

**Maßnahmenkatalog
für technische Komponenten
nach dem Signaturgesetz
- Stand: 15. Juli 1998 -**

Herausgegeben von
der Regulierungsbehörde für Telekommunikation und Post (RegTP)
nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Inhalt

- 1 Erzeugen und Laden der Signaturschlüssel
- 2 Speichern und Anwenden des privaten Signaturschlüssels
- 3 Darstellen zu signierender Daten
- 4 Prüfen einer digitalen Signatur
- 5 Nachprüfen von Zertifikaten
- 6 Vergabe von Zeitstempeln
- 7 Technische Komponenten, die geschäftsmäßig Dritten zur Nutzung angeboten werden

- Anlagen:**
- 1 Ergänzende Hinweise
 - 2 Prüfung der technischen Komponenten
 - 3 Abkürzungsverzeichnis

Aufgrund des § 16 Abs. 6 der Signaturverordnung vom 22. Oktober 1997 (BGBl. I S. 2498) gibt die Regulierungsbehörde für Telekommunikation und Post erstmals den nachstehenden „Maßnahmenkatalog für technische Komponenten nach dem Signaturgesetz“, heraus. Er richtet sich an die Hersteller technischer Komponenten, die den Anforderungen des Signaturgesetzes vom 22. Juni 1997 (BGBl. I S. 1870, 1872) und der Signaturverordnung entsprechen wollen, sowie an Prüfstellen und an Bestätigungsstellen nach § 14 Abs. 4 SigG.

Den Maßnahmen sind zum besseren Verständnis die jeweiligen Vorschriftentexte aus Signaturgesetz und Signaturverordnung vorangestellt.

Die Maßnahmenbeschreibungen sind grundsätzlich technikneutral, um den durch das Signaturgesetz und die Signaturverordnung vorgegebenen Raum für innovative Lösungen uneingeschränkt zu erhalten. Die beschriebenen Maßnahmen können im Hinblick auf die unterschiedlichen technischen und organisatorischen Lösungsmöglichkeiten dennoch nicht abschließend sein und entbinden daher die Hersteller technischer Komponenten nicht von ihrer Pflicht, nach Bedarf auch weitergehende Maßnahmen zu treffen. Auch alternative Maßnahmen bleiben im Einzelfall unbenommen, soweit dadurch die Vorgaben aus Signaturgesetz und Signaturverordnung ebenfalls erfüllt werden.

Neben diesem Maßnahmenkatalog wird ein „Maßnahmenkatalog für Zertifizierungsstellen nach dem Signaturgesetz“ (vgl. § 12 Abs. 2 SigV) herausgegeben.

1 Erzeugen und Laden der Signaturschlüssel

Die zur Erzeugung von Signaturschlüsseln erforderlichen technischen Komponenten müssen so beschaffen sein, daß

- **ein Schlüssel mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommt,**
- **aus dem öffentlichen Schlüssel nicht der private Schlüssel errechnet werden kann,**
- **die Geheimhaltung des privaten Schlüssels gewährleistet ist,**
- **der private Schlüssel nicht dupliziert werden kann und**
- **sicherheitstechnische Veränderungen an den technischen Komponenten für den Nutzer erkennbar werden**

(vgl. § 16 Abs. 1 SigV).

MK 1.1 Verwendung eines geeigneten Algorithmus und zugehöriger Parameter nach § 17 Abs. 2 SigV (s. Anlage 1) für die Schlüsselerzeugung.

MK 1.2 Verwendung eines Schlüsselgenerators, der mit an Sicherheit grenzender Wahrscheinlichkeit die Einmaligkeit der Signaturschlüssel und die vorgegebenen Parameter (z.B. Schlüssellängen) gewährleistet. Es wird empfohlen, im Zweifelsfalle eine Stellungnahme des BSI einzuholen.

MK 1.3 Erzeugung der Schlüssel

- auf dem Datenträger des privaten Signaturschlüssels (z.B. Chipkarte) selbst oder
- in einer gesonderten Schlüsselerzeugungskomponente und Laden auf den Schlüsseldatenträger in einer gesicherten Umgebung in einer Weise, daß die Geheimhaltung des privaten Signaturschlüssels gewährleistet und die Erstellung eines Duplikates (ausgenommen temporäre Zwischenspeicherungen beim Laden der Schlüssel) ausgeschlossen ist.

