

Publication under § 16(6) of the Digital Signature Ordinance of suitable security measures for technical components

**Published in Federal Gazette No 204a of 30 October 1998:**

# **Security Measures for Technical Components under the Digital Signature Act**

**- Date: 15 July 1998 -**

**Published by the  
Regulierungsbehörde für Telekommunikation und Post  
in cooperation with the Bundesamt für Sicherheit in der Informationstechnik (BSI)**

**Translation  
In case of divergent interpretation, the German text shall prevail**

## **Contents**

- 1 Generation and loading of signature keys
- 2 Storage and use of private signature keys
- 3 Display of data to be signed

- DRAFT TRANSLATION -

- 4 Verification of digital signatures
- 5 Verification of certificates
- 6 Issue of time stamps
- 7 Technical components commercially provided to third parties for use

**Annexes:** 1 Supplementary Information  
2 Verification of Technical Components  
3 Abbreviations

This document entitled "Security Measures for Technical Components under the Digital Signature Act" is the first of its kind to be published by the Regulatory Authority under § 16(6) of the Digital Signature Ordinance of 22 October 1997 (Federal Law Gazette I p. 2498). It is intended for manufacturers of technical components desirous of complying with the requirements of the Digital Signature Act (Federal Law Gazette I pp. 1870, 1872) and the Digital Signature Ordinance, and for the testing and confirmation bodies under § 14(4) of the Digital Signature Act.

The relevant excerpts from the Digital Signature Act (hereafter called the "Act") and Digital Signature Ordinance (hereafter called the "Ordinance") precede each set of security measures for clarity.

The measures described do not, in principle, relate to any particular technology so as to maintain unrestricted scope for innovative solutions as provided for by the Act and Ordinance. However, in view of the broad range of feasible solutions both from a technical and organisational viewpoint, this document cannot, and does not, claim to contain a comprehensive list of security measures, and the manufacturers of technical components are called upon to implement further measures as and when required. Alternative measures may be taken in given instances, provided that the requirements in the Act and Ordinance are met.

"Security Measures for Certification Authorities under the Digital Signature Act" (cf. § 12(2) of the Ordinance) are set forth in the first part of this publication.

## 1 Generation and loading of signature keys

### **The technical components required for generation of signature keys must function in such a manner that**

- **it is nearly certain that any given key can occur only once,**
- **the private key cannot be derived from the public key,**
- **the secrecy of the private key is assured,**
- **the private key cannot be duplicated, and**
- **security-relevant changes in technical components are apparent for the user**

**(cf. § 16(1) of the Ordinance).**

MC 1.1 Use of a suitable algorithm and associated parameters under § 17(2) of the Ordinance (see Annex 1) for key generation.

MC 1.2 Use of a key generator which functions in such a manner that the signature keys and specified parameters (e.g. key lengths) are almost certainly unique. It is recommended that the BSI be consulted in case of doubt.

MC 1.3 Key generation

- on the actual data storage medium of the private signature key (e.g. chip card), or
- in a separate key generation unit and loading of the key onto a data storage medium in a secure environment

in such a manner that the secrecy of the private signature key is guaranteed and the generation of a duplicate excluded (temporary storage of the key during loading excepted).

MC 1.4 Security measures alerting the user (e.g. by means of external damage or functional disruption) to security-relevant changes (i.e. changes impairing the prescribed security level). If a security-relevant change is not obvious at first sight, it must be ascertainable at least by indirect means (e.g. test procedures).

## 2 Storage and use of private signature keys

**The technical components required for generation and verification of digital signatures must function in such a manner that**

- **the private signature key cannot be derived from the signature and the signature cannot be forged by any other means,**
- **use of the private signature key is only possible following identification of the holder and requires proper possession and knowledge, and the key is not disclosed during use; biometrical characteristics may also be used for identification of the signature key holder,**
- **the identification data is not revealed and stored only on the data storage medium with the private signature key, and**
- **security-relevant changes in technical components are apparent for the user**

**(cf. § 16(2) of the Ordinance).**

MC 2.1 Use of a suitable algorithm and associated parameters under § 17(2) of the Ordinance for hashing the data to be signed.

