

Maßnahmenkatalog für Zertifizierungsstellen 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 Zertifikatsanträge und Identifikation der Antragsteller
- 2 Unterrichtung der Antragsteller
- 3 Bereitstellung von Signaturschlüsseln und Identifikationsdaten
 - 3.1 Bereitstellung durch die Zertifizierungsstelle
 - 3.2 Bereitstellung durch den Signaturschlüssel-Inhaber
- 4 Ausstellung von Zertifikaten
 - 4.1 Allgemeines Verfahren
 - 4.2 Inhalt von Zertifikaten
 - 4.3 Aufnahme von Vertretungsrechten oder Zulassungen in ein Zertifikat
 - 4.4 Gültigkeitsdauer von Zertifikaten
- 5 Öffentliche Verzeichnisse von Zertifikaten
- 6 Sperrung von Zertifikaten
- 7 Vergabe von Zeitstempeln
- 8 Datenschutz
- 9 Infrastruktur
 - 9.1 Personal
 - 9.2 Technische Komponenten
- 10 Sicherheitskonzept
- 11 Sicherheitsbestätigungen und Kontrollen
- 12 Dokumentation

Anlagen: 1 Ergänzende Hinweise
2 Abkürzungsverzeichnis

Aufgrund des § 12 Abs. 2 der Signaturverordnung vom 22. Oktober 1997 (BGBl I S. 2498) gibt die Regulierungsbehörde für Telekommunikation und Post erstmals den nachstehenden „Maßnahmenkatalog für Zertifizierungsstellen nach dem Signaturgesetz“, heraus. Er richtet sich an die Betreiber von Zertifizierungsstellen, die den Anforderungen des Signaturgesetzes (BGBl I S. 1870) und der Signaturverordnung entsprechen wollen, sowie an die Prüf- und Bestätigungsstellen nach § 4 Abs. 3 Satz 3 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 Zertifizierungsstellen 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 technische Komponenten nach dem Signaturgesetz“, (vgl. § 16 Abs. 6 SigV) herausgegeben.

1 Zertifikatsanträge und Identifikation der Antragsteller

Die Zertifizierungsstelle hat Personen, die ein Zertifikat beantragen, zuverlässig zu identifizieren (vgl. § 5 Abs. 1 SigG).

Die Zertifizierungsstelle hat die Identifikation des Antragstellers

- **anhand des Bundespersonalausweises oder Reisepasses oder**
- **auf andere geeignete Weise**

vorzunehmen. Der Antrag auf ein Zertifikat muß eigenhändig unterschrieben sein. Soweit ein Antrag auf ein Zertifikat mit einer digitalen Signatur des Antragstellers versehen ist, kann die Zertifizierungsstelle

von einer erneuten Identifikation und eigenhändigen Unterschrift absehen (vgl. § 3 Abs. 1 SigV).

MZ 1.1 Ausfüllen eines Antragsformulars auf Ausstellung eines Zertifikates durch den Antragsteller, das insbesondere folgendes enthält:

- Name und Adresse des Antragstellers sowie die Nummer des vorgelegten Ausweises oder Referenzdaten auf einen anderen Identitätsnachweis,
- Angaben, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen beschränkt werden soll (vgl. § 7 Abs. 1 Nr. 7 SigG) und ggf. Bezeichnung von Art und Umfang der Beschränkung (z.B. Geldtransaktionen nur bis 1.000,- DM/ Tag über die Bank „x,,)

sowie

- bei Bedarf Angaben, inwieweit
 - * eine Vertretungsmacht für Dritte,
 - * eine berufsrechtliche oder sonstige Zulassung oder
 - * sonstige Angaben

in das Zertifikat aufgenommen werden sollen.

MZ 1.2 Prüfung des vom Antragsteller vorgelegten Ausweises auf Echtheit und Unverfälschtheit.

MZ 1.3 Vergleich

- des Lichtbildes im Ausweis mit dem Antragsteller und
- der Unterschrift im Ausweis mit der Unterschrift auf dem Antrag, die bei der Zertifizierungsstelle erfolgt sein soll.

MZ 1.4 Fertigung einer Ablichtung vom vorgelegten Ausweis.

