SLOVENSKI STANDARD
SIST EN 419212-2:2018

01-april-2018

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

Uporabniški vmesnik za varnostne elemente za elektronsko identifikacijo, avtentifikacijo in zanesljivost storitev - 2. del: Podpis in dodatne storitve

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: Zusätzliche Dienste

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1d7c16b1-a05c-4864-83a0-5d6ffd1ce819/sist-en-419212-2-2018

Ta slovenski standard je istoveten z: EN 419212-2:2017

ICS:

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

SIST EN 419212-2:2018 **en,fr,de**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1d7c16b1-a05c-4864-83a0-5d6ffd1ce819/sist-en-419212-2-2018

SIST EN 419212-2:2018

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419212-2

December 2017

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 2: Signature and Seal Services

Interface applicative des éléments sécurisés utilisés comme dispositifs de création de signature électronique qualifiée (cachet) - Partie 2 : Services de signatures et de cachets

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1d7c16b1-a05c-4864-83a0-5d6ff11ee819/sist-en-419212-2-2018

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

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2017 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN 419212-2:2017 E

SIST EN 419212-2:2018

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1d7c16b1-a05c-4864-83a0-5d6ffd1ce819/sist-en-419212-2-2018

SIST EN 419212-2:2018

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1d7c16b1-a05c-4864-83a0-5d6ffd1ce819/sist-en-419212-2-2018

SIST EN 419212-2:2018

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1d7c16b1-a05c-4864-83a0-5d6ffd1ce819/sist-en-419212-2-2018

SIST EN 419212-2:2018

European foreword

This document (EN 419212-2:2017) has been prepared by Technical Committee CEN/TC 224 “Furniture”, the secretariat of which is held by AFNOR.

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1d7c16b1-a05c-4864-83a0-5d0ffd1ee819/sist-en-419212-2-2018

This standard consists of five parts:

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

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

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

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

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

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

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

SIST EN 419212-2:2018

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 Part 2, clause 8.3.6.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1d7c16b1-a05c-4864-83a0-5d6ffd1ce819/sist-en-419212-2-2018

SIST EN 419212-2:2018

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*

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1d7c16b1-a05c-4864-83a0-5d6ffd1ce819/sist-en-419212-2-2018

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*

SIST EN 419212-2:2018

BSI: "Technical report Signature creation and administration for eIDAS token", Part 1: Functional Specification Version 1.0 Date: 2015/07/21

BSI/TR-03110 "Part 2 – Protocols for electronic IDentification, Authentication and trust Services (eIDAS)“, Version 2.20, January 22nd, 2015[1]

3 Terms and definitions

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

4 Symbols and abbreviations

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

5 Signature application

5.1 Application Flow

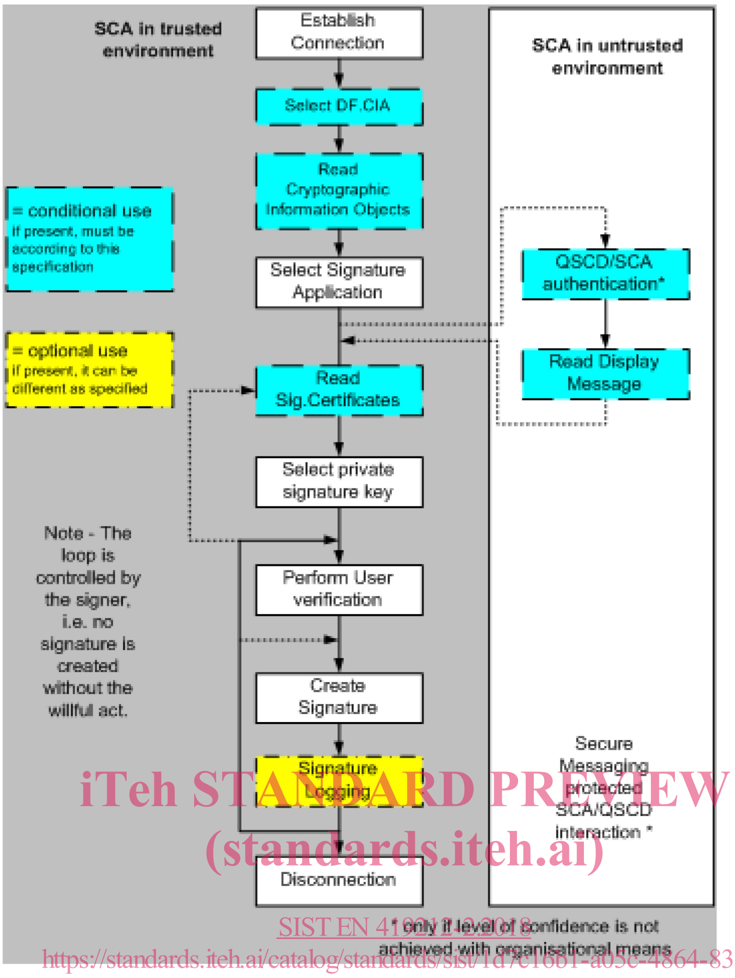
Figure 1 shows an execution flow for a signature creation as it is mandated in [1].