MK 1.4 Einsatz von Sicherheitsvorkehrungen, die sicherheitstechnische Veränderungen (d. h. Veränderungen, nach denen die erforderliche Sicherheit nicht mehr gegeben ist) für den Nutzer erkennbar machen (z.B. durch äußere Beschädigung oder Funktionsausfall). Soweit die sicherheitstechnische Veränderung nicht unmittelbar erkennbar ist, muß sie zumindest mittelbar (z.B. durch Anwendung bestimmter Prüfverfahren) erkennbar sein.

2 Speichern und Anwenden des privaten Signaturschlüssels

Die zur Erzeugung oder Prüfung digitaler Signaturen erforderlichen technischen Komponenten müssen so beschaffen sein, daß

- **aus der Signatur nicht der private Signaturschlüssel errechnet oder die Signatur auf andere Weise gefälscht werden kann,**
- **der private Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen angewendet werden kann und bei der Anwendung nicht preisgegeben wird; zur Identifikation des Signatur-**

schlüssel-Inhabers können zusätzlich biometrische Merkmale genutzt werden,

- **die Identifikationsdaten nicht preisgegeben und diese nur auf dem Datenträger mit dem privaten Signaturschlüssel gespeichert werden und**
- **sicherheitstechnische Veränderungen an den technischen Komponenten für den Nutzer erkennbar werden**

(vgl. § 16 Abs. 2 SigV).

MK 2.1 Verwendung eines geeigneten Algorithmus und zugehöriger Parameter nach § 17 Abs. 2 SigV für das Hashen zu signierender Daten.

MK 2.2 Verwendung eines geeigneten Algorithmus und zugehöriger Parameter nach § 17 Abs. 2 SigV für das Erzeugen digitaler Signaturen (zum „Signieren„ der Hash-Werte).

MK 2.3 Einsatz von Sicherheitsvorkehrungen, die sicherstellen, daß

- der private Signaturschlüssel erst nach Identifikation des Inhabers durch
 - * Besitz (z.B. Chipkarte) und Wissen (z.B. PIN) sowie
 - * bei Bedarf zusätzlich eines biometrischen Merkmals (z.B. Fingerstruktur)zur Anwendung freigegeben wird und
- der private Signaturschlüssel bei Anwendung den Schlüsseldatenträger nicht verläßt.

Dies kann z.B. durch ein entsprechendes Betriebssystem und entsprechende Applikationen auf einer Chipkarte erreicht werden.

MK 2.4 Einsatz von Sicherheitsvorkehrungen (insbesondere Hardware-Maßnahmen), die sicherstellen, daß der private Signaturschlüssel praktisch (d.h. mit realistischem Zeit- und Kostenaufwand) nicht aus dem Datenträger ausgelesen werden kann.

MK 2.5 Sicherung der Identifikationsdaten auf eine Weise, daß diese

- in der Erfassungseinheit,
- auf der Übertragungsstrecke und
- in der Speichereinheit

nicht preisgegeben werden. Nach Bedarf auch Schutz vor Preisgabe der Identifikationsdaten bei Eingabe (z.B. Ablesen der PIN) durch geeignete Sicherheitsvorkehrungen (z.B. Sichtschutz).

MK 2.6 Einsatz von Sicherheitsvorkehrungen analog MK 1.4.

3 Darstellen zu signierender Daten

Die zum Darstellen zu signierender Daten erforderlichen technischen Komponenten müssen so beschaffen sein, daß

- **die signierende Person die Daten, auf die sich die Signatur erstrecken soll, eindeutig bestimmen kann,**
 - **eine digitale Signatur nur auf Veranlassung der signierenden Person erfolgt,**
 - **die Erzeugung einer digitalen Signatur der signierenden Person vorher eindeutig angezeigt wird,**
 - **die signierende Person nach Bedarf den Inhalt der zu signierenden Daten eindeutig erkennen kann und**
 - **sicherheitstechnische Veränderungen an den technischen Komponenten für den Nutzer erkennbar werden**
- (vgl. § 16 Abs. 3 Satz 1, 4 und 6 SigV).**

MK 3.1 Anzeige von Informationen (z.B. Dateiname, Ersteller usw.), durch die die Daten, die signiert werden sollen, eindeutig bestimmt werden.