MC 2.2 Use of a suitable algorithm and associated parameters under § 17(2) of the Ordinance for the generation of digital signatures (for "signing" the hashed values).

MC 2.3 Security measures ensuring that

- the private signature key is only released for use after identification of the signature key holder on the basis of
  - \* possession (e.g. chip card) and knowledge (e.g. PIN), and
  - \* an additional biometrical characteristic (e.g. fingerprint), if necessary,and
- the private signature key is not removed from the data storage medium during use.

This can be achieved, for example by using a suitable operating system and equipping the chip card with appropriate applications.

MC 2.4 Security measures (especially hardware-based) ensuring that it is practically impossible to derive the private signature key from the data storage medium (i.e. within a realistic time-scale and at reasonable cost).

MC 2.5 Securing of the identification data in such a manner that it cannot be derived

- from the data collection terminal,
- along the transmission path, or
- from the storage device.

If necessary, protection of the identification data against disclosure during input (e.g. reading of the PIN) by suitable precautions (e.g. a screen).

MC 2.6 Security measures as in MC 1.4.

3 Display of data to be signed

**The technical components required for display of data for signing must function in such a manner that**

- **the signing person can reliably determine what data is to receive the signature,**
- **a digital signature is provided only at the initiation of the signing person,**
- **such initiation is clearly indicated in advance,**
- **the signing person can determine, as necessary, the contents of data to be signed, and**
- **security-relevant changes in technical components are apparent for the user**

**(cf. § 16(3) sentences 1, 4 and 6 of the Ordinance).**

MC 3.1 Display of data (e.g. file name, file creator, etc.) enabling the data to be signed to be reliably identified.

MC 3.2 Precautions ensuring that

- after identification of the signature key holder and release of the private signature key for use (see MC 2.3) a digital signature cannot be generated unless its generation is initiated by the signature key holder, and
- only data determined by the signature key holder is signed.

MC 3.3 Clear indication in advance that (upon activation of a specific function) a digital signature will be generated for the data displayed (e.g. by an appropriate message on the screen).

MC 3.4 Security measures ensuring that the displayed and signed data are identical.

MC 3.5 If necessary, security measures enabling the signing person to reliably identify the content of the data to be signed (e.g. by displaying the content on the screen or by a printout).

MC 3.6 Security measures as in MC 1.4.

4 Verification of digital signatures

**The technical components required for verifying signed data must function in such a manner that**

- **the verifying person can reliably establish the identity of the signature key holder and what data has received the digital signature,**
- **the correctness of the digital signature is reliably verified and appropriately displayed to the verifying person,**
- **the verifying person can adequately determine, as necessary, the contents of signed data, and**

- **security-relevant changes in technical components are apparent for the user**  
**(cf. § 16(3) sentences 2, 4 and 6).**

MC 4.1 Display of data (e.g. file name, file creator, etc.) to reliably identify the signed data to be verified.

MC 4.2 Reliable technical verification of the digital signature of the signed data displayed on the screen and reliable display of the verification result (e.g. "Signature OK" or "Signature not OK"). See MC 5.1 ff for verification of certificates of relevance to digital signatures.

MC 4.3 If necessary, security measures enabling the verifying person to reliably identify the content of the signed data (e.g. by displaying the content on the screen or by a printout).

MC 4.4 Security measures as in MC 1.4.

## 5 Verification of certificates

**The technical components for verifying certificates must permit clear, reliable determination of whether verified certificates**

- **were present,**
  - **without having been invalidated,**
- in the register. Security-relevant changes in technical components must be apparent for the user (§ 16(3) sentences 3 and 6 of the Ordinance).**

**The technical components used to store certificates in verifiable form must function in such a manner that**

- **only authorised persons can make entries and changes,**
- **the invalidation of a certificate cannot be undetectably rescinded,**
- **information can be checked for genuineness,**
- **the information includes mention of whether the verified certificates were present at the given time, without having been invalidated, in the register of certificates,**
- **only certificates kept available for verification purposes are not publicly available for retrieval, and**
- **security-relevant changes in technical components are apparent for the user**

**(cf. § 16(4) of the Ordinance).**

### Technical components of users

MC 5.1 Access by users to certificate registers to verify that certificates were listed and valid at a specific point in time and reliable display of the verification result (e.g. display of the following message on the screen: "Certificate no. ... available and valid on ... (date)").

