SLOVENSKI STANDARD
SIST EN 419212-2:2015

01-april-2015

Nadomešča:

SIST EN 14890-2:2009

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: EN 419212-2:2014

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST EN 419212-2:2015 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419212-2

December 2014

ICS 35.240.15

Supersedes 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 European Standard was approved by CEN on 27 September 2014.

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, 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

Contents

Foreword

This document (EN 419212-2:2014) 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 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 2015 and conflicting national standards shall be withdrawn at the latest by June 2015.

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

This document supersedes EN 14890-2:2008.

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

EN 419212, *Application Interface for smart cards used as Secure Signature Creation Devices*, consists of two parts:

- *Part 1: Basic services* which describes the specifications for IAS based services on smart cards to be used in compliance to the requirements of Article 5.1 of the Electronic Signature Directive; and
- *Part 2: Additional services* [the present document] which describes other services that may be used in conjunction with all, some or none of the services described in Part 1.

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 419212-1, 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/EC. 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 419212-2, the standard specifies mechanisms to support other services like generic Identification, Authentication, confidentiality, signature verification services and privacy features.

EN 419212 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.

Compared with the 2008 versions of EN 14890, the following broad change has been made:

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

Regarding EN 419212-1, the most significant technical changes that have been made are the following ones:

- 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 protocols.

Regarding EN 419212-2, the most significant technical changes that have been made are the following ones:

a) Added privacy services including:

   1) anonymity and pseudonymity services;

   2) auxiliary data transmission e.g. for Age verification;

   3) e-Services with trusted third party;

   4) e-Services with 2-parties.

According to the CEN-CENELEC Internal Regulations, the national standards organizations 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, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

1 Scope

This European Standard contains Identification, Authentication and Digital Signature (IAS) services in addition to the SSCD mechanisms already described in EN 419212-1 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 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.

EN 419212-1:2014, *Application Interface for smart cards used as Secure Signature Creation Devices — Part 1: Basic services*

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

ISO/IEC 7816-6:2006, *Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements for interchange*

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

ISO/IEC 9796 (all parts), *Information technology — Security techniques — Digital signature schemes giving message recovery*

ISO/IEC 9797-1, *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 following terms and definitions apply.

NOTE These definitions are in compliance with those given in the revision of ISO/IEC 7816-4.

3.1
anonymity
assurance in which a user may use a resource or service without disclosing the user's identity

3.2
anonymization
process that removes the association between an identifying data set and a data subject

3.3
anonymized data
data that was once linked to an individual but can now no longer be related to them

3.4
anonymous data
data that cannot be linked to a specific individual

3.5
C/S external authentication
authentication of the server by the client

Note 1 to entry: The client is regarded as the combination of the PC and the ICC. This external authentication is out of the scope of this specification.

3.6
C/S internal authentication
authentication of the client by the server

Note 1 to entry: The client is regarded as the combination of the PC and the ICC.

3.7
forward secrecy
security property of a protocol, that guarantees that the disclosure of long-term private key does not enable an opponent to compromise the secrecy property of the executions of the protocol made in the past, for example, by re-computing previously derived keys

3.8
identification
unique association of a set of descriptive parameters to an individual within a given context

3.9
IFD
device or entity that belongs to the external world (outside the ICC)

3.10
privacy
claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others

3.11
pseudonymity
ensurance that a user may use a resource or service without disclosing its user identity

3.12
secured channel
communication link between the ICC and a security module (possibly also an ICC) that provides authenticity and/or integrity and/or confidentiality

3.13
unlinkability
assurance that a user may make multiple uses of resources or services without others being able to link these uses together [14]

3.14
usage of expressions in this standard
use of the key words "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document as to be interpreted as described in [21]

Note 1 to entry: See the following list of key-words:

SHALL: This word, or the terms "**REQUIRED**" or "**SHALL**", means that the definition is an absolute requirement of the specification.

SHALL NOT: This phrase, or the phrase "**SHALL NOT**", means that the definition is an absolute prohibition of the specification.

SHOULD: This word, or the adjective "**RECOMMENDED**", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications will be understood and carefully weighed before choosing a different course.

SHOULD NOT: This phrase, or the phrase "**NOT RECOMMENDED**" means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed **before implementing any behaviour described with this label.**

MAY: This word, or the adjective "**OPTIONAL**", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.

An implementation which does not include a particular option will be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality.

[…] Square brackets indicate a freedom of choice. This can be either a:
- *choice of values* in a given range ['00' .. '03'] – typical for fixed length fields,
- or a choice whether to present a value or not – … || '80' L80 AlgID || ['83' L83 KeyId] …. whereas the set of data in square brackets is the *optional* part (= at the discretion of the implementation) or *conditional* (= depending on a condition given in the standard).

CONDITIONAL: The application of a specification depends on one or more conditions and shall only be applied if the condition(s) are met.

The associated condition(s) are always described if a *conditional* attribute is made with a specification. If the conditions are met, the specification may be *normative* or *informative* depending on the context in which the specification is made.

4 Abbreviations and notation

For the purposes of this document, the following symbols and abbreviations apply.