MK 3.2 Sicherstellung, daß

- nach Identifikation des Signaturschlüssel-Inhabers und Freigabe des privaten Signaturschlüssels zur Anwendung (s. MK 2.3) nicht eine digitale Signatur erzeugt werden kann, ohne daß diese vom Signaturschlüssel-Inhaber veranlaßt wird, und
- nur die vom Signaturschlüssel-Inhaber bestimmten Daten signiert werden.

MK 3.3 Eindeutige vorherige Anzeige, daß (bei Auslösung einer bestimmten Funktion) zu den angezeigten Daten eine digitale Signatur erzeugt wird (z.B. durch einen deutlichen Warnhinweis auf dem Bildschirm).

MK 3.4 Einsatz von Sicherheitsvorkehrungen, die sicherstellen, daß die angezeigten und signierten Daten übereinstimmen.

MK 3.5 Nach Bedarf Einsatz von Sicherheitsvorkehrungen, die es der signierenden Person ermöglichen, den Inhalt der zu signierenden Daten eindeutig zu erkennen (z.B. durch Darstellung des Inhalts auf dem Bildschirm oder durch Ausdruck).

MK 3.6 Einsatz von Sicherheitsvorkehrungen analog MK 1.4.

4 Prüfen einer digitalen Signatur

Die zum Prüfen signierter Daten erforderlichen technischen Komponenten müssen so beschaffen sein, daß

- **die prüfende Person die Daten, auf die sich die digitale Signatur erstreckt, sowie den Signaturschlüssel-Inhaber eindeutig feststellen kann,**
- **die Korrektheit der digitalen Signatur zuverlässig geprüft und der prüfenden Person zutreffend angezeigt wird,**
- **die prüfende Person nach Bedarf den Inhalt der signierten Daten eindeutig erkennen kann und**
- **sicherheitstechnische Veränderungen an den technischen Komponenten für den Nutzer erkennbar werden**

(vgl. § 16 Abs. 3 Satz 2, 4 und 6).

MK 4.1 Anzeige von Informationen (z.B. Dateiname, Ersteller usw.), durch die die signierten Daten, die geprüft werden sollen, eindeutig festgestellt werden können.

MK 4.2 Zuverlässige technische Prüfung der digitalen Signatur der angezeigten signierten Daten und zuverlässige Anzeige des Prüfergebnisses (z.B. „Signatur ok“ oder „Signatur nicht ok“). Zur Überprüfung der für die digitale Signatur relevanten Zertifikate s. MK 5.1 ff..

MK 4.3 Nach Bedarf Einsatz von Sicherheitsvorkehrungen, die es der prüfenden Person ermöglichen, den Inhalt der signierten Daten eindeutig zu

erkennen (z.B. durch Darstellung des Inhalts auf dem Bildschirm oder durch Ausdruck).

MK 4.4 Einsatz von Sicherheitsvorkehrungen analog MK 1.4.

5 Nachprüfen von Zertifikaten

Die technischen Komponenten zum Nachprüfen von Zertifikaten müssen eindeutig erkennen lassen, ob die nachgeprüften Zertifikate im Verzeichnis der Zertifikate zu einem angegebenen Zeitpunkt

- **vorhanden und**
- **nicht gesperrt**

waren. Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden (vgl. § 16 Abs. 3 Satz 3 und 6 SigV).

Die technischen Komponenten, mit denen Zertifikate nachprüfbar gehalten werden, müssen so beschaffen sein, daß

- **nur befugte Personen Eintragungen und Veränderungen vornehmen können,**
- **die Sperrung eines Zertifikates nicht unbemerkt rückgängig gemacht werden kann,**
- **die Auskünfte auf ihre Echtheit überprüft werden können,**
- **die Auskünfte beinhalten, ob die nachgeprüften Zertifikate im Verzeichnis der Zertifikate zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren,**
- **nur nachprüfbar gehaltene Zertifikate nicht öffentlich abrufbar sind und**
- **sicherheitstechnische Veränderungen an den technischen Komponenten für den Betreiber erkennbar werden**

(vgl. § 16 Abs. 4 SigV).