MZ 1.5 Bei Personen, die keine vergleichbar sicheren Ausweispapiere vorlegen können, sowie bei Zweifel an der Echtheit von Ausweisen oder der Identität einer Person Einschaltung der zuständigen Behörden oder eines Notars zur Feststellung der Identität. Um möglichen Fälschungen vorzubeugen, sollte eine behördliche oder notarielle Identitätsbescheinigung der Zertifizierungsstelle unmittelbar zugestellt werden (möglichst elektronisch mit digitaler Signatur).

MZ 1.6 Bei Aufnahme

- einer Vertretungsmacht für Dritte,
- einer berufsrechtlichen oder sonstigen Zulassung oder
- sonstiger Angaben

in ein Zertifikat Überprüfung der Angaben (s. auch MZ 4.5 ff).

MZ 1.7 Aufnahme

- des vom Antragstellers unterschriebenen Zertifikatantrages und
- der Ablichtung des vom Antragstellers vorgelegten Ausweises oder eines anderen Identitätsnachweises (s. MZ 1.5) in die Dokumentation (s. MZ 12.1).

MZ 1.8 Überprüfung der digitalen Signatur von (weiteren) Zertifikatsanträgen, die auf elektronischem Wege gestellt werden.

Wird das Signaturschlüssel-Zertifikat nach Eingang des elektronischen Zertifikatsantrages gesperrt, muß gegebenenfalls in geeigneter Weise eine Rückfrage erfolgen, da Unbefugte nach Entwendung eines Signaturschlüssel-Datenträgers unter dessen mißbräuchlicher Nutzung ein neues Signaturschlüssel-Zertifikat beantragt haben könnten, bevor das bestehende Zertifikat gesperrt wurde.

2 Unterrichtung der Antragsteller

Die Zertifizierungsstelle hat Personen, die ein Zertifikat beantragen, zu unterrichten

- **über die Maßnahmen, die erforderlich sind, um zu sicheren digitalen Signaturen und deren zuverlässiger Prüfung beizutragen,**
- **welche technischen Komponenten die Anforderungen nach dem Signaturgesetz und der Signaturverordnung erfüllen,**

- über die Zuordnung der mit einem privaten Signaturschlüssel erzeugten digitalen Signaturen und
 - daß Daten mit digitaler Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird
- (vgl. § 6 SigG).

Die Zertifizierungsstelle hat einen Antragsteller insbesondere über folgende erforderliche Maßnahmen zur Gewährleistung der Sicherheit der digitalen Signatur zu unterrichten:

1. Der Datenträger mit dem privaten Signaturschlüssel ist in persönlichem Gewahrsam zu halten. Bei dessen Verlust ist unverzüglich die Sperrung des Signaturschlüssel-Zertifikates zu veranlassen. Wird der Datenträger mit dem privaten Signaturschlüssel nicht mehr benötigt, ist er unbrauchbar zu machen und die Sperrung des Signaturschlüssel-Zertifikates zu veranlassen, falls es nicht abgelaufen ist.
2. Persönliche Identifikationsnummern oder andere Daten zur Identifikation gegenüber dem Datenträger mit dem privaten Signaturschlüssel sind geheim zu halten. Bei Preisgabe oder Verdacht der Preisgabe dieser Identifikationsdaten ist unverzüglich deren Änderung vorzunehmen.
3. Für die Erzeugung und Prüfung digitaler Signaturen sowie die Darstellung von zu signierenden oder zu prüfenden signierten Daten sind technische Komponenten einzusetzen, die den Anforderungen des Signaturgesetzes und der Signaturverordnung entsprechen und deren Sicherheit nach dem Signaturgesetz und der Signaturverordnung bestätigt wurde. Sie sind vor unbefugtem Zugriff zu schützen.
4. Soweit ein Zertifikat Beschränkungen nach § 7 Abs. 1 Nr. 7 des Signaturgesetzes oder Angaben nach § 7 Abs. 2 des Signaturgesetzes enthält und dies für die Aussage von signierten Daten von Bedeutung ist, ist das Zertifikat den Daten beizufügen und in die digitale Signatur einzuschließen.