In case of a verification requirement (see MC 4.2), additional precautions:

- automatic verification and display of the validity period of a certificate (cf. § 7(1) subpara 5 of the Act), indicating whether the validity period had begun and the certificate was still valid at the specified point in time, and
- verification of higher-level certificates and their validity period (depending on the validity model, it may also be necessary for the higher-level certificates to have been valid either at the time the signature being verified was generated or at least at the time at which the relevant lower-level certificate was signed).

The result of such a comprehensive verification procedure could be indicated by the message "Certificate OK" or "Certificate invalidated at ... (time) on ... (date)".

MC 5.2 Security measures as in MC 1.4.

#### Technical components of certification authorities

MC 5.3 Security measures ensuring that only authorised staff can supplement and modify the certificate register (e.g. reliable identification of authorised staff and secure access control).

MC 5.4 Security measures ensuring that the invalidation of a certificate cannot be reversed unnoticed (e.g. auditor-proof log).

MC 5.5 Reliable verification of certificates upon request (see MC 5.1) and provision of reliable information with a digital signature.

MC 5.6 Use of technical components for digital signature generation which meet the requirements set forth in sections 1 to 3.

MC 5.7 Security measures ensuring that

- certificates which are kept available for public verification only cannot be publicly retrieved from the certificate register, and
- internal access (e.g. for audit purposes) is restricted to authorised staff (see MC 5.3) and recorded.

MC 5.8 Security measures as in MC 1.4 to alert operators to any security-relevant changes.

MC 5.9 Adequate performance level to minimise the risk of undue delays in the provision of information (cf. § 5(1) of the Act).

## 6 Issue of time stamps

**The technical components with which time stamps pursuant to § 9 of the Act are generated must function in such a manner that**

- **the valid official time, without any distortion, is added to the time stamp when it is generated, and**
- **security-relevant changes in technical components are apparent for the user**

**(cf. § 16(5) of the Ordinance).**

MC 6.1 Use of the official time as given by the Federal Institute of Physics and Metrology for the time stamp service.

- MC 6.2 Security measures ensuring that
- the actual official time is indicated in the time stamp to be affixed to the data, and
  - the data is digitally signed in their entirety without modification at the stated time.

MC 6.3 Use of technical components for digital key generation which meet the requirements in sections 1 to 3.

MC 6.4 Security measures as in MC 1.4.

M 6.5 Adequate performance level to minimise the risk of undue delays in the time stamp service.

## 7 Technical components commercially provided to third parties for use

**If technical components for the display of signed data (see section 3), verification of digital signatures (see section 4) or verification of certificates (see section 5) are commercially provided to third parties for use, they must function in such a manner that**

- **clear, reliable interpretation of the relevant data is assured,**
- **the technical components are automatically checked for genuineness when used, and**
- **security-relevant changes in technical components are apparent for the user**

**(cf. § 16(3) sentences 5 and 6).**

MC 7.1 Use of information technology guaranteeing unambiguous interpretation of signed data and data to be signed.

MC 7.2 Implementation of an authentication procedure to indicate to the user of the technical component whether

- the component is genuine, and
- any security-relevant changes have been made (see MC 1.4).

This can be achieved by means of a hardware-protected safety module

- in which an authentication procedure adapted for the signature components used (e.g. chip cards) is carried out (e.g. by means of asymmetric keys and separate signature key certificates for the technical components),
- in which the integrated secret key is erased if a security-relevant change (e.g. as a result of manipulation) occurs,
- on which a codeword known only to the user is displayed when the authentication procedure has been successfully completed.

