

DIN EN 14890-1

ICS 35.240.15

Einsprüche bis 2012-07-07
Vorgesehen als Ersatz für
DIN EN 14890-1:2009-03

Entwurf

**Anwendungsschnittstelle für Chip-Karten, die zur Erzeugung
qualifizierter elektronischer Signaturen verwendet werden –
Teil 1: Allgemeine Dienste;
Englische Fassung prEN 14890-1:2012**

Application Interface for smart cards used as Secure Signature Creation Devices –
Part 1: Basic services;
English version prEN 14890-1:2012

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2012-03-19 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

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

Gesamtumfang 266 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Nationales Vorwort

Dieses Dokument (prEN 14890-1:2012) wurde vom Technischen Komitee CEN/TC 224 „Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat vom AFNOR (Frankreich) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 043-01-17-04 UA „Austauschprotokolle bei Chipkarten“ im Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN.

DIN EN 14890-1 ist Teil einer zweiteiligen Normenreihe zur Festlegung von Anwendungsschnittstellen für Chipkarten, die zur Erzeugung qualifizierter elektronischer Signaturen verwendet werden.

DIN EN 14890-1 soll die Implementierung des europäischen rechtlichen Rahmens für elektronische Signaturen unterstützen, indem Sie die funktions- und sicherheitsbezogenen Anforderungen an eine Chipkarte zur Verwendung als sichere Signaturerstellungseinheit (Secure Signature Creation Device, SSCD) entsprechend den Bedingungen der Europäischen Richtlinie 1999/93 über elektronische Signaturen definiert. Eine mit der Norm übereinstimmende Karte wird in der Lage sein, eine "qualifizierte elektronische Signatur" (QES) zu erzeugen, die Artikel 5.1 der Signaturrechtlinie erfüllt und daher als zu handschriftlichen Signaturen äquivalent betrachtet werden kann.

Diese Norm definiert eine Menge von Diensten, die die Entwicklung interoperabler Karten, die von einem beliebigen Kartensektor ausgegeben werden, ermöglicht. Sie beschreibt eine Anwendungsschnittstelle und das Verhalten von sicheren Signaturerstellungseinheiten, d.h. eine Implementierung in systemspezifische und interpreterbasierten Karten sollte somit möglich sein.

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 14890-1:2009-03 wurden folgende Änderungen vorgenommen:

- a) den Geräteauthentifizierungsprotokollen (z. B.: AES, ELC) wurden neue Algorithmen hinzugefügt;
- b) AES (en: Advanced Encryption Standard) wurde zur sicheren Nachrichtenübermittlung hinzugefügt;
- c) passwortbasierte Mechanismen (PACE v2) wurden eingeführt;
- d) Verweisungen wurden aktualisiert;
- e) Kodierung des Algorithmusbezeichners wurde hinzugefügt;
- f) Empfehlungen für den bestmöglichen Einsatz des Geräteauthentifizierungsprotokolls wurden hinzugefügt.

Nationaler Anhang NA (informativ)

Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe. Die Definitionen stimmen mit denjenigen überein, die in der Überarbeitung von ISO/IEC 7816-4 angegeben sind.

3.1

Anonymität

Anonymität ist die Zusicherung, dass ein Benutzer ein Betriebsmittel oder einen Dienst ohne Offenlegung seiner Benutzeridentität nutzen kann

3.2

Anonymisierung

Prozess, der die Zuordnung eines Kenndatensatzes zu einem Betroffenen löscht

3.3

anonymisierte Daten

ehemals mit einer Person verknüpfte Daten, die jetzt nicht mehr mit dieser Person in Verbindung gebracht werden können

3.4

anonyme Daten

Daten, die nicht mit einer bestimmten Person verknüpft werden können

3.5

Answer-to-Reset-Datei

Elementardatei, die die Betriebsmerkmale der Karte angibt

3.6

ohne Authentisierung vertrauenswürdig

Betriebsumgebung, die ohne eine weitere Geräteauthentisierung der Definition nach vertrauenswürdig ist. Ein Beispiel dafür ist die Anwendung innerhalb eines Unternehmens, in dem jeder vorhandene Zugangspunkt mit einem vertrauenswürdigen Netzwerk verbunden ist

3.7

Authentisierung

Authentisierung ist die Überprüfung, dass eine Instanz die geforderte Instanz ist [18]

3.8

Befehl-Antwort-Paar

Satz zweier Nachrichten: ein Befehl gefolgt von einer Antwort

3.9

Vertraulichkeitsschutz

Vertraulichkeitsschutz ist die Verhinderung der Offenlegung von Informationen für unberechtigte Personen, Instanzen oder Systeme [18]

3.10

Dateneinheit

kleinster Satz von Bits, der eindeutig referenziert werden kann

3.11**Datenelement**

Information, die an der Schnittstelle sichtbar ist und für die ein Name, eine Beschreibung des logischen Inhalts, ein Format und eine Kodierung definiert sind

3.12**Datenobjekt**

Information, die an der Schnittstelle sichtbar ist und die aus einem Tag, einer Länge und einem Wert besteht (d. h. ein Datenelement). In dieser Spezifikation werden Datenobjekte als BER-TLV-Datenobjekte bezeichnet. Siehe ISO/IEC 7816-4 [5]

3.13**zugeordnete Datei**

Datei, die Dateisteuerungsinformationen und wahlweise Speicher zur Zuteilung enthält. Sie kann Halter weiterer EF und/oder DF sein

3.14**DF-Name**

Byte-Strang, der eine zugeordnete Datei auf der Karte eindeutig kennzeichnet

3.15**Elementardatei**

Satz von Dateneinheiten oder Datensätzen, die denselben Identifikator aufweisen. Eine Elementardatei kann nicht Halter einer anderen Datei sein

3.16**Dateisteuerungsparameter**

logische, aufbaubezogene und sicherheitsbezogene Attribute einer Datei

3.17**Identifikator**

2-Byte-Binärwert zur Adressierung einer Datei

3.18**Folgenlosigkeit** (en: forward secrecy)

Folgenlosigkeit ist eine Eigenschaft eines Sicherheitsprotokolls, die die Geheimhaltung einer Transaktion auch dann sichert, wenn alle zukünftigen Langzeitschlüssel gefährdet sind

3.19**Identifikation**

Identifikation ist die eindeutige Zuordnung eines Satzes zu, einer innerhalb eines angegebenen Zusammenhangs, eine Person beschreibender Parameter

3.20**Integritätsschutz**

Integritätsschutz ist ein Mechanismus zur Sicherstellung, dass Daten nicht unerkannt verändert werden können

3.21**Masterdatei**

obligatorische eindeutige zugeordnete Datei, die die Wurzel des Dateiaufbaus darstellt

3.22**Nachricht**

Byte-Strang, der vom Schnittstellengerät zur Karte oder umgekehrt gesendet wird, ausgenommen übertragungsorientierte Zeichen nach ISO/IEC 7816-3 [4]

3.23**gegenseitige Authentisierung**

beide Beteiligten (ICC und IFD) werden gegenseitig authentisiert

3.24

Nichtbeweisbarkeit

siehe „nicht nachprüfbare Authentisierung“

3.25

Parentdatei

zugeordnete Datei, die einer bestimmten Datei in der Hierarchie unmittelbar vorangeht

3.26

Passwort

Daten, die der Kartenbenutzer der Karte vorlegen muss, wenn von der Anwendung gefordert. Ein Passwort im Sinne dieser Spezifikation ist ein Strang von Zahlen und/oder ASCII-Zeichen

3.27

Pfad

Verkettung von Identifikatoren ohne Begrenzung. Wenn der Pfad mit dem Identifikator der Masterdatei beginnt, handelt es sich um einen absoluten Pfad

3.28

Schutz personenbezogener Daten

der Schutz personenbezogener Daten ist der Anspruch von Personen, Gruppen oder Organisationen selbst zu bestimmen, wann, wie und in welchem Umfang anderen Informationen über sie mitgeteilt werden [64]

3.29

privater Schlüssel

geheimer Teil eines asymmetrischen Schlüsselpaars, z. B. Signaturerstellungsdaten entsprechend der EU-Richtlinie über elektronische Signaturen

3.30

Pseudonymisierung

eine spezielle Art der Anonymisierung, die sowohl die ursprünglichen Identifikationsdaten zu einer Person löscht als auch die Zuordnung eines speziellen Namens (Pseudonym) zu einer Person so ermöglicht, dass anhand des zugeordneten Namens (Pseudonym) kein Rückschluss auf die Identität der Person möglich ist

3.31

pseudonymisierte Daten

Daten, die nur mit einer bestimmten Person verknüpft werden können, wenn jemand im Besitz einer entsprechenden Zuordnungstabelle ist

3.32

Pseudonymität

Pseudonymität ist die Zusicherung, dass ein Benutzer ein Betriebsmittel oder einen Dienst ohne Offenlegung seiner Benutzeridentität nutzen kann

Im Gegensatz zur Anonymität erzeugt und nutzt der Benutzer einen mehrdeutigen Parameter — das Pseudonym — (z. B. einen Kunstnamen), der für die Identifikation des Benutzers nicht ausreicht, aber zur teilweisen Erkennung und Adressierung des Benutzers für zugeordnete Kommunikationszwecke (z. B. Chat-Room, Forum) zweckdienlich ist

3.33

öffentlicher Schlüssel

öffentlicher Teil eines asymmetrischen Schlüsselpaars

3.34

Datensatz

Byte-Strang, der von der Karte als Gesamtheit behandelt und durch eine Datensatznummer referenziert werden kann

3.35**Datensatznummer**

laufende Nummer, die jedem Datensatz zugewiesen wird und die den Datensatz innerhalb seiner Elementardatei eindeutig identifiziert

3.36**Wiederholungszähler**

Zähler, der verwendet wird, um die Anzahl fehlerhafter Verwendungen eines entsprechenden (Sicherheits-) Objekts zu zählen. Wenn das Objekt (z. B. Passworteingabe) korrekt verwendet wurde (korrektes Passwort eingegeben), wird der Wiederholungszähler auf seinen Ausgangswert zurückgesetzt. Ein typischer Wert eines Wiederholungszählers ist 3

3.37**geheimer Schlüssel**

entweder ein symmetrischer Schlüssel oder ein privater Teil eines öffentlichen Schlüsselpaars

3.38**nicht nachprüfbare Authentisierung**

eine nicht nachprüfbare Authentisierung ist eine Authentisierung, die keinen beständigen kryptografischen Nachweis dafür gibt, dass die Authentisierung stattgefunden hat

3.39**vertrauenswürdige Umgebung**

Betriebsumgebung, die durch Definition ihrer physikalischen Lage, ihres physikalischen Schutzes oder ihrer physikalischen Zugriffsbedingungen oder sonstige Maßnahmen den Betrug mit den an der Kommunikationsschnittstelle sichtbaren Daten verhindert, um gegen Fälschung oder Einschleusen von Daten zu schützen (siehe 8.2.3 „Umgebungsspezifikation“)

3.40**vertrauenswürdiger Kanal**

Mittel, durch das eine TSF und ein vertrauenswürdiges abgesetztes IT-Produkt mit dem erforderlichen Vertrauen kommunizieren können, um die TSP zu unterstützen