- 5. Soweit für die Verwendung signierter Daten ein Zeitpunkt von erheblicher Bedeutung sein kann, ist ein Zeitstempel anzubringen.**
- 6. Werden Daten über längere Zeit in signierter Form benötigt, ist gemäß § 18 erneut eine digitale Signatur anzubringen.**
- 7. Bei der Prüfung digitaler Signaturen ist festzustellen, ob das Signaturschlüssel-Zertifikat und Attribut-Zertifikate zum Zeitpunkt der Signaturerzeugung gültig waren, das Signaturschlüssel-Zertifikat gemäß § 7 Abs. 1 Nr. 7 des Signaturgesetzes Beschränkungen enthält und gegebenenfalls die Nummern 4 und 5 beachtet wurden.**

Soweit ein Antragsteller bereits über ein Zertifikat verfügt, kann eine erneute Unterrichtung unterbleiben (vgl. § 4 SigV).

MZ 2.1 Unterrichtung des Antragstellers über die Inhalte von § 4 Nr. 1 bis 7 SigV durch

- persönliche Erläuterung oder ein entsprechendes Video und
- Überlassung geeigneter Unterlagen (z.B. Broschüre oder Diskette), die es dem Antragsteller ermöglichen, sich auch später bei Bedarf über die seinerseits erforderlichen Maßnahmen zur Gewährleistung der Sicherheit digitaler Signaturen zu unterrichten.

Zusätzlich sollten dem Antragsteller Adressen bekanntgegeben werden, unter denen er bei Bedarf Auskunft zu speziellen technischen oder rechtlichen Fragen zur digitalen Signatur erhalten kann.

MZ 2.2 Übergabe einer aktuellen Liste der technischen Komponenten, für die eine Sicherheitsbestätigung nach § 14 Abs. 4 SigG vorliegt, sowie Bekanntgabe einer elektronischen Adresse, bei der die Liste auch später aktuell abgerufen werden kann.

Der Antragsteller sollte dabei auch darauf hingewiesen werden, welche Risiken bestehen, wenn er nicht geeignete technische Komponenten einsetzt, indem z.B. durch Hacker oder "trojanische Pferde,,

- fremde Daten zur digitalen Signatur untergeschoben oder
- die zum Signieren bestimmten Daten auf dem Weg zum Signieren verändert werden können.

MZ 2.3 Unterrichtung des Antragstellers, daß alle mit seinem privaten Signaturschlüssel erzeugten digitalen Signaturen ihm grundsätzlich zugeordnet werden, soweit

- das Signaturschlüssel-Zertifikat zum Zeitpunkt der Erzeugung der digitalen Signatur gültig war und
- die Vermutung, daß die digitalen Signaturen von ihm willentlich erzeugt wurden, nicht durch andere Fakten widerlegt werden kann.

MZ 2.4 Erstellung eines Nachweises über die Unterrichtung (mit Angaben über Art und Umfang), der vom Antragsteller unterschrieben oder digital signiert und in die Dokumentation (s. MZ 12.1) aufgenommen wird.

MZ 2.5 Bei online ausgestellten weiteren Zertifikaten Online-Unterrichtung mit digital signierter Bestätigung durch den Antragsteller, soweit nicht auf eine erneute Unterrichtung verzichtet wird.

3 Bereitstellung von Signaturschlüsseln und Identifikationsdaten

Die Zertifizierungsstelle hat Vorkehrungen zu treffen, um

- **die Geheimhaltung der privaten Signaturschlüssel zu gewährleisten und**
- **eine Speicherung privater Signaturschlüssel bei der Zertifizierung auszuschließen**

(vgl. § 5 Abs. 4 Satz 2 und 3 SigG).

3.1 Bereitstellung durch die Zertifizierungsstelle

Werden Signaturschlüssel durch die Zertifizierungsstelle bereitgestellt, so hat diese Vorkehrungen zu treffen, um eine Preisgabe von privaten Schlüsseln und eine Speicherung bei der Zertifizierungsstelle auszuschließen. Dies gilt auch für persönliche Identifikationsnummern oder andere Daten zur Identifikation des Signaturschlüssel-Inhabers gegenüber dem Datenträger mit dem privaten Signaturschlüssel (vgl. § 5 Abs. 2 SigV).