APDU	Application Protocol Data Unit
ARR	Access Rule Record
AT	Authentication Template
C/S	Client-Server
CA	Certification Authority
CC	Cryptographic Checksum
CCT	Cryptographic Checksum Template
CIA	Cryptographic Information Application
CLA	Class byte
CMS	Card Management System
CRT	Control Reference Template
CT	Confidentiality Template
CV	Card Verifiable
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	Digital Signature Template
E[key](msg)	Encipherment of <msg> with <key>
ECDSA	Signature Scheme based on elliptic curve cryptography (ELC)
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 SECURITY OPERATION
PSS	Probabilistic Signature Scheme
RA	Role authentication
RCA	Root CA
RFU	Reserved for Future Use
RND	Random Number
RSA	Cryptographic algorithm invented by Ronald Rivest, Adi Shamir and Leonard Adleman
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	Security Service Descriptor
SW1-SW2	Status bytes
TDES	Triple-DES, this standard only considers the 2-key variant
UQB	Usage Qualifier Byte

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 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 Annex B “(informative) Security environments”.

In addition to the descriptive information found in DF.CIA (refer to Clause 16 “Cryptographic Information Application” in EN 419212-1:2014) information might be required that can be presented in Security Service Descriptors. The concept of Security Service Descriptors is described in 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.

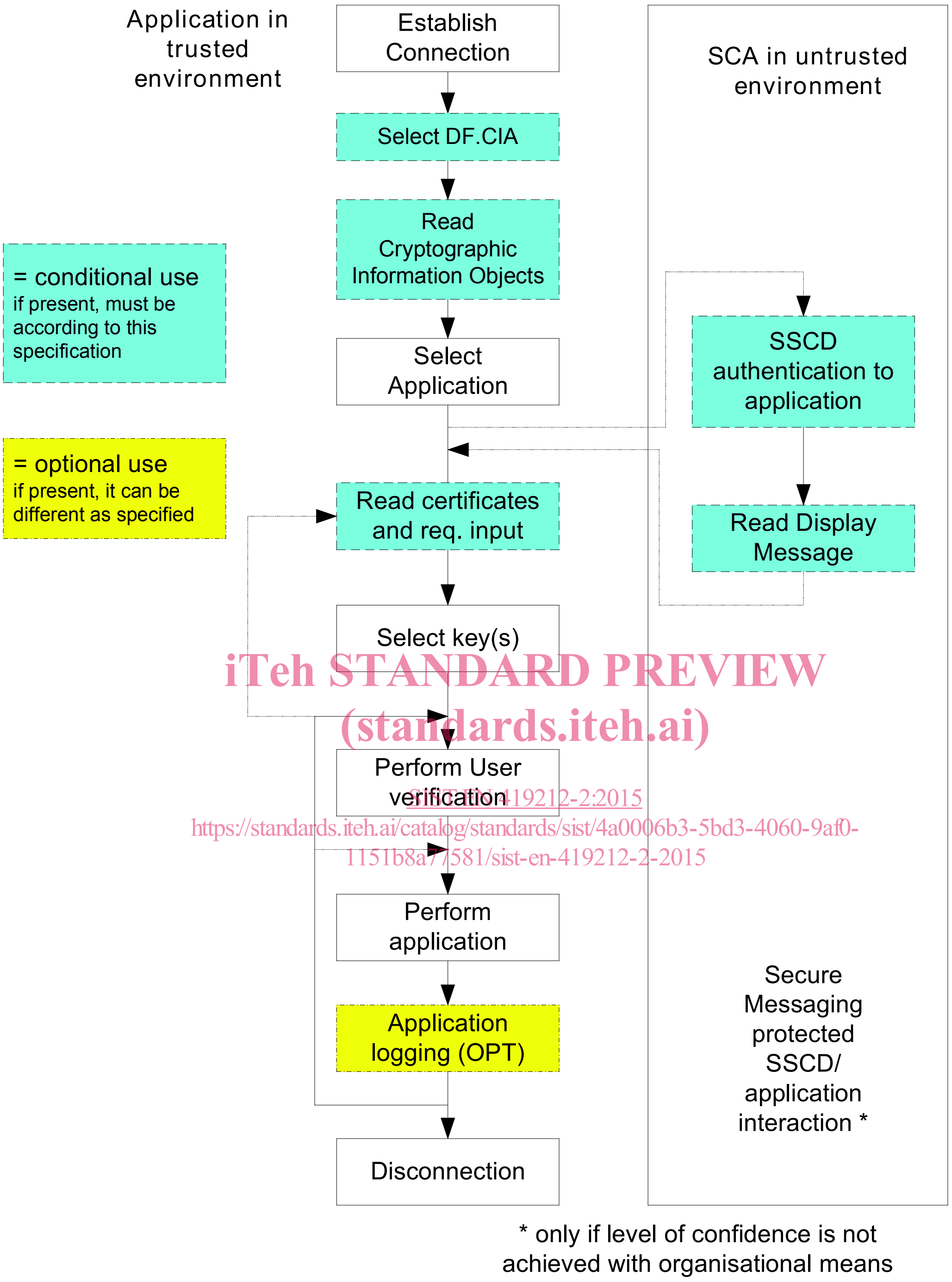
Application in trusted environment
Establish Connection
Select DF.CIA
Read Cryptographic Information Objects
Select Application
Read certificates and req. input
Select key(s)
Perform User verification
Perform application
Application logging (OPT)
Disconnection
SCA in untrusted environment
SSCD authentication to application
Read Display Message
Secure Messaging protected SSCD/ application interaction *
= conditional use
if present, must be according to this specification
= optional use
if present, it can be different as specified
* only if level of confidence is not achieved with organisational means

Figure 1 — Interaction sequences between application and SSCD

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.