3.41**vertrauenswürdiger Pfad**

Mittel, durch das ein Benutzer und eine TSF mit dem erforderlichen Vertrauen kommunizieren können, um die TSP zu unterstützen

3.42**Unverknüpfbarkeit**

Unverknüpfbarkeit ist die Zusicherung, dass ein Benutzer Betriebsmittel oder Dienste mehrfach nutzen kann, ohne dass andere in der Lage sind, diese Nutzungen miteinander zu verknüpfen [65]

3.43**nicht zuverlässige Umgebung**

Betriebsumgebung, die Fälschung und Einschleusen von an der Kommunikationsschnittstelle vorliegenden Daten zulässt. Eine Umgebung, die ohne Authentisierung nicht vertrauenswürdig ist und die ihre Vertrauenswürdigkeit nicht durch eine Geräteauthentisierung nachweisen kann, muss als nicht zuverlässig angesehen werden. In einer nicht zuverlässigen Umgebung sollten vom Karteninhaber keine weiteren Handlungen erfolgen

3.44**nicht vertrauenswürdige Umgebung**

Betriebsumgebung, die nicht als zuverlässig vorausgesetzt werden kann. Bis ein Vertrauensnachweis erbracht worden ist (in der Regel durch eine Geräteauthentisierung), sollte die Umgebung vom Karteninhaber keine sensiblen Daten erhalten, vor allem sollte keine PIN-Eingabe erfolgen

Nach einer erfolgreichen Geräteauthentisierung *wird die nicht vertrauenswürdige Umgebung eine vertrauenswürdige Umgebung*. Aus diesem Grund bezeichnet die Eigenschaft „nicht vertrauenswürdig“ nicht die Eigenschaft „nicht zuverlässig“, sondern beinhaltet die Forderung nach einem Vertrauensnachweis.

3.45

Verwendungszähler

Zähler, der bei jeder Verwendung eines entsprechenden Objekts aktualisiert wird. Im Gegensatz zu Wiederholungszählern werden Verwendungszähler nicht auf ihren Ausgangswert zurückgesetzt, nachdem das Objekt erfolgreich verwendet wurde

3.46

Zustimmung des Benutzers

die Zustimmung des Benutzers ist eine Willenserklärung für einen kartenbezogenen Dienst

3.47

Gebrauch von Wendungen in der vorliegenden Norm

die Schlüsselworte „MUSS“ (en: MUST, SHALL), „ERFORDERLICH“ (en: REQUIRED“), „DARF NICHT“ (en: MUST NOT, SHALL NOT), „SOLLTE“ (en: SHOULD), „SOLLTE NICHT“ (en: SHOULD NOT), „EMPFOHLEN“ (en: RECOMMENDED), „DARF“ (en: MAY) und „WAHLWEISE“ (en: OPTIONAL) im vorliegenden Dokument sind nach der Beschreibung in [58] zu interpretieren

MUSS: Dieses Wort oder die Benennung „ERFORDERLICH“ bedeutet, dass die Definition eine absolute Anforderung der Spezifikation darstellt.

DARF NICHT: Dieser Ausdruck bedeutet, dass die Definition ein absolutes Verbot der Spezifikation darstellt.

SOLLTE: Dieses Wort oder das Adjektiv „EMPFOHLEN“ bedeutet, dass unter bestimmten Umständen berechnete Gründe dafür bestehen, ein bestimmtes Element zu vernachlässigen, aber die vollständigen Auswirkungen nachvollzogen und sorgfältig abgewogen werden müssen, bevor ein anderer Ablauf gewählt wird.

SOLLTE NICHT: Dieser Ausdruck oder das Adjektiv „NICHT EMPFOHLEN“ bedeutet, dass unter bestimmten Umständen berechnete Gründe dafür bestehen, dass das jeweilige Verhalten zulässig oder sogar zweckdienlich ist, aber die vollständigen Auswirkungen sollten nachvollzogen und der Fall sorgfältig abgewogen werden, **bevor ein mit diesem Kennzeichen beschriebenes Verhalten implementiert wird.**

DARF: Dieses Wort oder das Adjektiv „WAHLWEISE“ bedeutet, dass ein Element wahlweise benutzt werden kann. Ein Hersteller kann sich für die Aufnahme des Elements entscheiden, weil es von einem bestimmten Marktsegment gefordert wird oder der Hersteller meint, dass es sein Produkt verbessert, während ein anderer Hersteller das gleiche Element weglassen kann.

Eine Implementierung, die eine bestimmte Wahlmöglichkeit nicht enthält, MUSS so vorbereitet sein, dass sie mit einer anderen Implementierung zusammenarbeiten kann, die die Wahlmöglichkeit enthält, wenn auch unter Umständen mit einer verringerten Funktionalität.

[...] Eckige Klammern zeigen eine Wahlfreiheit an. Das kann entweder sein:

- eine *Auswahl von Werten* in einem vorgegebenen Bereich [,00' .. ,03'] — typisch für Felder mit fester Länge,
- oder eine Auswahl, ob ein Wert angegeben wird oder nicht — ... || ,80' L80 AlgID || [,83' L83 KeyID] ..., wobei der Datensatz in eckigen Klammern den *wahlweisen* Teil (= im Ermessen der Implementierung) angibt oder *bedingt* ist (= abhängig von einer in der Norm angegebenen Bedingung).

— Leerseite —

Application Interface for smart cards used as Secure Signature Creation Devices — Part 1: Basic services

Anwendungsschnittstelle für Chip-Karten, die zur Erzeugung qualifizierter elektronischer Signaturen verwendet werden — Teil 1: Allgemeine Dienste

- — - — *Partie 1 : -*

ICS:

Descriptors:

Document type: European Standard
Document subtype:
Document stage: CEN Enquiry
Document language: E

STD Version 2.4e - RC2

Contents

Page

Foreword.....	7
Introduction	8
1 Scope	8
2 Normative references	9
3 Terms and definitions	10
4 Symbols and abbreviations	15
5 Signature application	18
5.1 Application Flow	18
5.2 Trusted environment versus untrusted environment	22
5.3 Digital signatures in privacy context	22
5.4 Selection of ESIGN application	23
5.4.1 Exceptions for Secure Messaging	23
5.5 Selection of cryptographic information application	24
5.6 Concurrent usage of signature applications	24
5.6.1 Methods of channel selection	24
5.6.2 Security issues on multiple channels	24
5.7 Security environment selection	24
5.8 Key selection	25
5.9 Security Services	25
6 User verification	26
6.1 Knowledge based user verification	26
6.1.1 Explicit user verification	26
6.1.2 Password based mechanisms	27
6.1.3 Presentation formats	27
6.1.4 Retry counters	28
6.1.5 Password Change	28
6.1.6 Reset of RC and setting a new password	29
6.2 Biometric user verification	30
6.2.1 Retrieval of the Biometric Information Template	31
6.2.2 Performing the biometric user verification	31
6.2.3 Reset of RC	34
7 Digital Signature Service	35
7.1 Signature generation algorithms	36
7.2 Activation of digital signature service	36
7.3 General aspects	37
7.4 Signature Generation	38
7.4.1 No hashing in Card	38
7.4.2 Partial hashing	39
7.4.3 All hashing in Card	40
7.5 Selection of different keys, algorithms and input formats	41
7.5.1 Restore an existing SE	42
7.5.2 Modify the HT of a current SE	42
7.5.3 Modify the DST of a current SE	43
7.6 Read certificates and certificate related information	44
7.6.1 Read certificate related CIOs	44
7.6.2 Read signer's certificate from ICC	44
7.6.3 Retrieval of the signer's certificate from a directory service	45
8 Device authentication	46
8.1 Certification authorities and certificates	47

8.1.1	Certificate chains.....	47
8.1.2	Usage of cross certificates.....	47
8.2	Authentication environments.....	49
8.2.1	SCA in trusted environment.....	49
8.2.2	SCA in untrusted environment	49
8.2.3	Specification of the environment.....	49
8.2.4	Display message mechanism	50
8.2.5	Additional authentication environments.....	50
8.3	Key transport and key agreement mechanisms	50
8.4	Key transport protocol based on RSA	50
8.4.1	Authentication Steps.....	52
8.4.2	Session Key creation	61
8.5	Device authentication with privacy protection.....	63
8.5.1	Authentication steps	63
8.6	Privacy constrained Modular EAC (mEAC) protocol with non-traceability feature.....	82
8.6.1	Example for traceability case	82
8.6.2	Notation	82
8.6.3	Authentication steps	83
8.6.4	Unlinkability Mechanism with individual private keys	98
8.7	Asymmetric Authentication summary.....	106
8.8	Symmetric authentication scheme	106
8.8.1	Authentication steps	106
8.8.2	Session Key creation	110
8.9	Password-based authentication protocols.....	111
8.9.1	Notation	111
8.9.2	Authentication steps	112
8.10	Compute Session keys from key seed $K_{IFD/ICC}$	120
8.10.1	Generation of key data.....	120
8.10.2	Partitioning of the key data	121
8.10.3	Algorithm and method specific definition for key derivation	121
8.11	Compute send sequence counter SSC	123
8.12	Post-authentication phase.....	123
8.13	Ending the secure session	124
8.13.1	Example for ending a secure session	124
8.13.2	Rules for ending a secure session	124
8.14	Reading the Display Message	125
8.15	Updating the Display Message	127
9	Secure Messaging	128
9.1	CLA byte.....	128
9.2	TLV coding of command and response message	128
9.3	Treatment of SM-Errors	129
9.4	Padding for checksum calculation	129
9.5	Send sequence counter (SSC)	129
9.6	Message structure of Secure Messaging APDUs	129
9.6.1	Cryptograms	129
9.6.2	Cryptographic Checksums.....	132
9.6.3	Final command APDU construction	136
9.7	Response APDU protection.....	137
9.8	Use of TDES and AES	143
9.8.1	TDES/AES encryption/decryption.....	143
9.8.2	CBC mode	144
9.8.3	Retail MAC with TDES.....	144
9.8.4	EMAC with AES	145
9.8.5	CMAC with AES	146
10	Key Generation	148
10.1	Key generation and export using PrK.ICC.AUT	148
10.2	Key generation and export with dynamic or static SM.....	148
10.3	Write certificates.....	149

