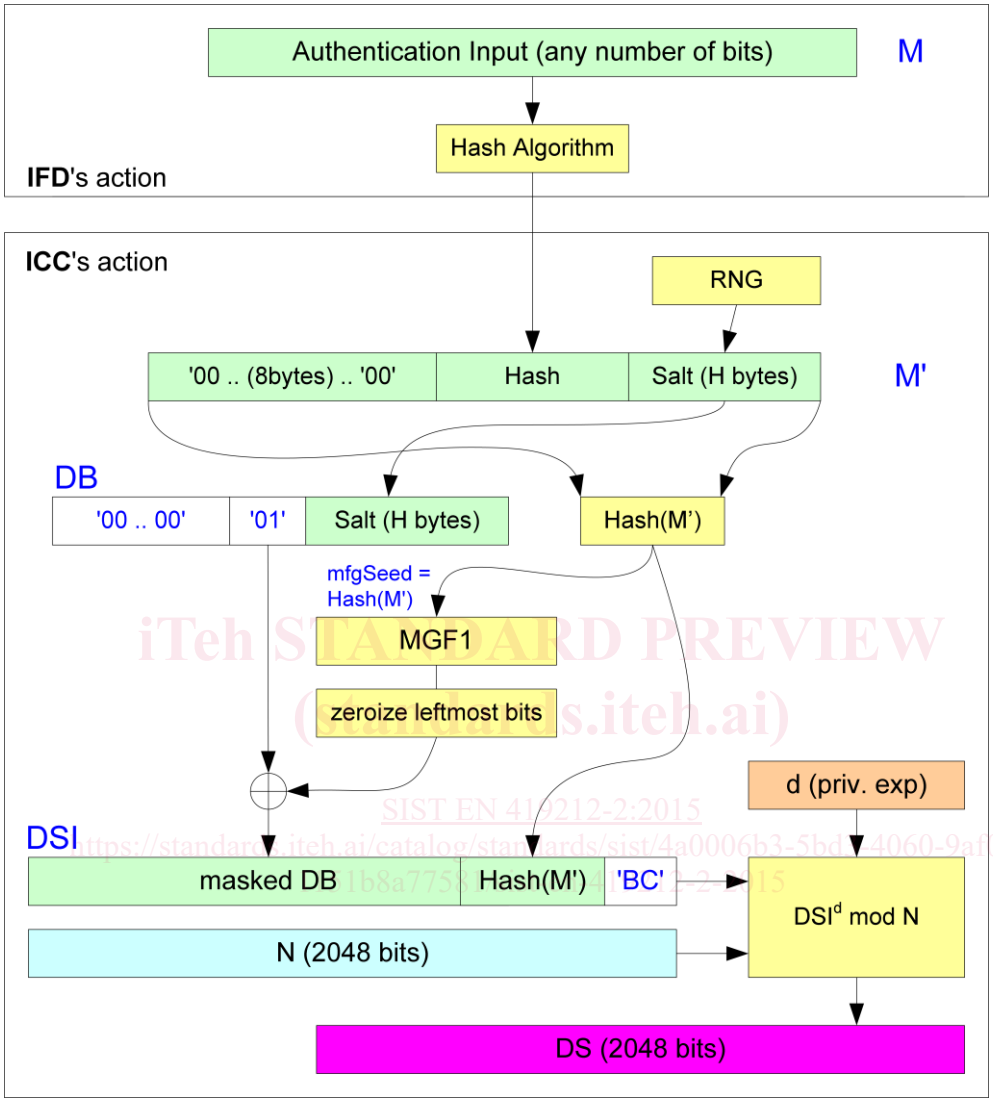

Figure 4 — Example for 2048 bit DSI according to PKCS #1 V2.1"

The hashing function used in MGF-1 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 [7] [PKCS 1 — V.2.1, Chapter B.2.1].

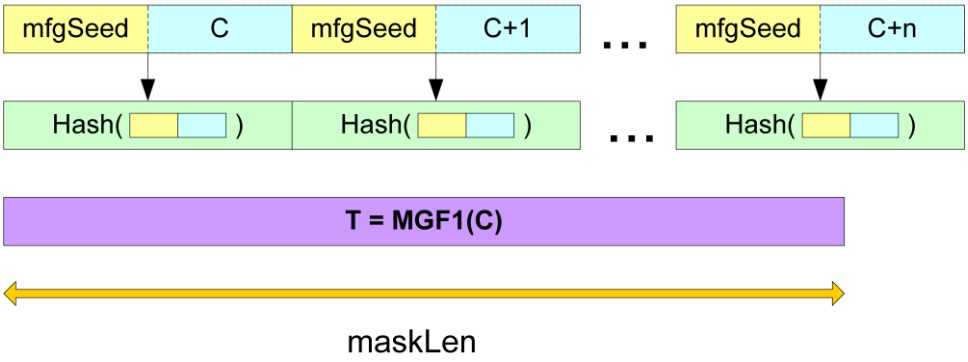

Figure 5 — Example for the mask generating function MGF1

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 [7] . The initial value of C is zero. The concatenation of [*mfgSeed* || *C*] pairs is right truncated at the length of *maskLen*.

Finally the digital signature input.

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 9796 (option 1)

6.3.3 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).

6.4 Client/Server protocol

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