

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
|               | <p>Chipkarten mit Digitaler Signatur-Anwendung/Funktion<br/>nach SigG und SigV<br/>Teil 2: Personalisierungs-Prozesse</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <p>Vornorm<br/><b>DIN V</b><br/>66291-2</p> |
| ICS 35.240.15 | <div data-bbox="603 304 1066 403" data-label="Section-Header"> <h2>Vornorm</h2> </div> <p>Chip cards with digital signature application/function according to SigG and SigV —<br/>Part 2: Personalisation processes</p> <p>Cartes à circuit intégré avec application/fonction signature digitale selon SigG et SigV —<br/>Partie 2: Procès personnalisation</p> <p>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.</p> <p>Zur vorliegenden Vornorm wurde kein Entwurf veröffentlicht.</p> <p><b>Vorwort</b></p> <p>DIN V 66291-2 wurde vom Arbeitsausschuss Identifikationskarten im Normenausschuss Informationstechnik (NI) erarbeitet. Sie beschreibt Personalisierungsabläufe für Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV.</p> <p>Im Mittelpunkt der Personalisierung stehen</p> <ul style="list-style-type: none"> <li>— die Signaturschlüssel-Generierung,</li> <li>— die Erzeugung und das Einbringen von DS-Zertifikaten (Schlüsselzertifikat und gegebenenfalls Attributzertifikate),</li> <li>— die Erzeugung und Eintragung der wissensbasierten Benutzerauthentisierungsdaten (PIN oder PW und gegebenenfalls Resetting Code) und gegebenenfalls die Erstellung der PIN-Briefe,</li> <li>— das Erzeugen und Einbringen von optischen Personalisierungsdaten,</li> <li>— das Erzeugen und Einbringen persönlicher Daten (Cardholder Name, benutzerspezifische Display Message) in Abhängigkeit vom Personalisierungsmodell, sowie</li> <li>— das Erzeugen und Eintragen von Authentisierungs-Schlüsseln und AUT-Zertifikaten.</li> </ul> <p style="text-align: right;">Fortsetzung Seite 2 bis 30</p> <p>Normenausschuss Informationstechnik (NI) im DIN Deutsches Institut für Normung e. V.</p> |                                             |

## — Vornorm —

DIN V 66291-2 wurde in Englisch verfasst, um so die Vornorm bei Normungsaktivitäten auf europäischer und internationaler Ebene nutzen zu können und sie auch für nicht-deutschsprachige Experten verwendbar zu machen.

Stellungnahmen werden erbeten

- vorzugsweise als Datei per E-Mail an [ni@din.de](mailto: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., 10772 Berlin (Hausanschrift: Burggrafenstraße 6, 10787 Berlin).

## Contents

|          | Page                                                                                           |
|----------|------------------------------------------------------------------------------------------------|
| <b>1</b> | <b>Scope..... 4</b>                                                                            |
| <b>2</b> | <b>Normative references..... 4</b>                                                             |
| <b>3</b> | <b>Terms and definitions ..... 4</b>                                                           |
| 3.1      | Definitions..... 5                                                                             |
| 3.2      | Abbreviations ..... 7                                                                          |
| 3.3      | Notations..... 7                                                                               |
| <b>4</b> | <b>Personalisation models for a ZS..... 9</b>                                                  |
| 4.1      | Key generation from the smart card's point of view..... 9                                      |
| 4.2      | Key generation from the ZS' point of view..... 11                                              |
| <b>5</b> | <b>Phase model / Lifecycle..... 11</b>                                                         |
| 5.1      | Pre-initialisation phase ..... 11                                                              |
| 5.2      | Initialisation phase ..... 12                                                                  |
| 5.3      | Pre-personalisation phase ..... 13                                                             |
| 5.4      | Key generation phase..... 13                                                                   |
| 5.5      | Personalisation phase ..... 13                                                                 |
| 5.6      | Operational phase ..... 14                                                                     |
| <b>6</b> | <b>Process description of the decentralised model ..... 14</b>                                 |
| 6.1      | General requirements ..... 14                                                                  |
| 6.2      | Key generation by the card manufacturer ..... 15                                               |
| 6.3      | Key generation by the participant - first personalisation..... 18                              |
| 6.4      | Storage of participant secondary keys into smart cards already used by the participant..... 21 |
| <b>7</b> | <b>Generation of PK keys at the certification agency, centralised model ..... 23</b>           |
| 7.1      | Phase 3: Personalisation phase at the certification agency ..... 23                            |
| 7.2      | Phase 4: Operational phase ..... 23                                                            |
| <b>8</b> | <b>Interaction Diagrams..... 24</b>                                                            |

## 1 Scope

DIN V 66291-2 describes personalisation processes for smart cards with digital signature application/function according to SigG/SigV. The personalisation focuses on

- the signature key generation
- the generation and the storage of DS certificates (key certificate and if necessary attribute certificates)
- the generation and the storage of the knowledge-based user authentication data (PIN or password and resetting code if necessary) or biometrics and the generation of PIN-letters if necessary
- the generation and the storage of optical personalisation data
- the generation and the storage of personal data (cardholder name, participant-specific display message)
- in dependence on the personalisation model the generation and the storage of
  - authentication keys
  - and AUT-certificates.