10.4	Setting keys in static secure messaging	149
11	Key identifiers and parameters	150
11.1	Key identifiers (KID).....	150
11.1.1	Secret and private keys.....	150
11.2	Public Key parameters	150
11.2.1	RSA public key parameters	151
11.3	Diffie-Hellman key exchange parameters	151
11.4	The compression function Comp()	151
11.5	DSA with ELC public key parameters.....	151
11.5.1	The plain format of a digital signature	152
11.5.2	The uncompressed encoding.....	152
11.6	ELC key exchange public parameters	153
12	Data structures.....	154
12.1	CRTs.....	154
12.1.1	CRT AT for the selection of internal private authentication keys.....	154
12.1.2	CRT AT for selection of internal authentication keys	154
12.1.3	CRT for selection of IFD's PuK.CA _{IFD} .CS_AUT	155
12.1.4	CRT for selection of IFD's PuK.IFD.AUT	155
12.1.5	CRT AT for selection of the public DH / ECDH key parameters.....	156
12.1.6	CRT AT for selection of the PBM key parameters.....	156
12.1.7	GENERAL AUTHENTICATE DH key parameters used by the Privacy Protocol.....	156
12.1.8	CRT AT for selection of ICC's private authentication key	157
12.1.9	CRT for selection of IFD's PuK.IFD.AUT	157
12.1.10	CRT for selection of PrK.ICC.KA.....	158
12.2	Key transport device authentication protocol	158
12.2.1	EXTERNAL AUTHENTICATE	158
12.2.2	INTERNAL AUTHENTICATE.....	159
12.3	Privacy device authentication protocol.....	159
12.3.1	EXTERNAL AUTHENTICATE (DH case).....	159
12.3.2	EXTERNAL AUTHENTICATE (ECDH case).....	160
12.3.3	INTERNAL AUTHENTICATE (DH case).....	161
12.3.4	INTERNAL AUTHENTICATE (ECDH case).....	162
13	AlgIDs, Hash- and DSI Formats.....	163
13.1	Algorithm Identifiers and OIDs.....	163
13.2	Hash Input-Formats	163
13.2.1	PSO:HASH without command chaining	164
13.2.2	PSO:HASH with command Chaining	164
13.3	Formats of the Digital Signature Input (DSI).....	165
13.3.1	DSI according to ISO/IEC 14888-2 (scheme 2).....	166
13.3.2	DSI according to PKCS #1 V 1.5.....	167
13.3.3	Digest Info for SHA-X	168
13.3.4	DSI according to PKCS #1 V 2.x.....	169
13.3.5	DSA with DH key parameters	171
13.3.6	Elliptic Curve Digital Signature Algorithm - ECDSA	171
14	CV_Certificates and Key Management	172
14.1	Level of trust in a certificate	172
14.2	Key Management	172
14.3	Card Verifiable Certificates	173
14.3.1	Signature-Certificates	173
14.3.2	Authentication Certificates	173
14.4	Use of the public key extracted from the certificate	173
14.5	Validity of the key extracted from a certificate	174
14.6	Structure of CVC	174
14.6.1	Non-self-descriptive certificates	175
14.6.2	Self-descriptive certificates	175
14.7	Certificate Content.....	175
14.7.1	CPI-Certificate Profile Identifier.....	176

14.7.2	CART-Certification Authority Reference Template	177
14.7.3	CHRT-Certificate Holder Reference Template	178
14.7.4	CHA-Certificate Holder Authorization Data Object (CHA-DO)	179
14.7.5	Role identifier specifications	181
14.7.6	CHAT-Certificate Holder Authorization Template (CHAT)	184
14.7.7	OID — Object identifier	184
14.7.8	CEDT — Certificate Effective Date Template	184
14.7.9	CXDT — Certificate Expiration date Template	184
14.8	Certificate signature	185
14.8.1	Non self-descriptive certificates	185
14.8.2	Self descriptive certificates	186
14.9	Coding of the certificate content	186
14.9.1	Non self-descriptive certificates	186
14.9.2	Self-descriptive certificates	187
14.9.3	Self-descriptive certificates for elliptic curve cryptography	187
14.10	Steps of CVC verification	191
14.10.1	First round: CVC verification from a Root PuK	192
14.10.2	Subsequent round(s)	193
14.11	Commands to handle the CVC	193
14.12	C_CV.IFD.AUT (non self-descriptive)	193
14.13	C_CV.CA.CS-AUT (non self-descriptive)	195
14.14	C.ICC.AUT	196
14.15	Self-descriptive CV Certificate (Example)	197
14.15.1	Public Key	198
15	Files	199
15.1	File structure	199
15.2	File IDs	200
15.3	EF.DIR	200
15.4	EF.SN.ICC	200
15.5	EF.DH	201
15.6	EF.ELC	201
15.7	EF.C.ICC.AUT	202
15.8	EF.C.CA _{ICC} .CS-AUT	203
15.9	EF.C_X509.CH.DS	203
15.10	EF.C_X509.CA.CS (DF.ESIGN)	203
15.11	EF.DM	204
16	Cryptographic Information Application	205
16.1	ESIGN cryptographic information layout example	206
16.1.1	EF.CIAInfo	208
16.1.2	EF.AOD	209
16.1.3	EF.PrKD	212
16.1.4	EF.PuKD	214
16.1.5	EF.CD	215
16.1.6	EF.DCOD	216
Annex A (normative)	Algorithm Identifiers — Coding and specification	219
Annex B (informative)	Device authentication Protocol Properties	225
Annex C (informative)	Device authentication — Cryptographic view	227
C.1	Algorithms for authentication with key exchange or key negotiation	227
C.2	Device authentication with key transport	228
C.2.1	Conformance to ISO/IEC 11770-3	228
C.2.2	Using min(SIG, N-SIG) for the signature token	229
C.3	Device authentication with key negotiation	231
C.3.1	Diffie-Hellman Key Exchange	231
C.4	Device authentication with privacy protection	233
C.4.1	Providing privacy quality	233
C.4.2	Adding non-traceability	235
C.4.3	Adding non-linkability	236

C.4.4	The authenticity of the public DH parameters	236
C.5	Device authentication with non traceability	237
C.5.1	Diffie-Hellman Key Exchange	237
C.6	Unlinkability Mechanism in the mEAC protocol with individual private keys	240
C.6.1	Use of Diffie-Hellman on base of the discrete logarithm	240
C.6.2	Use of Diffie-Hellman on base of EC-KAEG (in short ECKA)	243
C.7	The "Grandmaster Chess Attack"	246
Annex D (informative)	Personalization scenarios	247
Annex E (informative)	OID values	249
E.1	OIDs for non mEAC protocols	249
E.2	OIDs for mEAC protocols	251
Annex F (informative)	Build scheme for object identifiers defined by EN 14890	253
Bibliography		255

Foreword

This document (prEN 14890-1:2012) 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 14890-1:2008.

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

In EN 14890 Part 1, the standard allows support of implementations 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" that fulfils the requirements of Article 5.1 of the Electronic Signature Directive and therefore can be considered equivalent to a hand-written signature.

In EN 14890 Part 2, the standard specifies mechanisms to support other services like generic identification, authentication, confidentiality and signature verification services.

The standard defines a set of services that will enable the development of interoperable cards issued by any card industry sector. The standard describes 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 the 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

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 International Organization for Standardization (ISO) [and/or] International Electrotechnical Commission (IEC) 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 8.9.2.5 "Step 4.2 — Map nonce and compute generator point for integrated mapping " 117.

— The patent relates to "Sagem, MorphoMapping Patents FR09-54043 and FR09-54053, 2009".

1 Scope

This part specifies mandatory mechanisms for smart cards to be used as secure signature creation devices covering

- Signature creation
- User verification
- Device authentication
- Establishment of a secure channel
- others

The specified mechanisms are suitable for other purposes like services in the context of IAS.

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.

Note: For future implementations refer to the latest versions of the referenced documents, the following list refers to documents relevant at publication of this standard EN14890.

- [1] ISO 3166-1:2006, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*
- [2] ISO 7498-2 *Information processing systems -- Open Systems Interconnection -- Basic Reference Model – Part 2: Security Architecture*
- [3] ISO 11568-2:2005, *Banking — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*
- [4] ISO/IEC 7816-3: 2006, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts -- Electrical interface and transmission protocols protocols*
- [5] ISO/IEC 7816-4:2005, *Identification cards — Integrated circuit(s) cards with contacts — Part 4: Organization, security and commands for interchange*
< UNDER REVISION >
- [6] ISO/IEC 7816-5:2004, *Identification cards — Integrated circuit cards — Part 5: Registration of application providers*
- [7] ISO/IEC 7816-6:2004, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange*
- [8] ISO/IEC 7816-8:2004, *Identification cards — Integrated circuit cards — Part 8: Commands for security operations*
- [9] ISO/IEC 7816-11:2004, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*
- [10] ISO/IEC 7816-15:2004, *Identification cards — Integrated circuit cards — Part 15: Cryptographic Information Application*
- [11] ISO/IEC 9796-2:2010, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*
- [12] ISO/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*
- [13] ISO/IEC 11770-3:2008, *Information technology — Security techniques — Key management — Part 3, Mechanisms using asymmetric techniques - including Cor 1:2009*
- [14] ISO/IEC 14888-2:2008, *Information technology — Security techniques — Digital Signatures with appendix — Part 2, Integer factorization based mechanisms*
- [15] ISO/IEC 15946-5:2009, *Information Technology — Security Techniques — Cryptographic Techniques based on elliptic curves — Part 5: Elliptic curve generation*
- [16] ISO/IEC 18033-3:2010, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

[17] ISO/IEC 19794-2:2005, *Information technology -- Biometric data interchange formats -- Part 2: Finger minutiae data*

[18] CEN / EN 14890-1 "Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services", 2008

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

Anonymity

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

3.2

Anonymization

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

3.3

Anonymized data

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

3.4

Anonymous data

Data that cannot be linked to a specific individual

3.5

Answer-to-Reset file

Elementary file which indicates operating characteristics of the card.

3.6

a priori trusted

An operating environment which by definition can be trusted without further device authentication. An example of this is the use within a company where any available access point is connected to a trustable network.

3.7

Authentication

Authentication is the verification that an entity is the claimed one [18].

3.8

command-response pair

Set of two messages: a command followed by a response.

3.9

confidentiality protection

Confidentiality protection is the prevention of information disclosure to unauthorized individuals, entities or systems [18].

3.10

data unit

The smallest set of bits which can be unambiguously referenced.

3.11

data element

Item of information seen at the interface for which are defined a name, a description of logical content, a format and a coding.

3.12

data object

Information seen at the interface which consists of a tag, a length and a value (i.e., a data element). In this specification, data objects are referred to as BER-TLV data objects. Refer to ISO/IEC ISO/IEC 7816-4 [5].

3.13

dedicated file

File containing file control information and, optionally, memory available for allocation. It may be the parent of EFs and/or DFs.

3.14

DF name

String of bytes which uniquely identifies a dedicated file in the card.

3.15

elementary file

Set of data units or records which share the same file identifier. It cannot be the parent of another file.

3.16

file control parameters

Logical, structural and security attributes of a file.

3.17

file identifier

A 2-bytes binary value used to address a file.

3.18

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.

3.19

identification

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

3.20

integrity protection

Integrity protection is a mechanism ensuring that data cannot be modified undetectably

3.21

master file

The mandatory unique dedicated file representing the root of the file structure.

3.22

message

String of bytes transmitted by the interface device to the card or vice-versa, excluding transmission-oriented characters as defined in Part 3 of ISO/IEC 7816 [4].

3.23

mutual authentication

Both parties (ICC and IFD) are authenticated to each other.

3.24

non-traceability

→ traceless authentication

3.25

parent file

The dedicated file immediately preceding a given file within the hierarchy.

3.26

password

Data which may be required by the application to be presented to the card by its user. A password in the context of this specification is a string of numbers and/or ASCII characters.

3.27

path

Concatenation of file identifiers without delimitation. If the path starts with the identifier of the master file, it is an absolute path.

3.28

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 [64].

3.29

private key

Secret part of an asymmetric key pair e.g. signature creation data as specified in the EU directive for electronic signatures.

