

	Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV Teil 3: Personalisierungs-Kommandos	Vornorm DIN V 66291-3
ICS 35.240.15	Vornorm Chip cards with digital signature application/function according to SigG and SigV — Part 3: Commands for personalisation Cartes à circuit intégré avec application/fonction signature digitale selon SigG et SigV — Partie 3: Commandements de personnalisation Eine Vornorm ist das Ergebnis einer Normungsarbeit, das wegen bestimmter Vorbehalte zum Inhalt oder wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens vom DIN noch nicht als Norm herausgegeben wird. Zur vorliegenden Vornorm wurde kein Entwurf veröffentlicht. Erfahrungen mit dieser Vornorm sind erbeten — vorzugsweise als Datei per E-Mail an ni@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter http://www.din.de/stellungnahme abgerufen werden; — oder in Papierform an den Normenausschuss Informationstechnik (NI) im DIN, Deutsches Institut für Normung e.V., Burggrafenstraße 6, 10787 Berlin Fortsetzung Seite 2 bis 18 Normenausschuss Informationstechnik (NI) im DIN Deutsches Institut für Normung e.V.	



Vorwort

DIN V 66291-3 wurde vom Arbeitsausschuss Identifikationskarten im Normenausschuss Informationstechnik (NI) erarbeitet.

Am 22. Juli 1997 wurde vom Deutschen Bundestag als Artikel 3 des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) das Gesetz zur digitalen Signatur (SigG) verabschiedet, am 22. Oktober 1997 wurde dieses Gesetz um die Verordnung zur digitalen Signatur (Signaturverordnung – SigV) ergänzt. Beide Gesetze liegen in der überarbeiteten Fassung vom November 2001 vor.

DIN V 66291-3 ist Bestandteil einer vierteiligen Normenreihe für Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, von der bisher die Teile 1 (Beschreibung der Anwendungsschnittstelle), 2 (Personalisierungsprozesse) und 4 (Grundlegende Sicherheitsdienste) veröffentlicht worden sind.

DIN V 66291-3 beschreibt Personalisierungskommandos für Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, die auf den in DIN V 66291-2 beschriebenen Personalisierungsabläufen basieren.

Die Prä-Initialisierung von Karten ist nicht Bestandteil dieser Vornorm.

Die in DIN V 66291-3 beschriebenen Kommandos stehen nicht in Konkurrenz zu bereits anderswo existierenden Personalisierungskonzepten und sollen diese auch nicht ersetzen.

Alle beschriebenen Kommandos beruhen auf den in ISO/IEC 7816-4, ISO/IEC 7816-6, ISO/IEC 7816-8 und ISO/IEC 7816-9 beschriebenen Kommandos und Datenelementen.

DIN V 66291-3 wurde in englischer Sprache verfasst, um so die Vornorm bei Normungsaktivitäten auf europäischer und internationaler Ebene unmittelbar nutzen zu können und sie auch für nicht-deutschsprachige Experten verwendbar zu machen.

Contents

	Page
1 Scope	4
2 Normative references	4
3 Abbreviations	5
4 Cards with GENERATE ASYMMETRIC KEY PAIR command	6
4.1 Pre-Initialisation Phase (V-Phase)	6
4.2 Initialisation by the CM (Phase 0)	6
4.2.1 Storage of ICCSN	6
4.2.2 Generation of SK.ICC.AUT / PK.ICC.AUT	7
4.2.3 Storage of the Certificate C.ICC.AUT	8
4.3 Pre-Personalisation Phase (Phase 1)	9
4.4 Signature Key Pair Generation (Phase 2)	9
4.4.1 PK Export with SK.ICC.AUT Signature from EF.PK_GEN	9
4.4.2 PK Export with SM	11
4.4.3 Generation of AKP and separate export of the PK	12
Annex A (normative) Structure and Content of EF.PK_GEN	15
Annex B (informative) Creation of Files	17

1 Scope

This specification defines command sequences for the personalisation of cards with signature application/function on the basis of the personalisation procedures described in DIN V 66291-2. The pre-initialisation of cards is not subject of this standard.