The Prestandard considers

- the DIN-Prestandard V 66291-1 (DINSIG )
- the technology requirements according to §16 (VI) SigV of the RegTP package of measures
- the BSI (Bundesamt für Sicherheit in der Informationstechnik) manual
- relevant ISO/IEC JTC 1 SC 27 (IT Security Techniques) standards

This Prestandard is in no contradiction with the CWA "Secure Signature Creation Devices" edited by the CEN/ISSS Workshop Electronic Signatures.

## 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).

DIN V 66291-1:1999, *Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG/SigV — Teil 1: Anwendungsschnittstelle*

ISO/IEC PDTR 14516-2:1997, *Information technology - Security techniques — Guidelines for the use and management of Trusted Third Parties — Part 2: Technical aspects*

ITU-T X.509:2000, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks*

*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)*

# — Vornorm —

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

*Maßnahmenkatalog für technische Komponenten nach dem Signaturgesetz (Stand: 15. Juli 1998) der Regulierungsbehörde für Telekommunikation und Post (RegTP) nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI)*

*Maßnahmenkatalog für Zertifizierungsstellen nach dem Signaturgesetz (Stand: 15. Juli 1998) der Regulierungsbehörde für Telekommunikation und Post (RegTP) nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI)*

*CWA Secure Signature Creation Devices Delivery ESIGN- Workshop (under preparation)*

## 3 Definitions, abbreviations and notations

### 3.1 Definitions

#### 3.1.1 Certification agency (ZS)

A certification agency (Zertifizierungsstelle, ZS) is defined as an authority having the task to create and provide signature key certificates for a participant. A ZS may in a different context also be called a trust centre, a trusted third party (TTP) or a certification service provider (CSP). In this document, ZS is used to differentiate between the subordinate authorities of a ZS.

#### 3.1.2 Certification authority (CA)

A certification authority (CA) is defined as the authority which creates the certificates. It is an authority which is subordinate to the ZS.

#### 3.1.3 Registration authority (RA)

A registration authority (RA) is defined as the authority which identifies participants and registers them in a way that allows an unambiguous allocation of certificates to participants. A RA may be supported by a naming authority.

#### 3.1.4 Registration number (RN)

The personal data recorded during the registration or the participant's certificate raw data are referenced by a registration number.

#### 3.1.5 Directory service (DIR)

A directory service (DIR) is defined as the authority which makes a directory service available for a ZS, in which certificates and/or information about certificates (CRL) have been stored.

#### 3.1.6 Personalisation system (PS)

A personalisation system (PS) is defined as the authority which transfers the participant-relevant personalisation data, i.e. if necessary also the signature key pair, to the smart card.

#### 3.1.7 Key generation authority (KG)

A key generation authority (KG) is defined as the authority which generates the signature key pair. In dependence on the personalisation model the key generation may be controlled by the CA, the participant, the card manufacturer or the RA.

### 3.1.8 Centralised model

In this model the key generation and the personalisation authorities are subordinate to and directly controlled by the ZS, the participant keys are generated by the ZS. At the ZS the signature card is made ready for use.

### 3.1.9 Decentralised model

In this model, which operates according to the principle of distributed tasks, other authorities are ordered by the ZS to perform the tasks of key generation and/or personalisation so that the representatives of the ZS are able to check the regularity of the process. The participant may as well perform the key generation. As before, the CA service (certificate generation) is handled in a centralised way.

### 3.1.10 Participant

The user who has been identified by the registration authority and who aims to get a signature key certificate is defined as participant. The property of being a participant begins with the registration process and ends at the moment when the user does not possess a valid signature key certificate any more.

### 3.1.11 Naming authority

The naming authority is an authority which in a secure way (trusted channel) transfers the characteristic data of the relevant participant group to an RA or CA (e.g. professional association, business administration).

### 3.1.12 Cardholder

A cardholder is a user who has received a smart card accredited for the digital signature application/function according to SigG/SigV.

### 3.1.13 Card manufacturer

A card manufacturer is an institution which produces or issues smart cards.

### 3.1.14 Registration data

Registration data are data recorded during the registration.

### 3.1.15 Certificate raw data

Certificate raw data are registration data to be imported into a certificate; they can be referenced by a registration number.

### 3.1.16 Personal data

Personal data consist of the personal card data and the registration number.

### 3.1.17 Personal card data

Personal card data are individual data like cardholder name, PIN, display message.