3.30

pseudonymisation

A particular type of anonymization that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms.

3.31

pseudonymised data

Data that can only be linked to such a person if one has possession of a decoding “key”.

3.32

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).

3.33

public key

Public part of an asymmetric key pair.

3.34

record

String of bytes which can be handled as a whole by the card and referenced by a record number.

3.35

record number

Sequential number assigned to each record which uniquely identifies the record within its elementary file.

3.36

retry counter

A counter being used to count the number of erroneous usages of a related (security) object. If the object (e.g. password entry) was used correctly (correct password entered) then the retry counter is reset to its initial value. A typical value of a retry counter is 3.

3.37

secret key

Either a symmetric key or private part of a public key pair.

3.38

traceless authentication

Traceless Authentication is an authentication which does not give any persistent cryptographic proof that the authentication has occurred.

3.39

trusted environment

An operating environment that avoids the fraud with data that is seen at the communication interface by the definition of its physical location, physical security protection or physical access conditions or other measures to protect from tampering or intrusion of data. (Refer to 8.2.3 "Specification of the environment" on page 49.)

3.40

trusted channel

A means by which a TSE and a remote trusted IT product can communicate with necessary confidence to support the TSP.

3.41

trusted path

A means by which a user and a TSE can communicate with necessary confidence to support the TSP.

3.42

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 [65].

3.43

untrustable environment

An operating environment that allows tampering and intrusion of data available at the communication interface. An environment which is not a priori trustable and which cannot prove trustability through a device authentication, must be considered as untrustable. No further operations should be done by the card holder on untrustable environment.

3.44

untrusted environment

An operating environment which is not known to be trustable. Until a proof of confidence is given (typically through a device authentication) the environment should not receive any sensitive data from the card holder, in particular a PIN entry should not be made.

After a successful device authentication, *untrusted environment turns into trusted environment*. Therefore the quality 'untrusted' does not imply 'untrustable' but the requirement of trust verification.

3.45

usage counter

A counter updated each time a related object is used. Opposite to retry counters, usage counters are not reset to their initial value after the object was successfully used.

3.46

user consent

User content is the expression of the act-of-will to a card related service.

3.47

Usage of expressions in this standard

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [58].

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

4 Symbols and abbreviations

AES	Advanced Encryption Standard
AID	Application Identifier
APDU	Application protocol data unit
AKI	Authority Key Identifier
AT	Authentication Template, CRT for Authentication
AUT	Authentication
BCD	Binary Coded Decimal
BER	Basic Encoding Rules
C	Certificate
CA	Certification Authority
CAR	CA Reference
CC	Cryptographic Checksum
CDA	Card Device Authentication
CG	Cryptogram
CH	Cardholder
CHA	Certificate Holder Authorization
CHN	Cardholder Name
CHR	Certificate Holder Reference
CIA	Cryptographic Information Application
CIO	Cryptographic Information Object
CLA	Class byte
CRT	Control Reference Template
CPI	Certificate Profile Identifier
CS	CertSign, certificate containing the public part of a signature key pair
CT	CRT for confidentiality
CV	Card Verifiable
CWA	CEN Workshop Agreement
C/S	Client/Server
D[key](msg)	Decipherment of <msg> with <key>
DE	Data Element
DES	Data Encryption Standard
DF	Dedicated File
DH	Diffie-Hellman
DH.P	DH parameter, $DH.P = g, p, q$
DIR	Directory
DO	Data Object
DS[key](msg)	Digital Signature of <msg> with <key>
DSA	Digital Signature Algorithm

DSI	Digital Signature Input
DST	Digital Signature Template, CRT for DS
E[key](msg)	Encipherment of <msg> with <key>
ECC	European Citizen Card
ECDH	DH key agreement based on elliptic curve cryptography (ELC)
ECDH.P	ECDH parameters based on elliptic curve cryptography. ECDH.P = p, a, b, G, n
ECDSA	Signature Scheme based on elliptic curve cryptography (ELC)
ELC	Elliptic Curve Cryptography
EDFB	Encrypted Data Formatted Block
FCI	File Control Information
FID	File Identifier
h(msg)	hash-code of <msg>
HT	CRT for hash code
ICC	Integrated Circuit(s) Card
ID	Identifier
IFD	Interface Device
INS	Instruction byte
KE	Key Encipherment
KID	Key Identifier
MAC[key](msg)	Message Authentication Code of <msg> built with <key>
MF	Master File
MSE	MANAGE SECURITY ENVIRONMENT
OAEP	Optimal Asymmetric Encryption Padding
OID	Object Identifier
P1-P2	Parameter bytes
PBM	Password based mechanism
PrK	Private Key
PuK	Public Key
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standards
PI	Padding Indicator
PIN	Personal Identification Number
PP	Protection Profile
PRND	Padding Random Number
PSO	PERFORM SECURITY OPERATION
PSS	Probabilistic Signature Scheme
RC	Retry Counter
RCA	RootCA
RD	Reference Data

RFU	Reserved for Future Use
RID	Registered application provider identifier
RND	Random number
RSA	Sig-Alg. of Rivest, Shamir, Adleman
SCA	Signature-Creation Application
SHA	Secure Hash Algorithm
SE	Security Environment
SIG()	Signature of
SK	Secret Key
SN	Serial Number
SM	Secure Messaging
SSC	Send Sequence Counter
SSCD	Secure Signature Creation Device
SW1-SW2	Status bytes
TDA	Terminal Device Authentication
TDES	Triple-DES
TOE	Target Of Evaluation
TPDU	Transmission Protocol Data Unit
TLS	Transport Layer Security
TLV	Tag, Length, Value
TSF	TOE Security Functions
TSP	TOE Security Policy

5 Signature application

5.1 Application Flow

The following diagram demonstrates a typical application flow as described in [22].

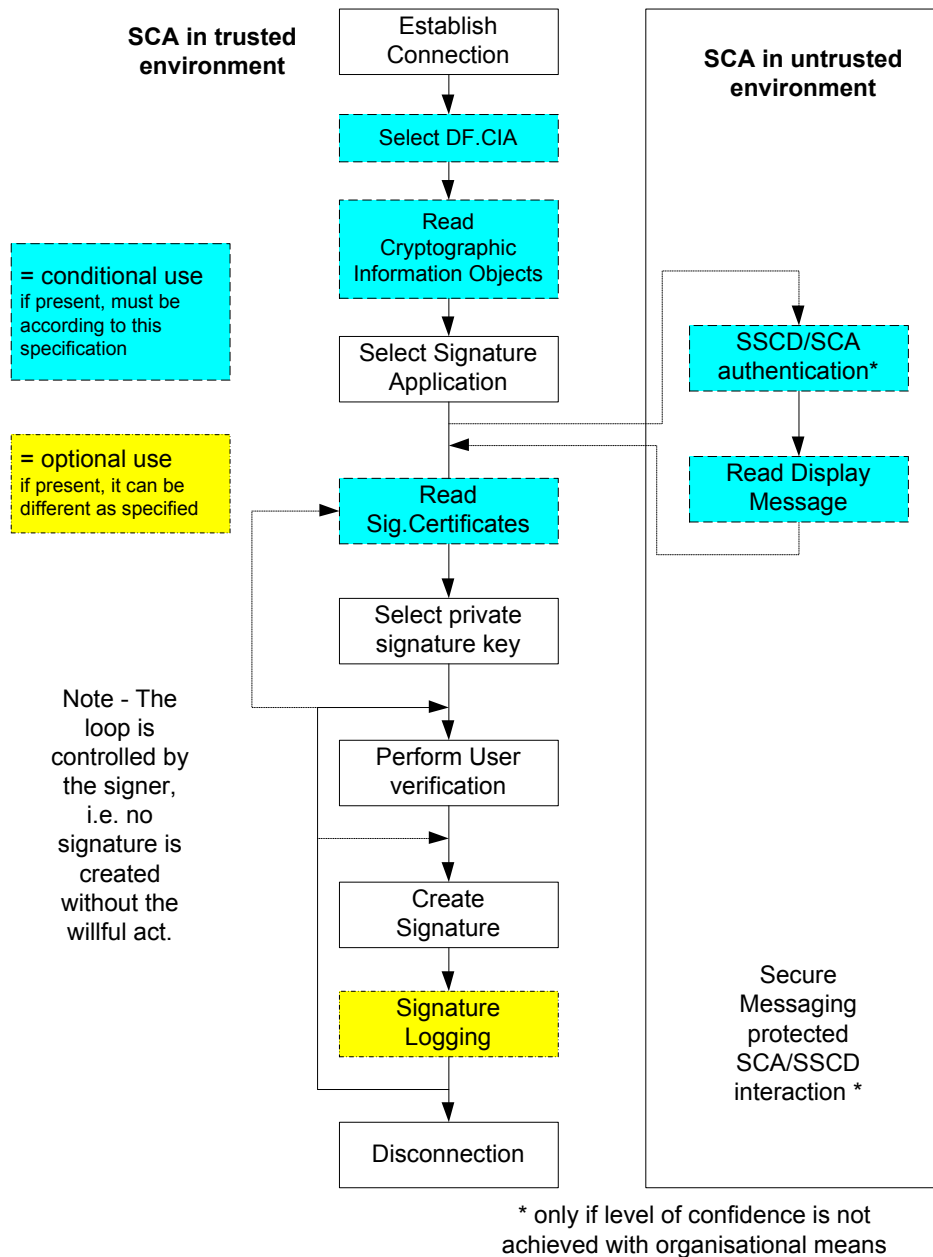


Figure 1 — Interaction sequences between SCA and SSCD in compliance with EU directive

NOTE If applications are organized on the SSCD such that they share a common device authentication, the device authentication may alternatively be done before the selection of the Signature Application.

Figure 1 shows an execution flow for a signature creation as it is mandated in [22], which specification on the security requirements. The corresponding technical implementation is given in this document which uses slightly different wording from the view point of SmartCard technology. Therefore Figure 2 corresponds to Figure 1 as seen from this specification. The following diagram demonstrates an application flow for cards used for generic applications or in privacy contexts where the unauthorized reading of a specific Card ID e.g. a Serial Number such as the SN.ICC is not allowed for privacy reasons.