## **Supplementary Information**

### **1 Suitable algorithms and associated parameters**

The algorithms and associated parameters deemed suitable under § 17(2) of the Ordinance are published regularly in the Federal Gazette (see Federal Gazette of 14 February 1998, p. 1787). An up-to-date list of these algorithms and parameters is also available at the Regulatory Authority's Internet address given below.

### **2 Technical interoperability**

For interoperability reasons the following should be observed with regard to the technical components:

- DIN-Spezifikation der Schnittstelle zu chip cards mit Digitaler Signatur-Anwendung/-Funktion nach SigG und SigV (DIN - 17.4) (DIN specification for the interface to chip cards with a digital signature application/function under the Digital Signature Act and Digital Signature Ordinance),
- X.509.

Up-to-date information about further standards, recommendations and specifications regarding technical interoperability is available on the web sites of the Regulatory Authority and BSI as given below.

### **3 Verification of technical components**

#### **3.1 Recognised testing and confirmation bodies**

The testing and confirmation bodies recognised by the Regulatory Authority in connection with the security of technical components (cf. § 14(4) of the Act) are published regularly in the Federal Gazette (see Federal Gazette of 14 February 1998, p. 1787). An up-to-date list of these bodies and accredited testing bodies is also available at the Regulatory Authority's Internet address given below.

### **3.2 Mandatory test standards**

Annex 2 contains a list of mandatory test standards for technical components under § 17(2) of the Ordinance.

### **3.3 List of suitable technical components**

An up-to-date list of the technical components for which a security confirmation certificate under § 14(4) of the Act has been issued to confirm compliance with the security requirements in the Act, is available at the Regulatory Authority's Internet address given below.

## **4 Addresses**

Additional information (e.g. available signature applications and other addresses) can be obtained from the following addresses:

- Regulierungsbehörde für Telekommunikation und Post  
Postfach 80 01  
55003 Mainz  
Federal Republic of Germany  
Tel.: +49 6131 18-2210 or 18-0 (switchboard)  
Fax: +49 6131 18-5618  
<http://www.regtp.de>
  
- Bundesamt für Sicherheit in der Informationstechnik (BSI)  
Postfach 20 03 63  
53133 Bonn  
Federal Republic of Germany  
Tel.: +49 228 9682-0 (switchboard)  
Fax: +49 228 9582-400  
<http://www.bsi.bund.de>

**Verification of Technical Components**

**Evaluation standards**

The test and evaluation standards for technical components depend on the functions provided:

1	Signature key generation and loading of private signature keys (with suitable algorithms and associated parameters under § 17(2) of the Ordinance)	<b>E 4</b>
2	Storage and use of private signature keys (use of the key in conjunction with suitable algorithms and associated parameters under § 17(2) of the Ordinance)	<b>E 4</b>
3	Registration, storage and use of identification data	<b>E 2</b>
4	Determination and hashing (with suitable algorithms and associated parameters under § 17(2) of the Ordinance) of data to be signed	<b>E 2</b>
5	Presentation of the content of data to be signed	<b>E 2</b>
6	Verification of digital signatures (verification of the signature data and display of the result)	<b>E 2</b>
7	Verification of certificates (including requests to the certificate register service and responses). NB: <b>E 4</b> is required in the case of private signature keys used to sign invalidation lists and provide information	<b>E 2</b>
8	Issue of time stamps (transmission of the data and specification of the official time by a time stamp service). NB: <b>E 4</b> is required in the case of private signature keys used to sign data	<b>E 2</b>
9	Technical components for commercial use by third parties (this concerns functions 3 to 6 and user-related parts of functions 7 and 8) <sup>1)</sup>	<b>E 4</b>

**Strength of security mechanisms**

In all cases the strength of the security mechanisms must be rated as "high".

---

<sup>1)</sup> These functions are normally implemented in a separate terminal offered on a commercial basis to third parties for their signature components (e.g. chip cards).

**Abbreviations**

BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal IT Security Agency)
MC	Security <u>m</u> ea <sup>u</sup> re to be taken to meet the requirements relating to technical <u>c</u> omponents in the Digital Signature Act and Digital Signature Ordinance