### 3.1.18 Public key additional information

Public key additional information defines properties of the public key, which are relevant for the use of the private as well as the public key, e.g. key entries or headers.

The PK additional information can be used for authentic key storage during key generation.

### 3.2 Abbreviations

|              |                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------|
| AUT          | Authentication                                                                                                 |
| BSI          | Bundesamt für Sicherheit in der Informationstechnik<br>(Federal Agency for Security in Information Technology) |
| C            | Certificate                                                                                                    |
| CA           | Certification Authority                                                                                        |
| C_CV<br>card | Card Verifiable Certificate, representative of certificates that can be interpreted by the smart card          |
| CH           | Cardholder                                                                                                     |
| CM           | Card Manufacturer                                                                                              |
| CS           | CA Signature                                                                                                   |
| CV           | Card Verifiable                                                                                                |
| C_X509v3     | X 509v3 certificate, representative of certificates that cannot be interpreted by the smart card               |
| DA           | key generation outside the smart card, decentralised                                                           |
| DI           | key generation within the smart card, decentralised                                                            |
| DINSIG       | DIN V 66291-1                                                                                                  |
| DIR          | Directory Service Provider                                                                                     |
| DS           | Digital Signature                                                                                              |
| ICC          | Integrated Circuit Card(s)                                                                                     |
| ICCSN        | Serial Number of the ICC                                                                                       |
| IFD          | InterFace Device (a device communicating with the card)                                                        |
| KG           | Key Generation                                                                                                 |
| PS           | Personalisation System                                                                                         |
| PK           | Public Key (verification data)                                                                                 |
| RA           | Registration Authority                                                                                         |
| RCA          | Root Certification Authority                                                                                   |
| RegTP        | (German) regulation authority for telecommunication and postal services                                        |
| RN           | Registration Number                                                                                            |
| SigG         | German digital signature law                                                                                   |
| SigV         | German digital signature ordinance                                                                             |
| SK           | secret key or private key (signature creation data)                                                            |

|    |                                                    |
|----|----------------------------------------------------|
| TN | participant (Teilnehmer)                           |
| ZA | key generation outside the smart card, centralised |
| ZI | key generation within the smart card, centralised  |
| ZS | certification agency (Zertifizierungsstelle)       |

### 3.3 Notations

The following notation according to DINSIG serves to characterise keys and certificates:

<object descriptor> := <key descriptor> | <certificate descriptor>

<key descriptor>:=<key>.<keyholder>.<usage>

<key>:= <secret key> | <public key>

<secret key>:= SK

<public key>:= PK

<keyholder>:= <cardholder> | <certification authority> | <integrated circuit(s) card>| <interface device>

<cardholder>:= CH

<certification authority>:= CA | RCAICMIPS

<integrated circuit(s) card>:= ICC

<interface device>:= IFD

<usage>:= <digital signature> | <authentication> | <CertSign>

<digital signature>:= DS

<authentication>:= AUT

<CertSign> := CS

<certificate descriptor>:= <certificate> .<certholder>.<usage>

<certificate>:= CI C\_CVI C\_X509V3

<certholder>:= <cardholder> | <certification authority> | <integrated circuit(s) card> |<interface device>

The following notation serves to represent data sequences:

||=Concatenation of data

NOTE Apart from X 509v3 codings other certificate codings (e.g. XML) may exist as well.

## 4 Personalisation models for a ZS

The authority which performs the key generation of participant keys is particularly important for the personalisation of smart cards that can be used according to SigG and SigV; on the other hand the medium which performs the key generation is of significant importance.

**Table 1 — Basic models for key generation**

| Key generation | outside the smart card | within the smart card |
|----------------|------------------------|-----------------------|
| Centralised    | ZA                     | ZI                    |
| Decentralised  | DA                     | DI                    |

### 4.1 Key generation from the smart card's perspective

There are the following fundamental differentiation:

- Key generation outside the smart card

The key generation for the signature key pair of a participant with private and public part is performed outside the card and controlled by a certification agency ZS (ZA and DA).

- Key generation within the smart card

The key generation for the signature key pair is performed within the participant card (ZI and DI).

In the first case the key is generated under the control of the ZS. The private key is confidentially and authentically loaded into the smart card by use of a trusted channel. The public key is included in a signature key certificate which unambiguously links the name or a pseudonym of the cardholder with his public key (PK) and certifies it by means of the signature of the certification authority (CA).

In the second case the public key of the key pair generated in the smart card is retrieved and if necessary connected with further data elements and authentically transferred to the certification authority.

In both cases it is vitally important to secure the communication between smart card and certification agency (trusted channel).

Both cases are described in detail in the following diagram; only asymmetrical processes for the key management are used in this context.

The basic function of a certification agency is the generation and issue of signature key certificates to the participants.