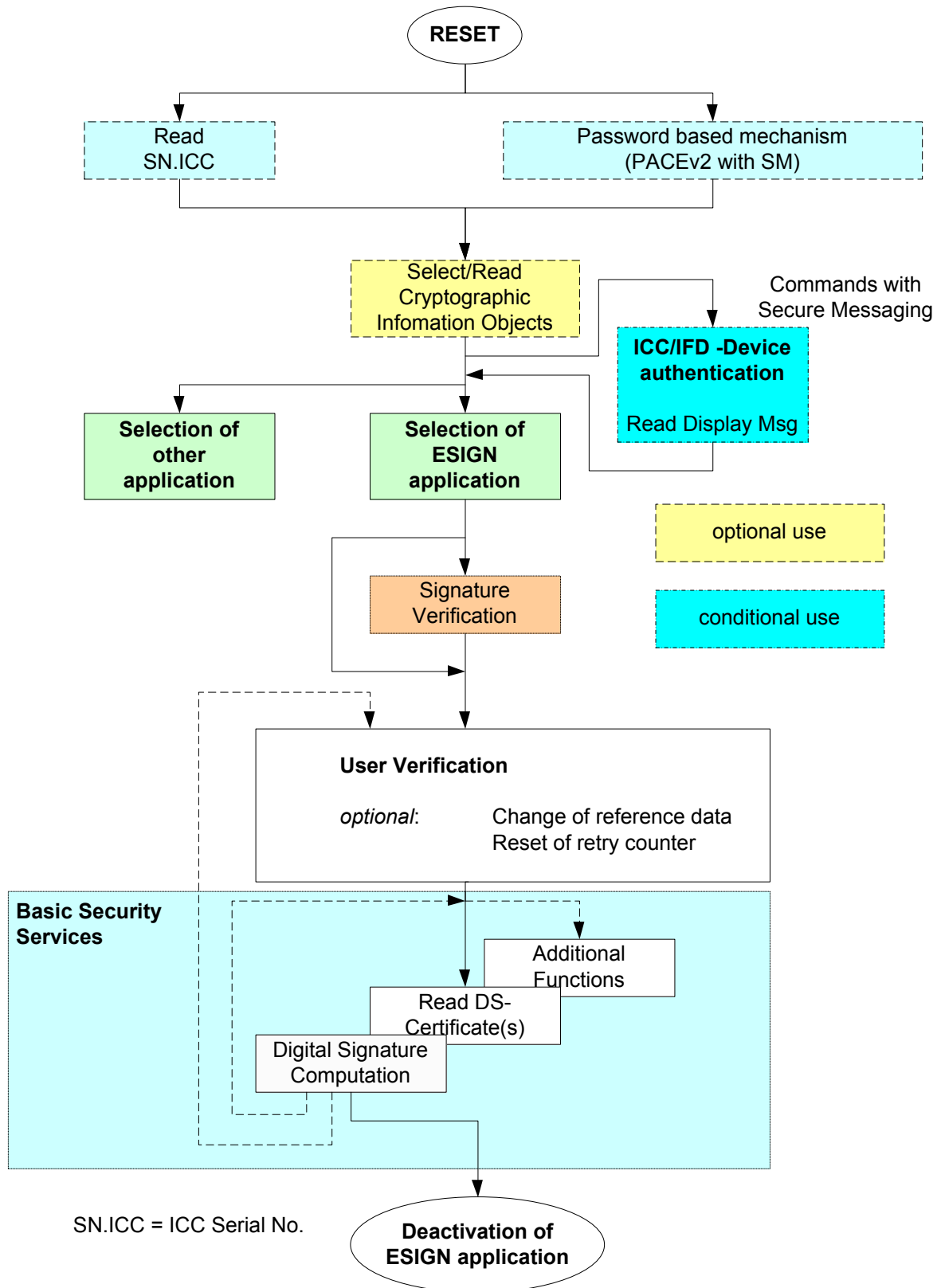


Figure 2 — Flowchart example for ICCs with ESIGN-Application as specified in this standard

Note: One well known use case for this scenario is contactless cards which are to be protected against skimming and eavesdropping attacks. Instead of reading the SN.ICC a password based mechanism

In Figure 2 dashed boxes are optional and depend on the actual device authentication protocol being applied. Reading SN.ICC would be a possible start for a non-privacy protecting device authentication (e.g. 8.4) whereas the card is addressed through contacts. For privacy protection (e.g. 8.5/8.6) reading SN.ICC would not be desirable. Instead a password based mechanism may be involved which does not allow to address the card unless a PIN is entered first. This is most suitable for contactless cards which shall not allow communication without the explicit act-of-will of the card holder.

In the example below PACEv2 is performed after the RESET or at latest after selecting the ESIGN Application, if no personal data is stored inside the CIA Application. If a device authentication protocol has been done a Restricted Identification (RI) mechanism can be performed. For details see [Part 2 – "Restricted Authentication"](#)

Reading cryptographic objects (see 16) is another optional step to let the IFD understand the particular profile of the ICC. Care has to be taken in reading those objects to avoid leaking any information which is card holder specific and that could leak privacy parameters. Typically, the information stored in the cryptographic objects is only technical and not related to card holder identity.

If the device authentication is implemented card specific (in contrast to application specific) then according to Figure 2 the device authentication may be executed prior to application selection.

Signature verification – an optional service – could precede a signature generation if a two-faced signed transaction was about to be closed.

Signature creation demands the card holder to perform a user verification in order to create a qualified electronic signature. The provision of the signature input (data to sign) is not shown in Figure 2.

For each additional signature, another user verification is mandatory to express the explicit act-of-will of the card holder to sign the transaction in question.

The example Figure 3 focusses on the execution of additional services. The same rules as in Figure 2 apply, although not again explicitly expressed, in contrast to the mandatory user verification, additional services do not require an explicit act-of-will. The additional services are described in Part 2 of this specification.

Whether for basic or additional services, a device authentication is always mandatory if the environment where the signature device is being use, is not known to be trustable. This is typical for public environment (e.g. airport, merchandise, POS). Only in trusted environment (e.g. company, campus) a device authentication can be skipped.

The user can decide to abort the operation when s(he) is prompted to enter the PIN/password during user verification. Only if the IFD did perform a device authentication, a display message can be shown on the terminal screen to inform the card holder that a device authentication is in place and s(he) may continue entering the PIN/password since the environment is safe. More information about this mechanism can be found in 8.14 "Reading the Display Message" on page 125.

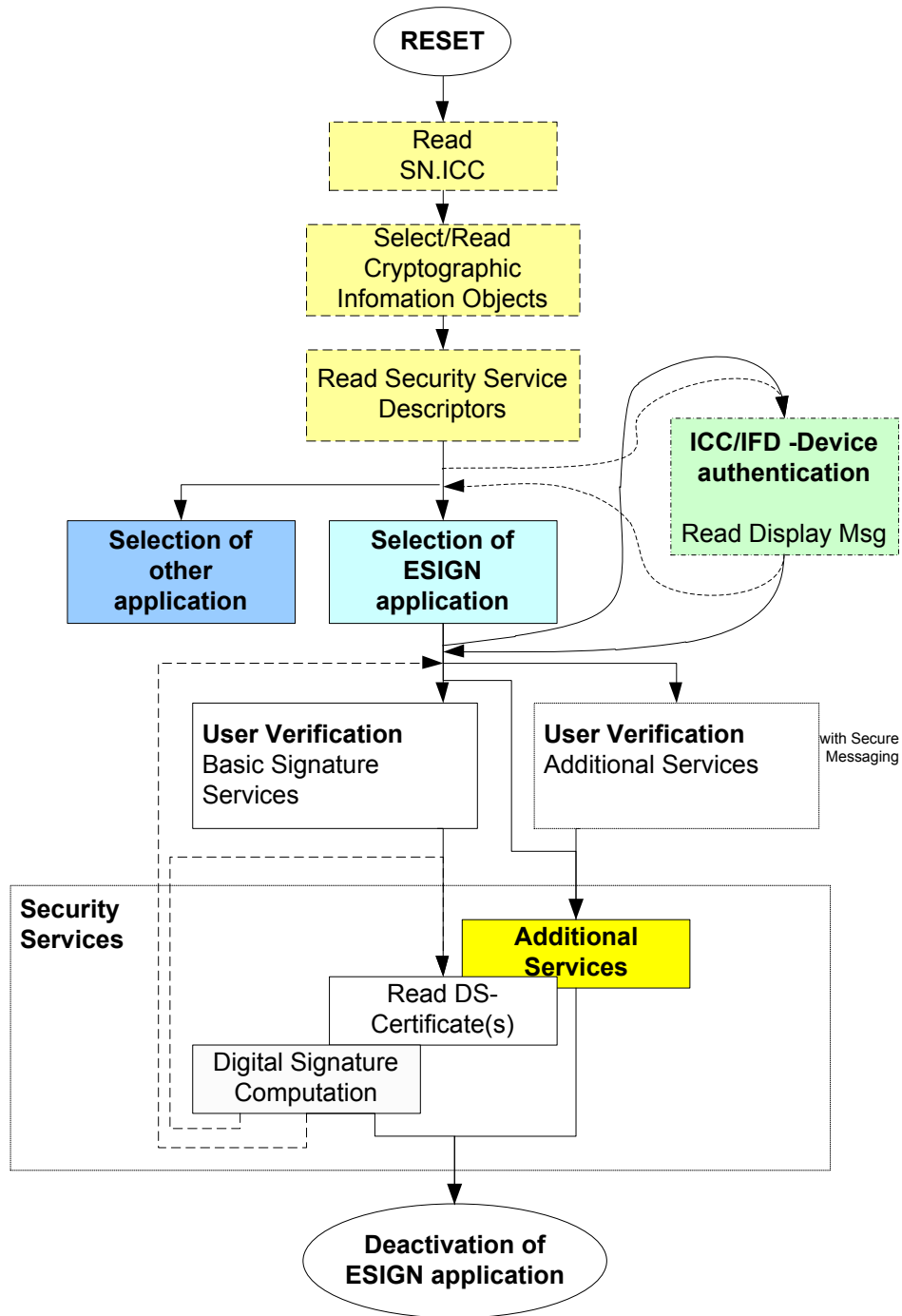


Figure 3 — Execute additional services

5.2 Trusted environment versus untrusted environment

According to the definitions in "trusted environment" and "untrusted environment", this specification describes additional mechanisms in order to accomplish the required security as claimed in the protection profile [21]. The additional mechanisms according to this specification are:

- Device authentication
- Secure messaging

5.3 Digital signatures in privacy context

On top of the question of (un-)trusted environment, "privacy context" is another environment to be considered. A card holder may be exposed to an environment that might read privacy parameters from the card ahead of any device authentication. Such privacy parameters can be the unique Card ID or other personalized parameters that allow a medium bandwidth leakage.

For instance, if the nationality of a card holder can be identified by the nature of the card description parameters (e.g. algorithm ID), then a card holder of certain nationality could be exposed to observation. Privacy context describes the requirement to allow a card holder to be confident that privacy parameters will not be exposed to unauthorized environment.

The following clause shows which authentication method is to be used for digital signatures in privacy contexts, e.g. for contactless cards as a representative of this class compared to contact oriented cards.

Table 1 – What authentication protocol to secure contactless signatures compared to contact cards

Digital Signatures according to Chapter 7 can be performed after ...	Trusted Environment (private) to be secured by organisational means	Untrusted Enviroment (public) to be secured by cryptographical means
<i>Contact</i> communication channel has been established	As in generic case no authentication protocol necessary (see 5 "Signature application" on page 18)	Chip and Terminal Authentication , see any device authentication protocols according to 8 "Device authentication" on page 46.
<i>Contactless</i> 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 card (see 8.9 "Password-based authentication protocols" on page 111.)	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 8 "Device authentication" on page 46. NOTE: The RSA transport protocol is not suitable, unless the SN.ICC is set to a "dummy value" for privacy reasons.

5.4 Selection of ESIGN application

An ESIGN application is selected by its Application Identifier (AID) [6]. The RID is registered by the ISO registration authority and has the following value:

A0 00 00 01 67.