Technische Komponenten bei den Nutzern

MK 5.1 Technische Durchführung der Nachfragen der Nutzer bei Zertifikatsverzeichnissen zwecks Nachprüfung, ob Zertifikate zu einem angegebenen Zeitpunkt vorhanden und nicht gesperrt waren, und zuverlässige

Anzeige der Prüfergebnisse (z.B. durch Bildschirmanzeige „Zertifikat Nr. am(Datum) vorhanden und nicht gesperrt“).

Bei entsprechender Prüfvorgabe s. MK 4.2 zusätzlich

- automatische Überprüfung und Anzeige, ob der Gültigkeitszeitraum des Zertifikates (vgl. § 7 Abs. 1 Nr. 5 SigG) zum angegebenen Zeitpunkt begonnen hatte und noch nicht abgelaufen war, und
- Einbeziehung übergeordneter Zertifikate in die Nachprüfung und Überprüfung des Gültigkeitszeitraumes (je nach „Gültigkeitsmodell“ müssen auch die übergeordneten Zertifikate zum Zeitpunkt, zu dem die aktuell zu überprüfende Signatur erzeugt wurde, gültig gewesen sein oder zumindest zu dem Zeitpunkt, zu dem das jeweils nachgeordnete Zertifikat signiert wurde).

Das Ergebnis einer entsprechenden vollständigen Nachprüfung kann z.B. lauten „Zertifikat ok“ oder „Zertifikat ab (Datum, Uhrzeit) gesperrt“.

MK 5.2 Einsatz von Sicherheitsvorkehrungen analog MK 1.4.

Technische Komponenten bei den Zertifizierungsstellen

MK 5.3 Einsatz von Sicherheitsvorkehrungen, die sicherstellen, daß nur befugte Personen Eintragungen und Veränderungen im Zertifikatsverzeichnis vornehmen können (z.B. sichere Identifikation der befugten Personen und zuverlässige Zugangs-/Zugriffskontrolle).

MK 5.4 Einsatz von Sicherheitsvorkehrungen, die sicherstellen, daß die Sperrung eines Zertifikates nicht unbemerkt rückgängig gemacht werden kann (z.B. revisionssichere Protokollierung).

MK 5.5 Zuverlässige Nachprüfung von Zertifikaten auf entsprechende Anfrage (s. MK 5.1) und Erteilung zuverlässiger Auskünfte mit digitaler Signatur.

MK 5.6 Verwendung technischer Komponenten für die Erzeugung der digitalen Signaturen, die den Anforderungen in den Abschnitten 1 bis 3 entsprechen.

MK 5.7 Einsatz von Sicherheitsvorkehrungen, die sicherstellen, daß

- Zertifikate, die nur öffentlich nachprüfbar sein sollen, im Zertifikatsverzeichnis nicht öffentlich abgerufen werden können und
- interne Zugriffe (z.B. für Revisionszwecke) nur befugten Personen möglich sind (s. MK 5.3) und protokolliert werden.

MK 5.8 Einsatz von Sicherheitsvorkehrungen analog MK 1.4, die sicherheitstechnische Veränderungen für den Betreiber erkennbar machen.

MK 5.9 Sicherstellung einer Leistungsfähigkeit, die im Regelfalle unververtretbare Wartezeiten bei Auskünften ausschließt (vgl. § 5 Abs. 1 SigG).

6 Vergabe von Zeitstempeln

Die technischen Komponenten, mit denen Zeitstempel nach § 9 des Signaturgesetzes erzeugt werden, müssen so beschaffen sein, daß

- **die zum Zeitpunkt der Erzeugung des Zeitstempels gültige gesetzliche Zeit unverfälscht in diesen aufgenommen wird und**
 - **sicherheitstechnische Veränderungen an den technischen Komponenten für den Betreiber erkennbar werden**
- (vgl. § 16 Abs. 5 SigV).**

MK 6.1 Verwendung der von der Physikalisch-technischen Bundesanstalt (PTB) bereitgestellten Standardzeit für den Zeitstempeldienst.