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1d7c16b1-a05c-4864-83a0-5d6ffd1ce819/sist-en-419212-2-2018

[1] Available at https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03110/index_htm.html

SIST EN 419212-2:2018


SCA in trusted environment
Establish Connection
SCA in untrusted environment
Select DF.CIA
Read Cryptographic Information Objects
= conditional use
If present, must be according to this specification
QSCD/SCA authentication*
Select Signature Application
Read Display Message
= optional use
if present, it can be different as specified
Read Sig.Certificates
Select private signature key
Note - The loop is controlled by the signer, i.e. no signature is created without the willful act.
Perform User verification
Create Signature
Secure Messaging protected SCA/QSCD interaction *
Signature Logging
Disconnection
* only if level of confidence is not achieved with organisational means

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1d7c1661-a05c-4864-83a0-5d6ffd1ce819/sist-en-419212-2-2018

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.

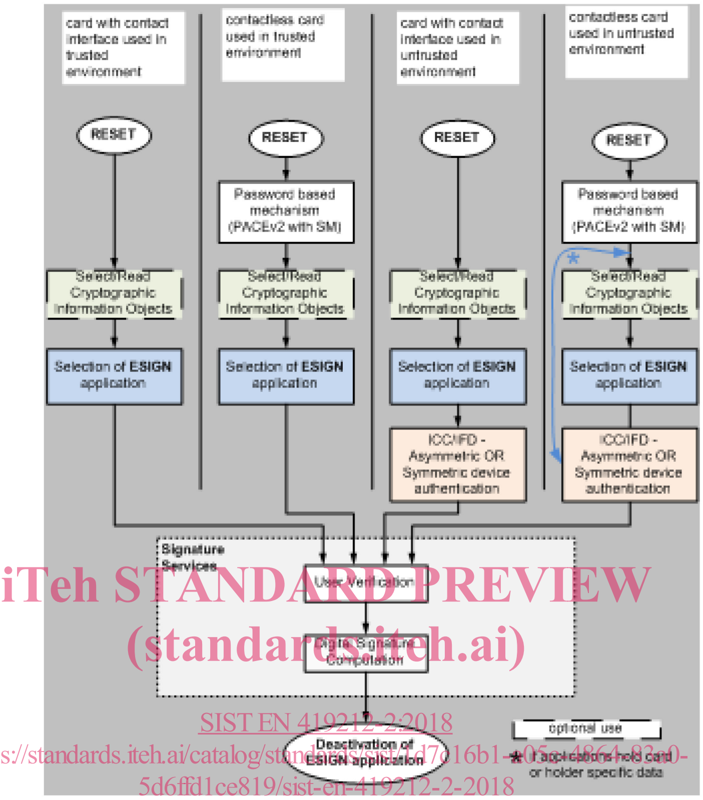
Reading SN.ICC would be a possible start for a non-privacy protecting device authentication (e.g. EN 419212-3, 3.9) whereas the card is addressed through contacts. For privacy protection (e.g. EN 419212-3, 3.6, EN 419212-3, 3.7) reading SN.ICC would not be desirable. Instead a password based mechanism 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.

SIST EN 419212-2:2018

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 EN 419212-3, 3.14.


card with contact interface used in trusted environment
contactless card used in trusted environment
card with contact interface used in untrusted environment
contactless card used in untrusted environment
RESET
RESET
RESET
RESET
Password based mechanism (PACEv2 with SM)
Password based mechanism (PACEv2 with SM)
*
Select/Read Cryptographic Information Objects
Select/Read Cryptographic Information Objects
Select/Read Cryptographic Information Objects
Select/Read Cryptographic Information Objects
Selection of ESIGN application
Selection of ESIGN application
Selection of ESIGN application
Selection of ESIGN application
ICC/IFD - Asymmetric OR Symmetric device authentication
ICC/IFD - Asymmetric OR Symmetric device authentication
Signature Services
User Verification
Digital Signature Computation
Deactivation of ESIGN application
optional use
* Applications hold card or holder specific data

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1d7c16b1-a05e-4864-83a0-5d6ffd1ce819/sist-en-419212-2-2018

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” (EN 419212-1, 3.58) and “untrusted environment” (EN 419212-1, 3.63), 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

SIST EN 419212-2:2018

- 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
Contact 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 to EN 419212-3, clause 3.
Contactless 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 to EN 419212-3, clause 3. NOTE The RSA transport protocol (EN 419212-3, clause 3.8) is not suitable, unless the SN.ICC is set to a “dummy value” for privacy reasons.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1d7c16b1-a05c-4864-83a0-5d6ffd1ce819/sist-en-419212-2-2018

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.

SIST EN 419212-2:2018

Table 2 — SELECT ESIGN application — command APDU

Command Parameter	Meaning
CLA INS	according to ISO/IEC 7816-4 'A4' — SELECT
P1 P2	'04' select by DF Name '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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1ll7c161-a05e-4864-83a0-5d6ffd1ce819/sist-en-419212-2-2018

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 to EN 419212-3, clause 3.13.3.

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.

SIST EN 419212-2:2018

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:

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-2:2018
https://standards.iteh.ai/catalog/standards/sist/1d7c16b1-a05c-4864-83a0-5d6ffd1ce819/sist-en-419212-2-2018

- User verification (PIN, Password or biometric).
- Signature creation as described in EN 419212-2, clause 7.
- Device authentication as described in EN 419212-3, clause 3.
- Key Generation as described in EN 419212-2, clause 2.10.
- Verification of card verifiable certificates as described in EN 419212-3, clause 5.
- Authentication services as described in EN 419212-5, clause 6.
- Authentication services as described in EN 419212-5, clause 7.
- Key decipherment as described in EN 419212-5, clause 8.
- Signature verification as described in EN 419212-5, clause 9.

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.