The entire AID has 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

Table 2 — SELECT ESIGN application — command APDU

Command Parameter	Meaning
CLA	according to ISO 7816-4
INS	'A4' — SELECT
P1	'04' select by DF Name
P2	'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, chapter 7.1.1.

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

5.4.1 Exceptions for Secure Messaging

In case of a card without a MF, the SELECT by AID of an application must always be issued by the terminal in clear, even if a secure messaging session is currently active. For such cards this SELECT by AID in clear shall not break the current secure messaging session (if any). For such cards this behavior is necessary in

order to allow the association of one applet instance to one application in a Java Card. Refer to 8.11 "Compute send sequence counter SSC" on page 123.

5.5 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.

5.6 Concurrent usage of signature applications

Concurrent usage of signature applications can be realized using the mechanisms of logical channel as defined in ISO/IEC 7816-4.

5.6.1 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 [5] and will not be discussed in the specification.

5.6.2 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.

5.7 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, chapter 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:

- User verification (PIN, Password or biometric).
- Signature creation as described in chapter 7 "Digital Signature Service" on page 35.
- Device authentication as described in chapter 8 "Device authentication" on page 46.
- Key Generation as described in chapter 10 "Key Generation" on page 148.
- Verification of card verifiable certificates as described in chapter 14 "CV Certificates and Key Management" on page 172.

- Authentication services as described in chapter 6 "Client/Server Authentication" in Part 2.
- Authentication services as described in chapter 7 "Role Authentication" in Part 2.
- Key decipherment as described in chapter 8 "Encryption Key Decipherment" in Part 2.
- Signature verification as described in chapter 9 "Signature verification" in Part 2.

The actual application of the MANAGE SECURITY ENVIRONMENT is discussed in the appropriate chapters.

5.8 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.

A keyID is typically a number represented by one or more bytes describing a non-standardized value which is application- or operating system specific. The IFD may retrieve the link between a certificate and a corresponding KeyID from the DF.CIA application data as described in 16 "Cryptographic Information Application" on page 205.

5.9 Security Services

A security service is a set of SSCD functions that serve the purpose of signature generation, verification, authentication or key en-/decipherment.

Extended security services comprise the installation of data and keys, card life cycle management and other functionalities that extend the scope described in the EU directive [19]. Extended services are out of the scope of this standard.

The two volumes of this document specify the following security services.

- **User verification** service, refer to chapter 6 "User verification" on page 26
- **Key generation**, refer to chapter 10 "Key Generation" on page 148
- **Device authentication** service including secure messaging, refer to chapter 8 "Device authentication" on page 46
- **Digital signature service** for the advanced electronic signatures services of the cardholder, refer to chapter 7 "Digital Signature Service" on page 35.
- **Authentication service** as required for specific authentication procedure, refer to chapter 6 "Client/Server Authentication" in Part 2
- **Role authentication** 7 "Role Authentication" in Part 2.
- **Encryption key decipherment** service, refer to chapter 8 "Symmetric key transmission between a remote server and the ICC" in Part 2
- **Signature verification** service, refer to 9 "Signature verification" in Part 2.
- **Auxiliary data** comparison, refer to 11.2 "Auxiliary Data Verification " in Part 2.
- **Anonymity services** refer to to 11.4 "mERA-based eServices with trusted third party protocol" in Part 2.

— **Pseudonymity services**

- **Two party** service, refer to 11.3 "Restricted Identification" in Part 2.
- **Three party** service, refer to 11.4 "mERA-based eServices with trusted third party protocol" in Part 2.

6 User verification

User verification is part of the application flow as described in Figure 2 on page 19.

Three general methods of user verification are available:

- Explicit user verification
- Password Based Mechanisms (PBM)
- Biometric user verification

Specific local verification data, dedicated to protect the use of the private key for signature generation shall be applied. If several private keys for signature generation are in the card, their use may optionally be protected by different verification data.

For protection of the client/server authentication function and the key decipherment function separate (global or local according to the security policy) verification data shall be used.

In either of these cases the verification data might be subject to alteration.

The following commands, as defined in ISO/IEC 7816-4 [5], are used to manage the verification process:

- VERIFY
- CHANGE REFERENCE DATA
- RESET RETRY COUNTER.

Regardless of the usage of these commands, at any time it shall be ensured that the usage of the signature key is protected by a preceding user verification

NOTE If knowledge based or biometric user verification is part of a Common Criteria evaluation a Strength of Function (SOF) analysis shall be performed. The assessment of a knowledge based mechanism is a relatively simple and well established probabilistic analysis. For biometric authentication mechanisms the SOF analysis is more complex as e.g. the proof that a claimed False Acceptance Rate (FAR) is met might need comprehensive data bases of fingerprints.

6.1 Knowledge based user verification

Knowledge based user verification requires a password to be entered by the user. The explicit verification is done with the VERIFY command in contrast to Password based mechanisms.

6.1.1 Explicit user verification

Applications in the European domain frequently restrict passwords to numbers only. As such they are also known as 'PIN'. This standard does not restrict passwords to numbers – specifications using this standard have the freedom to restrict the range of possible input characters.

Find further information under 6.1.2.

Execution Flow 1 of 1

Table 4 — VERIFY command APDU

Command Parameter	Meaning
CLA	according to ISO 7816-4
INS	'20' VERIFY
P1	'00'
P2	<KeyRef> password reference
Lc field	Length of command data field
Data field	<verification data>

The structure and coding of the VERIFY command refer to ISO/IEC 7816-4, chapter 7.5.6.).

Table 5 — VERIFY — response APDU

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

6.1.2 Password based mechanisms

6.1.2.1 Password reference value (described as key identifier KID)

The parameter P2 codes the reference value of the password.

This standard specifies the following KIDs

KID = '8x' Key reference to local reference data for protection of the use of a private signature key (min. 6 digits or characters); the value of the KID and the purpose of the signature password shall be indicated in the cryptographic information objects.

Also other passwords may be of the type "local".

KID = '0x' Key reference to global reference data; the value of the KID and the purpose of the password shall be indicated in the cryptographic information objects.

NOTE In order to allow the co-existence of EMV-applications and ESIGN-applications on the same ICC, only the three least significant bits should be used to differentiate keys. Refer to chapter 6.5.12.2 – Table 23 of [30].

NOTE Password Based Mechanisms shall implement PIN error counters in order to avoid exhaustive retries with the PIN or password.

6.1.3 Presentation formats

The data field codes the verification data in one of the following formats.

The password to be coded is '12345'

BCD coding	12	34	5F						
ASCII coding	31	32	33	34	35				
UTF8	31	32	33	34	35				special (e.g. language specific) characters will be different from ASCII coding
Half nibble bcd	F1	F2	F3	F4	F5				
PIN in Format 2 PIN Block (see ISO 9564-1)	25	12	34	5F	FF	FF	FF	FF	

Figure 4 — Example of coding '12345' in different presentation formats

Figure 4 demonstrates the coding when the different presentation formats are used. The actual presentation format may be retrieved from information presented in DF.CIA (refer to 16 "Cryptographic Information Application" on page 205), unless implicitly known.

The passphrase length shall follow national regulations. Unless otherwise specified passwords protecting the usage of signature keys, shall have a minimum of 6 digits or characters. All other passwords shall have a minimum of 5 digits or characters.

NOTE The specifications are in compliance with appropriate protection profiles e.g. CEN CWA 14169 [21].

6.1.4 Retry counters

In order to avoid exhaustive search attacks, the password shall be protected by an appropriate retry counter.

In order to avoid an exhaustive search attack on the password under a known resetting code, the resetting code should be protected by an appropriate usage counter with a usage counter limit with a low value (typically U = 3).

After successful presentation, the appropriate retry counter is automatically reset to its initial value (typically N = 3).

For the definition of the counter types refer to 3 "Terms and definitions" on page 10.

6.1.5 Password Change

The CHANGE REFERENCE DATA command for changing the global password may be used under the same access conditions defined for the VERIFY command.

The change of DF-specific (local) password can only be performed after selection of the appropriate DF.

Execution Flow 1 of 1

Table 6 — Password Change — command APDU

Command Parameter	Meaning
----------------------	---------

CLA	according to ISO 7816-4
INS	'24' CHANGE REFERENCE DATA
P1	'00' no algorithm specified
P2	['0x' '8x'] KID of referenced password
Lc field	Length of command data field
Data field	<password> <new password>

For the description of the command refer to ISO/IEC 7816-4, chapter 7.5.6.

The length of the existing Reference Data is known in the card, so that neither a delimiter nor padding for filling up fixed formats is necessary. The length of the new password therefore computes $L_{\text{new}} = L_c - L_{\text{old}}$.

Table 7 — Password Change — response APDU

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

6.1.6 Reset of RC and setting a new password

After N (N as specified by application) subsequent false presentations of the password, the password is locked and does not allow further usage of the protected functions.

With the ISO/IEC 7816-4 command RESET RETRY COUNTER, the cardholder can initiate the reset of the RC to its initial value N. The Resetting Code shall have a minimum length of 6 digits¹⁾.

It is also possible to define a new password with the RESET RC command.

The reset of DF-specific (local) retry counter can only be performed after selection of the appropriate DF.

Table 8 — RESET RETRY COUNTER — command APDU

Command Parameter	Meaning
CLA	according to ISO 7816-4
INS	'2C' RESET RETRY COUNTER
P1	['00' .. '03']
P2	['0x' '8x'] KID of referenced password
Lc field	Length of command data field
Data field	see below

For the coding of the RESET RETRY COUNTER command refer to ISO/IEC 7816-4, chapter 7.5.10.

The content of the data field depends on the value of P1. The RESET RETRY COUNTER shall not change the security status, i.e. for using the signature creation key a VERIFY command is still required.

¹⁾ 'digit' can also be a character as part of a password.

P1 = '00' Resetting code followed without delimitation by new reference data

P1 = '01' Resetting code

P1 = '02' New reference data

P1 = '03' Data field absent

Table 9 — RESET RETRY COUNTER — response APDU

Response Parameter	Meaning
Data field	absent
SW1-SW2	See ISO/IEC 7816-4

After successful presentation of the Resetting Code, the retry counter of the referenced password is automatically reset to its initial value (typically $N = 3$).

6.2 Biometric user verification

The support of a biometric user verification (on-card matching) is optional. User verification shall always be done with a password. If biometric user verification is available in the IFD and ICC then in addition to the password verification the biometric user verification can be performed additionally, however it cannot be used instead of password verification.

The following general methods of biometric user verification are available:

1. The **sensor is off-card**, whereas the following cases apply:
 - a. The biometric verification data is sent from the interface device to the card and is compared by a match on card mechanism.
 - b. The biometric **verification and reference data are transformed** by a suitable application specific mechanism as e.g. Fuzzy Vault [59] to password / PIN format.

The verification mechanism is then performed as used for passwords / PINs by means of the VERIFY command or a password based mechanism
2. The **sensor is on-card**, so there is no need to transmit the biometric verification data from the interface device to the card.

Transforming biometric data to a unique value (b.) has the consequence that the biometric algorithm is performed completely in the offcard application and the card only has to perform a user verification by means of direct comparison with yes / no response.