MK 6.2 Einsatz von Sicherheitsvorkehrungen, die sicherstellen, daß

- die zum Zeitpunkt der Erzeugung des Zeitstempels gültige gesetzliche Zeit unverfälscht den für einen Zeitstempel bestimmten Daten hinzugefügt wird und
- diese Daten zu diesem Zeitpunkt zusammen und unverändert eine digitale Signatur erhalten.

MK 6.3 Verwendung technischer Komponenten für die Erzeugung der digitalen Signaturen, die den Anforderungen in den Abschnitten 1 bis 3 entsprechen.

MK 6.4 Einsatz von Sicherheitsvorkehrungen analog MK 1.4.

M 6.5 Sicherstellung einer Leistungsfähigkeit, die im Regelfalle unvertretbare Wartezeiten bei der Ausstellung eines Zeitstempels ausschließt.

7 Technische Komponenten, die geschäftsmäßig Dritten zur Nutzung angeboten werden

Werden technische Komponenten zum Darstellen zu signierender Daten (s. Kapitel 3), Prüfen einer digitalen Signatur (s. Kapitel 4) oder Nachprüfen von Zertifikaten (s. Kapitel 5) geschäftsmäßig Dritten zur Nutzung angeboten, müssen diese so beschaffen sein, daß

- **die eindeutige Interpretation der Daten sichergestellt ist,**
- **die technischen Komponenten bei Benutzung automatisch auf ihre Echtheit überprüft werden und**
- **sicherheitstechnische Veränderungen an den technischen Komponenten für den Nutzer erkennbar werden**

(vgl. § 16 Abs. 3 Satz 5 und 6).

MK 7.1 Einsatz von Informationstechnik, die eine eindeutige Interpretation zu signierender und signierter Daten sicherstellt.

MK 7.2 Anwendung eines Authentisierungsverfahrens, das dem Nutzer der technischen Komponente unmittelbar anzeigt, ob

- diese authentisch ist und
- keine sicherheitstechnischen Veränderungen (s. MK 1.4) erfolgt sind.

Dies kann über ein hardware-geschütztes Sicherheitsmodul erreicht werden, bei dem

- eine auf die eingesetzten Signierkomponenten (z.B. Chipkarten) abgestimmte Authentisierung (z.B. über asymmetrische Schlüssel und gesonderte Signaturschlüssel-Zertifikate für die technischen Komponenten) erfolgt,
- der geheime Schlüssel im Sicherheitsmodul gelöscht wird, wenn - etwas in Folge einer Manipulation - eine sicherheitstechnische Veränderung erfolgt,
- ein nur dem Nutzer bekanntes Codewort angezeigt wird, wenn die Authentisierung positiv abgeschlossen wird.

Ergänzende Hinweise

1 Geeignete Algorithmen und zugehörige Parameter

Die nach § 17 Abs. 2 SigV geeigneten Algorithmen und zugehörigen Parameter werden im Bundesanzeiger veröffentlicht (s. Bundesanzeiger vom 14. Februar 1998, S. 1787). Sie können auch unter der nachstehenden elektronischen Adresse der RegTP aktuell abgerufen werden.

2 Technische Interoperabilität

Aus Gründen der Interoperabilität sollten bei technischen Komponenten folgende Normen beachtet werden:

- DIN-Spezifikation der Schnittstelle zu Chipkarten mit Digitaler Signatur-Anwendung/-Funktion nach SigG und SigV (DIN - 17.4),
- X.509.

Informationen zu weiteren Normen/Standards und Spezifikationen zum Zwecke der technischen Interoperabilität können unter den nachstehenden elektronischen Adressen der Reg TP oder des BSI aktuell abgerufen werden.

3 Prüfung der technischen Komponenten

3.1 Anerkannte Prüf- und Bestätigungsstellen

Die von der RegTP anerkannten Bestätigungsstellen für die Sicherheit technischer Komponenten (vgl. § 14 Abs. 4 SigG) werden im Bundesanzeiger bekanntgegeben (s. Bundesanzeiger vom 14. Februar 1998, S. 1787). Diese und die akkreditierten Prüfstellen können auch unter der nachstehenden elektronischen Adresse der RegTP aktuell abgerufen werden.