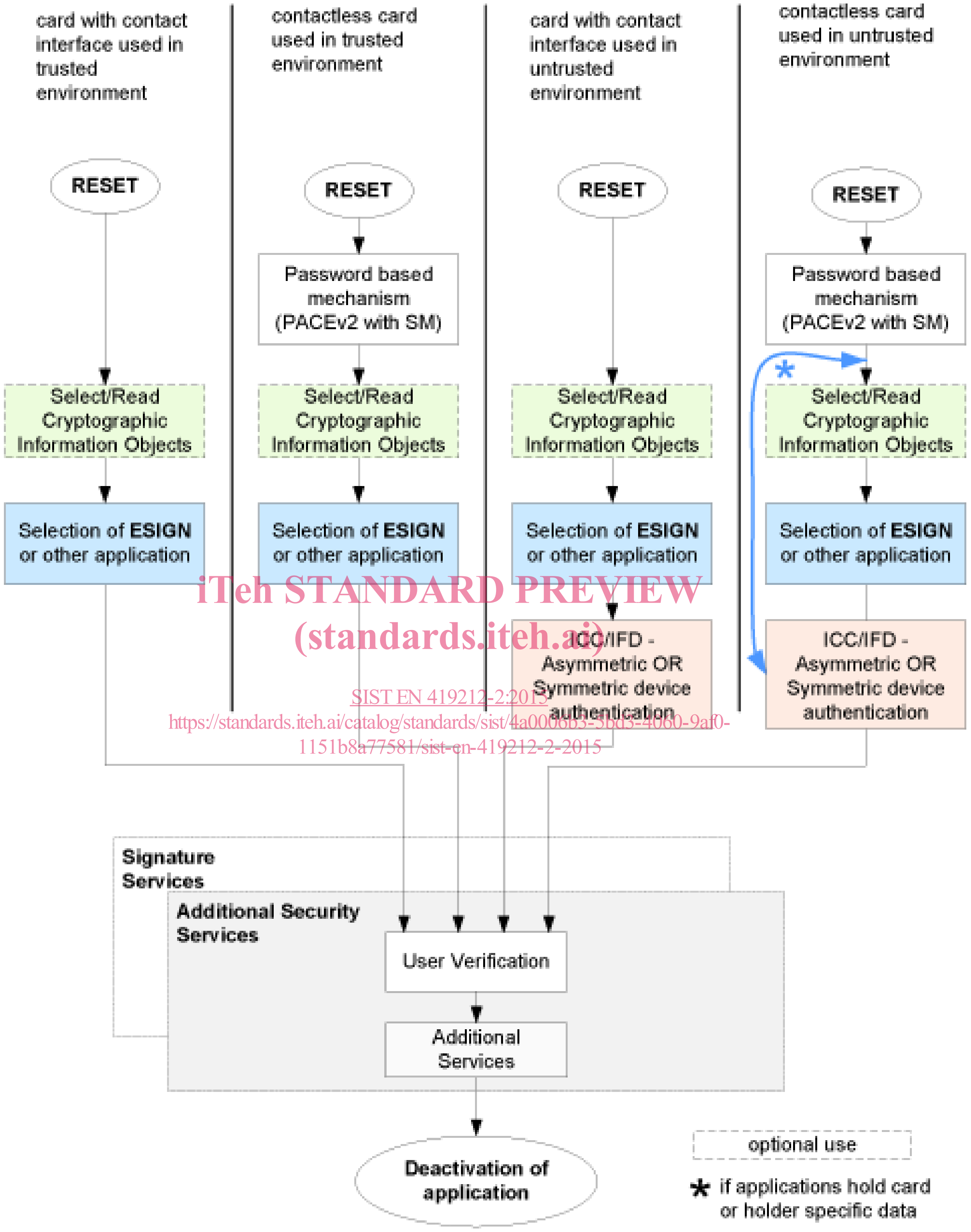
card with contact interface used in trusted environment
contactless card used in trusted environment
card with contact interface used in untrusted environment
contactless card used in untrusted environment
RESET
RESET
RESET
RESET
Password based mechanism (PACEv2 with SM)
Password based mechanism (PACEv2 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 or other application
Selection of ESIGN or other application
Selection of ESIGN or other application
Selection of ESIGN or other application
ICC/IFD - Asymmetric OR Symmetric device authentication
ICC/IFD - Asymmetric OR Symmetric device authentication
Signature Services
Additional Security Services
User Verification
Additional Services
Deactivation of application
optional use
* if applications hold card or holder specific data

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.