The users have the benefit that they do not have to remember their password because it is linked to their biometrics and usually to an additional randomizer. The security of this mechanism is, however, only as sound as the underlying biometric algorithm i.e it is in general weaker than a password / PIN Comparison based on random passwords.

If biometric user verification is supported and the sensor is off-card, the Finger Minutiae Matcher compliant to ISO/IEC 19794-2 [17] shall be used. The On-Card Biometric Comparison Format identified by the CBEFF format type '0005' shall be applied as encoding format for finger minutiae.

The ICC shall provide the IFD with information about the supported biometric verification service using a Biometric Information Template (BIT) compliant to ISO/IEC 7816-11 [9] that shall be encoded as presented in

Table 15. The BIT shall not contain a data object for minutiae order referenced by tag '82', i.e., the card shall not rely on an ordering procedure performed by the IFD.

6.2.1 Retrieval of the Biometric Information Template

Prior to the verification, the SCA may need information about:

- AlgID of the matching algorithm and key reference of the biometric reference data;
- biometric type (e.g. fingerprint);
- biometric type instance (e.g. left pointer finger enrolled);
- format owner of the biometric data;
- format type of the biometric data;
- on-/off-card sensor.

This information may be found in the DF.CIA description (refer to 16 "Cryptographic Information Application" on page 205).

Alternatively this information may be provided in the Biometric Information Template (BIT), refer to ISO/IEC 7816-11 [9]. The BIT may be present in the DF.CIA or be retrieved with the GET DATA command.

The enrolment process is out of the scope of this standard.

Table 10 — Retrieve Biometric Information Template(s) — command APDU (optional)

Command Parameter	Meaning
CLA	according to ISO 7816-4
INS	'CA' GET DATA
P1-P2	'7F60' Example: Biometric Information Template
Le field	'00'

For the coding of the command GET DATA refer to ISO/IEC 7816-4, chapter 11.4.3.

Table 11 — Retrieve Biometric Information Template(s) — response APDU (optional)

Response Parameter	Meaning
Data field	BIT (Value field of Biometric Information Template(s))
SW1-SW2	Refer to ISO/IEC 7816-4

For the format of the biometric information template refer to 6.2.2.2 "Biometric Templates" on page 33.

6.2.2 Performing the biometric user verification

Two situations have to be distinguished:

- Sensor **off**-card;

— Sensor **on**-card.

Secure messaging (refer to 9.6 "Message structure of Secure Messaging APDUs" on page 129 is required when executing commands on biometric user verification with Sensor off-card.

6.2.2.1 Sensor off-card

The sensor is outside the ICC, i.e. the captured biometric data needs to be sent to the ICC for on-card matching.

The IFD retrieves the Biometric Information Template by means of a GET DATA command according to 6.2.1. The corresponding path attribute in the Cryptographic Information Application denotes the DF that shall be selected prior to this GET DATA command.

Then the IFD uses a VERIFY command to process the biometric data structured according to the biometric template.

Table 12 — Biometric user verification — command APDU (Biometric verification)

Command Parameter	Meaning
CLA	according to ISO 7816-4
INS	'21' VERIFY
P1	'00'
P2	'xx' reference data qualifier according to 6.1.2.1.
Lc field	Length of command data field
Data field	<biometric data template> refer to Table 14

For the structure and content of the APDU refer to ISO/IEC 7816-4, chapter 7.5.6.

Table 13 — Biometric user verification 2 of 2- response APDU

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

6.2.2.2 Biometric Templates

Table 14 — Biometric data template

Tag	Length	Value		
'7F 2E'	Var.	Biometric Data Template		
		Tag	Length	
		'81'	Var.	Biometric data with standardized format (primitive encoding)

Table 15 — Biometric Information Template

Tag	Length	Value				Presence
'7F 60'	Var.	Biometric Information Template (BIT)				
		Tag	Length	Value		
		'83'	'01'	Reference data qualifier according to 6.1.2.1.		Mandatory
		'A1'	Var.	Biometric Header Template (BHT) in compliance with CBEFF		Mandatory
				Tag	Length	Value
				'81'	'01'	'08' (fingerprint)
				'82'	'01'	Biometric subtype (refer to ISO 7816-11 Table C.3)
				'87'	'02'	'0101' (ISO/IEC JTC 1/SC37)
				'88'	'02'	'00 05'
				Biometric matching algorithm parameters		Optional
				Tag	Length	Value
				'B1'	Var.	Minimum number of minutiae required (1 byte, binary coding) Maximum number of minutiae accepted (1 byte, binary coding)
				'81'	'02'	

6.2.2.3 Sensor on-card

For the on-card verification, the VERIFY command selects the biometric data reference through P2.

Execution Flow

Table 16 — Biometric verification — command APDU

Command Parameter	Meaning
CLA	according to ISO 7816-4
INS	'21' VERIFY
P1	'00' no algorithm specified
P2	['0x' '8'x] KID of referenced password or biometric data reference
Lc field	Length of command data field
Data field	'5F2E' '00' '4D' '00' empty verification DO and extended. header list DO

For the description of the command refer to ISO/IEC 7816-4, chapter 7.5.6.

The length of the existing Reference Data is known in the card, so that neither a delimiter, nor padding for filling up fixed formats is necessary.

Table 17 — Biometric verification — response APDU

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

For the structure and content of the APDU refer to ISO/IEC 7816-4, chapter 7.5.6.

6.2.3 Reset of RC

For resetting the RC refer to 6.1.5 "Reset of RC and setting a new password".

With respect to biometric reference data only the RESET RETRY COUNTER command variants that make use of P1 = '01' and P1 = '03' are specified in this document. The usage of the command variants with P1 = '00' and P1 = '02' is outside the scope of the document as the enrolment process is not defined in this document.

7 Digital Signature Service

This chapter is related to technical aspects of electronic signatures according to Article 5 of the EU Directive 1999/93/EC [1].

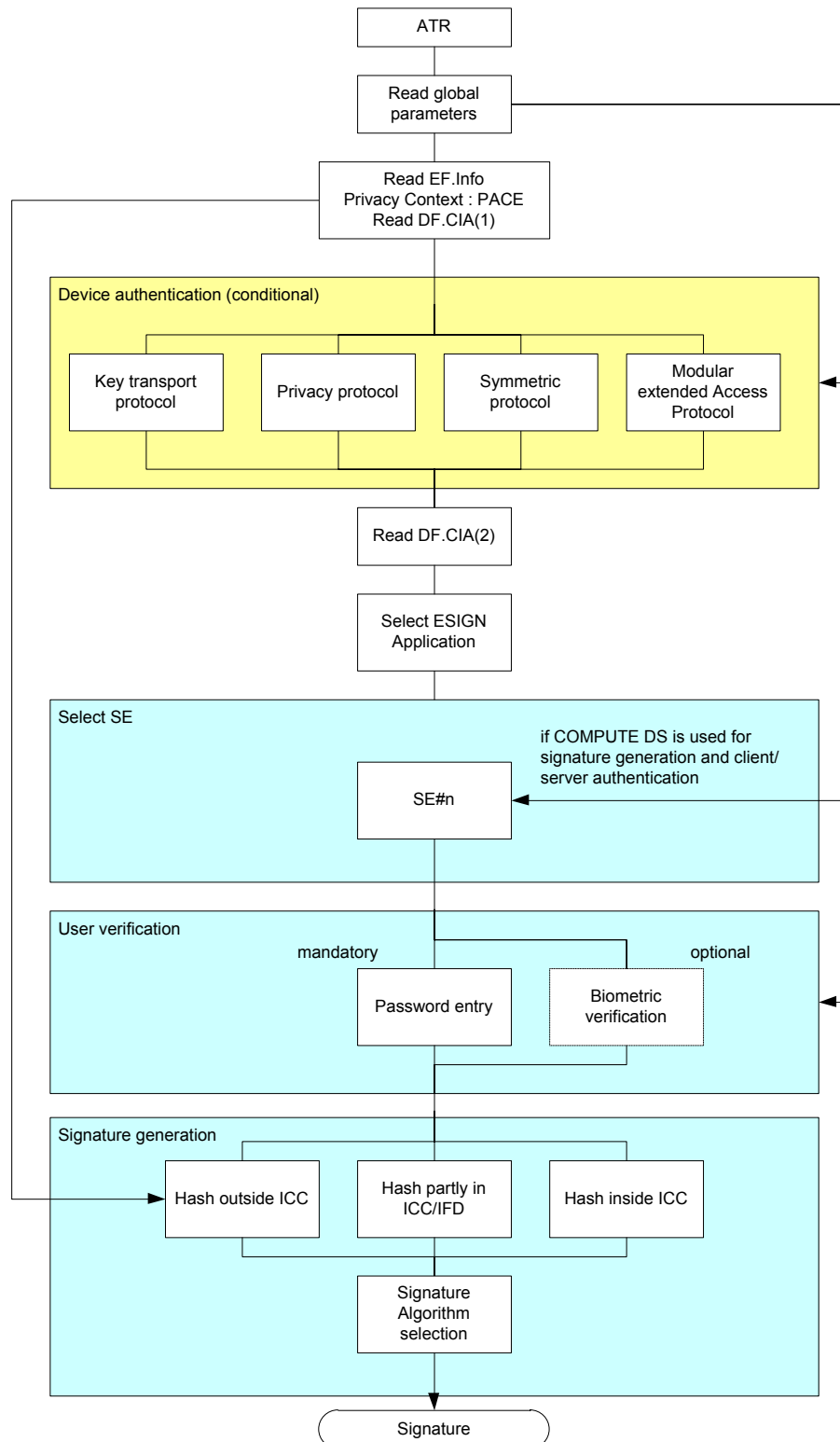


Figure 5 — Flow of selectable options for signature generation

Note: For QES additional organizational aspects need to be considered like evaluation (e.g. according to the PP SSCD (e.g. [21]), certification, CA accreditation).

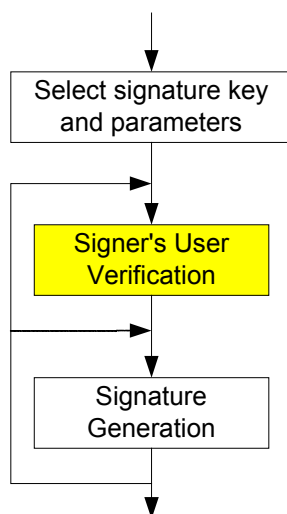
The technical requirements are fulfilled by the specifications of this standard.

7.1 Signature generation algorithms

For signature generation, algorithms as referenced in the current European and national algorithm catalogs shall be applied. Examples of existing documents are given in [23] [24] [25] [26] [27].

7.2 Activation of digital signature service

In order to enable the digital signature service a user verification shall be applied prior to signature generation.



NOTE The loop is controlled by the signer, i.e. no signature is created without a willful act.

Figure 6 — Signer's User Verification

Refer to Figure 1 on page 18 for the overview of the signature generation flow.

A knowledge based interaction always expresses the explicit will of the card holder to sign a document whereas a biometric identification does not necessarily imply the intention to sign. Therefore knowledge based user verification is a mandatory feature, unless a particular specification in a corresponding protection profile supersedes the claim of this standard.

For the description of the user verification refer 6 "User verification" on page 26.