3.2 Vorgeschriebene Prüfstufen

Eine Übersicht über die nach § 17 Abs. 2 SigV vorgeschriebenen Prüfstufen für die verschiedenen technischen Komponenten enthält Anlage 2.

3.3 Übersicht über geeignete technische Komponenten

Eine Übersicht über die geprüften technischen Komponenten, für die eine Bestätigung gemäß § 14 Abs. 4 SigG vorliegt, daß sie den Sicherheitsanforderungen des Signaturgesetzes entsprechen, kann unter der nachstehenden elektronischen Adresse der RegTP abgerufen werden.

4 Adressen

Unter folgenden Adressen können zusätzliche Informationen (z.B. vorhandene Signaturanwendungen und weitere Adressen) abgerufen werden:

- Regulierungsbehörde für Telekommunikation und Post
Postfach 80 01
55003 Mainz
Telefon: 0 61 31/18-22 10 oder 18-0 (Zentrale)
Fax: 0 61 31/18-56 18
www.regtp.de
- Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Telefon: 0 2 28/96 82-0 (Zentrale)
Fax: 0 2 28/95 82-400
<http://www.bsi.bund.de>

Prüfung der technischen Komponenten

Evaluierungsstufen

Die Prüfungs- bzw. Evaluierungsstufen der technischen Komponenten bestimmen sich wie folgt nach den damit realisierten Funktionen:

- | | | |
|----|---|------------|
| 1. | Erzeugen von Signaturschlüsseln und Laden privater Signaturschlüssel (mit geeigneten Algorithmen und dazugehörigen Parameter nach § 17 Abs. 2 SigV) | E 4 |
| 2. | Speichern und Anwenden des privaten Signaturschlüssels (Anwendung mit geeigneten Algorithmen und dazugehörigen Parametern nach § 17 Abs. 2 SigV) | E 4 |
| 3. | Erfassen, Speichern und Anwenden der Identifikationsdaten | E 2 |
| 4. | Bestimmen und Hashen (mit geeigneten Algorithmen und dazugehörigen Parameter nach § 17 Abs. 2 SigV) zu signierender Daten | E 2 |
| 5. | Erkennbarmachen des Inhalts zu signierender Daten | E 2 |
| 6. | Prüfen einer digitalen Signatur (Verifizieren der Signaturdaten und Anzeigen des Ergebnisses) | E 2 |
| 7. | Nachprüfen von Zertifikaten (mit Anfrage und Auskunft beim Verzeichnisdienst); Hinweis: für das Anwenden privater Signaturschlüssel zum Signieren von Sperrlisten und Auskünften ist E 4 erforderlich | E 2 |
| 8. | Vergabe eines Zeitstempels (Übermittlung der Daten und Zuordnung der gesetzlichen Zeit durch einen Zeitstempeldienst); Hinweis: für das Anwenden privater Signaturschlüssel zum Signieren der Daten ist E 4 erforderlich | E 2 |
| 9. | Technische Komponenten zur geschäftsmäßigen Nutzung durch Dritte
(dies betrifft die Funktionen Nr. 3 bis 6 sowie die nutzerseitigen Anteile der Funktionen 7 und 8) ¹⁾ | E 4 |

Stärke der Sicherheitsmechanismen

Die Stärke der Sicherheitsmechanismen muß in allen Fällen mit „hoch„ bewertet sein.

¹⁾ Realisiert sind die Funktionen i.d.R. in einem gesonderten Terminal, das geschäftsmäßig Dritten für die Anwendung ihrer Signierkomponenten (z.B. Chipkarten) angeboten wird.

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
MK	<u>M</u> aßnahme zur Erfüllung der Vorgaben aus Signaturgesetz und Signaturverordnung bei technischen <u>K</u> omponenten
RegTP	Regulierungsbehörde für Telekommunikation und Post
SigG	Gesetz zur digitalen Signatur (Signaturgesetz)
SigV	Verordnung zur digitalen Signatur (Signaturverordnung)