Existing personalisation concepts may coexist with the procedures described in this document.

2 Normative references

This Prestandard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this Prestandard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz — SigG) vom 16. Mai 2001 — in Kraft seit dem 22. Mai 2001, BGBl. I S. 876 (German digital signature law).

Verordnung zur elektronischen Signatur (Signaturverordnung — SigV) vom 16. November 2001 — in Kraft seit dem 22. November 2001, BGBl. I S. 3074 (German signature ordinance).

DIN V 66291-1:2000, *Chip cards with digital Signature Application / Function according to SigG and SigV — Part 1: Application interface.*

DIN V 66291-2:2003, *Chip cards with digital Signature Application / Function according to SigG and SigV — Part 2: Personalisation Processes.*

DIN V 66291-4:2002, *Chip cards with digital Signature Application / Function according to SigG and SigV — Part 4: Basic security services.*

ISO/IEC 7816-3:1997 *Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocols.*

ISO/IEC FCD 7816-4.2:2002, *Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange.*

ISO/IEC FCD 7816-6:2002, *Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements for interchange.*

ISO/IEC FCD 7816-8:2002, *Identification cards — Integrated circuit(s) cards with contacts — Part 8: Interindustry commands for a cryptographic toolbox.*

ISO/IEC FCD 7816-9:2002, *Identification cards — Integrated circuit(s) cards with contacts — Part 9: Interindustry commands for card and file management.*

ISO/IEC FCD 7816-15:2002, *Identification cards — Integrated circuit(s) cards with contacts — Part 15: Cryptographic Token Information in IC Cards.*

ISO/IEC 9796-2:1997, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Mechanisms using a hash-function.*

CEN/ISSS WS/E-SIGN, *CEN Workshop Agreement, Group F: Secure signature-creation devices, 01.03.2001.*

3 Abbreviations

AID	Application Identifier
AKP	Asymmetric Key Pair
AlgID	Algorithm Identifier
AM	Access Mode
AUT	Authentication
AT	CRT for Authentication
C	Certificate
CC	Cryptographic Checksum
CIA	Cryptogr. Information Application
CH	Certificate Holder
CM	Card Manufacturer
CRT	Control Reference Template
DF	Dedicated File
DO	Data Object
DS	Digital Signature
DSB	Digital Signature Block
DSI	Digital Signature Input
DST	CRT for Digital Signature
EF	Elementary File
FCI	File Control Information
FCP	File Control Parameter
FID	File Identifier
GDO	Global Data Objects
ICC	Integrated Circuit(s) Card
ICCSN	ICC Serial Number
LCSI	Life Cycle Status Indicator
MSE	MANAGE SECURITY ENVIRONM.
PK	Public Key

PV	Plain Value
Ref	Reference
SC	Security Condition
SigG	Signatur-Gesetz (Signature Act)
SigV	Sig.-Verordnung (Sig. Ordinance)
SM	Secure Messaging

4 Cards with GENERATE ASYMMETRIC KEY PAIR command

4.1 Pre-Initialisation Phase (V-Phase)

The loading of the initial card data and structures, e.g. system specific keys for the personalisation process etc., is implementation dependent.

4.2 Initialisation by the CM (Phase 0)

4.2.1 Storage of ICCSN

According to DIN V 66291-2, for the initialisation by a card manufacturer, as a first step the ICCSN is stored in the EF.GDO. See tables 1 to 4.

Table 1 — SELECT Command for Selection of EF.GDO

CLA	As defined in ISO/IEC 7816-4
INS	'A4' = SELECT
P1	'02' = EF file selection
P2	'0C' = No FCI to be returned
Lc	'02' = Length of subsequent data field
Data field	'2F02' = FID of EF.GDO, see DIN V 66291-4
Le	Absent (for encoding $N_e = 0$)

Table 2 — SELECT Response

Data field	Absent
SW1-SW2	'9000' or specific status bytes