7.3 General aspects

A digital signature process consists of several steps. Some of them are done outside the ICC, some of them are done inside the ICC, and some could be done on either side.

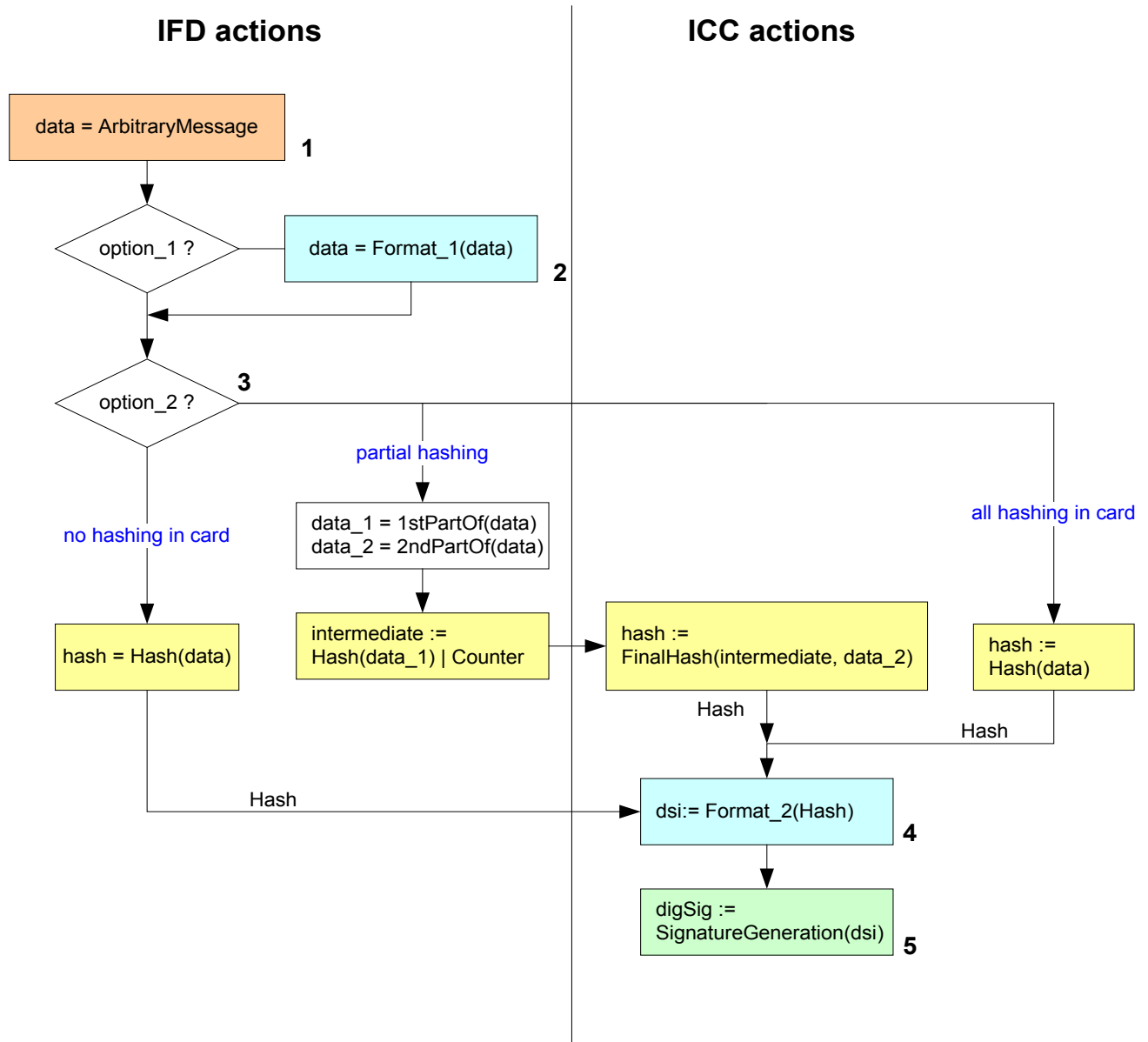


Figure 7 — Data-Flow chart for signature generation process (RSA Example)

Figure 7 shows an example of the alternatives to process a hash data signing. Signature input formatting aspects are not covered by Figure 7. The numbers 1..5 refer to the steps described below. The intermediate hash-code is the digest of preceding hash rounds followed by the big endian bit count. Only fully hashed blocks are transmitted, therefore the length of *data_1* (on partial hashing) is always a multiple of the digest size, related to the applied algorithm.

In principle, the signature generation process works as follows:

1. The signature generation process starts with an arbitrary message.
2. Optionally the original message is formatted in an application specific way. Typically, signature attributes and other format information besides the actual document to be signed, are added to the arbitrary

message. The process of pre-formatting the data to be hashed is expressed as **Format_1** mechanism. The specification of the optional format mechanism **Format_1** is outside the scope of this document.

3. The data shall be hashed by applying a hash function which is on the list of the applicable hash functions. The hash-code could be considered as a compressed version of the text. Depending on *option_2* the hashing will be done either
 - completely outside the ICC,
 - partly outside and partly inside the ICC, thus data is split into two parts,
 - completely inside the ICC depending on the card functionality and the software organization.
4. Depending on the signature algorithm the *hash-code* shall be formatted by a format mechanism **Format_2**. Typically this is a *padding mechanism* as described in 13.3 "Formats of the Digital Signature Input (DSI)" on page 165. The result of this formatting is a *Digital Signature Input (dsi)*. Several format mechanisms have been defined, some of them are evaluated as "weak" and should not be used. The algorithm catalogues cover these aspects and propose formatting schemes which are approved until a specified date.
5. The final *dsi* (Digital Signature Input) is the string to be transformed by the signature algorithm. The result is the Digital Signature DS[<key>](*dsi*).

7.4 Signature Generation

Depending on which data path is used in Figure 7, from the ICC's point of view the following cases could be distinguished.

7.4.1 No hashing in Card

The data to be signed is completely hashed outside the ICC. Depending on the algorithm the *hash-code* is transferred to and signed by the ICC using the PSO:COMPUTE DIGITAL SIGNATURE command.

Execution Flow 1 of 1

Table 18 — Signature computation (no hashing in card) — command APDU

Command Parameter	Meaning
CLA	according to ISO 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'9E' COMPUTE DIGITAL SIGNATURE
P2	'9A' 'data to be signed'
Lc field	Length of command data field
Data field	data to be signed
Le field	'00'

For the structure and content of the APDU refer to ISO/IEC 7816-8, chapter 5.2.

The response data field contains the *plain signature* without further TLV coding.

Table 19 — Signature computation (no hashing in card) — response APDU

Response Parameter	Meaning
Data field	plain signature without further TLV coding
SW1-SW2	Refer to ISO/IEC 7816-4

7.4.2 Partial hashing

The first part of the data to be signed is hashed outside the ICC. The intermediate hash-code is transferred to the ICC by the PSO:HASH command together with the remaining part of the data. Afterwards the signature is generated by the PSO:COMPUTE DIGITAL SIGNATURE command.

Execution Flow 1 of 2

Table 20 — Signature computation 1 of 2 (transfer intermediate hash-code) — command APDU

Command Parameter	Meaning
CLA	according to ISO 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'90' hash
P2	'A0' input template for hash computation
Lc field	Length of command data field
Data field	'90' L ₉₀ <intermediate hash-code followed by big endian bit counter> '80' L ₈₀ <data to be hashed>

For the structure and content of the APDU refer to ISO/IEC 7816-8, chapter 5.2.

For the content of the command data field or DO 'A0' refer to 13.2 "Hash Input-Formats" on page 163.

The response data field is absent.

Table 21 — PSO-Hash response

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

Execution Flow 2 of 2

The second command performs a digital signature on the hashed value.

Table 22 — Signature computation 2 of 2 (compute signature) — command APDU

Command Parameter	Meaning
CLA	according to ISO 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'9E' COMPUTE DIGITAL SIGNATURE
P2	'9A' data to be signed
Le field	'xx'

For the structure and content of the APDU refer to ISO/IEC 7816-8, chapter 5.2.

The response data field contains the plain signature without further TLV coding.

Table 23 — PSO-COMPUTE DIGITAL SIGNATURE response

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

7.4.3 All hashing in Card

The data to be signed is hashed inside the ICC. This is done by the PSO:HASH command. Finally the signature is generated by the PSO:COMPUTE DIGITAL SIGNATURE command.

Execution Flow 1 of 2

Table 24 — Signature computation 1 of 2 (all hashing in ICC) — command APDU

Command Parameter	Meaning
CLA	according to ISO 7816-4
INS	'2A' PSO:HASH
P1	'90' hash operation
P2	'80' plain value
Lc field	'xx'
Data field	plain data to be hashed

For the structure and content of the APDU refer to ISO/IEC 7816-8, chapter 5.2.

The response data field is absent.

Table 25 — Signature computation 1 of 2 (all hashing in ICC) — response APDU

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

Execution Flow 2 of 2

The second command computes the digital signature.

Table 26 — Signature computation 2 of 2 (compute signature) — command APDU

Command Parameter	Meaning
CLA	according to ISO 7816-4
INS	'2A' PERFORM SECURITY OPERATION
P1	'9E' COMPUTE DIGITAL SIGNATURE
P2	'9A' data to be signed
Le field	'00'

For the structure and content of the APDU refer to ISO/IEC 7816-8, chapter 5.2.

The response data field contains the plain signature without further TLV coding.

Table 27 — PSO-COMPUTE DIGITAL SIGNATURE response

Response Parameter	Meaning
Data field	plain signature
SW1-SW2	Refer to ISO/IEC 7816-4
^a In the case of ECDSA the digital signature is calculated according to ISO/IEC 15946-2 [15], for the format refer to [42] chapter 5.3	

7.5 Selection of different keys, algorithms and input formats

If the card supports more than one key and an implicit selection is not available, then the private signature key needs to be selected.

If the card supports several digital signature algorithms or different Digital Signature Input formats (refer to 13 "AlgIDs, Hash- and DSI Formats" 163, then the algorithm or the DSI format respectively shall be selectable. However, it is possible that either (e.g. an algorithm), is implicitly specified if a key is selected.

It is further possible that an algorithm, a key or a signature input format is not implicitly known, nor uniquely specified.

In all of the above cases the appropriate parameter shall be selected explicitly with a MANAGE SECURITY ENVIRONMENT command as described in ISO/IEC 7816-4, chapter 11.5.11.

This can be achieved by

- restoring an existing SE (refer to 7.5.1)
- modifying a KeyID/[AlgID] in a template (refer to 7.5.3)

7.5.1 Restore an existing SE

Execution Flow 1 of 1

Table 28 — MANAGE SECURITY ENVIRONMENT — command APDU

Command Parameter	Meaning
CLA	according to ISO 7816-4
INS	'22' MANAGE SECURITY ENVIRONMENT
P1	'F3' RESTORE
P2	SE# security environment number

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

The response data field is absent.

Table 29 — MANAGE SECURITY ENVIRONMENT response

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

NOTE The actual SE# is described in Part 2 of this specification.

7.5.2 Modify the HT of a current SE

If a hash algorithm is not implicitly known by the ICC, it shall be selected with the MANAGE SECURITY ENVIRONMENT command.