Soweit die Zertifizierungsstelle Signaturschlüssel oder Identifikationsdaten nach § 5 Abs. 2 bereitstellt, hat sie den privaten Signaturschlüssel sowie die Identifikationsdaten dem Signaturschlüssel-Inhaber persönlich zu übergeben und die Übergabe von diesem schriftlich bestätigen zu lassen, es sei denn, dieser verlangt schriftlich eine andere Übergabe. Mit Übergabe des privaten Signaturschlüssels oder Signaturschlüssel-Zertifikates hat sie auch den öffentlichen Signaturschlüssel der zuständigen Behörden zu übergeben (vgl. § 6 SigV).

3.2 Bereitstellung durch den Signaturschlüssel-Inhaber

Werden Signaturschlüssel durch den Signaturschlüssel-Inhaber erzeugt, so hat sich die Zertifizierungsstelle zu überzeugen, daß er hierfür sowie für die Speicherung und Anwendung des privaten Signaturschlüssels geeignete technische Komponenten nach dem Signaturgesetz und der Signaturverordnung einsetzt (vgl. § 5 Abs. 1 SigV).

MZ 3.1 Verwendung geeigneter technischer Komponenten (s. MZ 9.2) für das

- Erzeugen der Signaturschlüssel und
- Laden der privaten Signaturschlüssel auf den Datenträger (z.B. Chipkarte).

MZ 3.2 Verwendung geeigneter technischer Komponenten (s. MZ 9.2) für das

- Erzeugen von persönlichen Identifikationsnummern (PIN) oder anderen Daten zur Identifikation des Signaturschlüssel-Inhabers und

- Laden der PIN oder anderer Identifikationsdaten auf den Signaturschlüssel-Datenträger (z.B. Chipkarte).

MZ 3.3 Persönliche Übergabe des Datenträgers (z.B. Chipkarte) mit

- dem privaten Signaturschlüssel,
- den Identifikationsdaten und
- dem öffentlichen Signaturschlüssel der RegTP.

Zusätzlich können das Signaturschlüssel-Zertifikat und ggf. weitere Zertifikate aufgenommen werden.

MZ 3.4 Überprüfung der Datenträger mit dem privaten Signaturschlüssel (z.B. Chipkarten) anhand eines eindeutigen, unfälschbaren Identifikationsmerkmals daraufhin, daß für diese eine entsprechende Sicherheitsbestätigung nach § 14 Abs. 4 SigG vorliegt, insbesondere soweit die privaten Signaturschlüssel

- extern geladen oder
- auf dem Datenträger selbst erzeugt werden.

MZ 3.5 Strikte Sicherung der Bereiche der Zertifizierungsstelle, in denen Signaturschlüssel erzeugt und geladen werden, gegen Zutritt Unbefugter.

4 Ausstellung von Zertifikaten

4.1 Allgemeines Verfahren

Die Zertifizierungsstelle hat die Zuordnung eines öffentlichen Signaturschlüssels zu einer identifizierten Person durch ein Zertifikat zu bestätigen (vgl. § 5 Abs. 1 Satz 2 SigG).

Die Zertifizierungsstelle hat auf Verlangen eines Antragstellers im Zertifikat anstelle seines Namens ein Pseudonym aufzuführen (vgl. § 5 Abs. 3 SigG).

Die Zertifizierungsstelle hat Vorkehrungen zu treffen, damit Daten für Zertifikate nicht unbemerkt gefälscht oder verfälscht werden können. Sie hat weiter Vorkehrungen zu treffen, um die Geheimhaltung der privaten

Signatur Schlüssel zu gewährleisten. Eine Speicherung privater Signatur Schlüssel bei der Zertifizierungsstelle ist unzulässig (vgl. § 5 Abs. 4 SigG).

4.2 Inhalt von Zertifikaten

Ein Signatur Schlüssel-Zertifikat muß folgende Angaben enthalten:

- 1. den Namen des Signatur Schlüssel-Inhabers, der im Falle einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen ist, oder ein dem Signatur Schlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muß,**
- 2. den zugeordneten öffentlichen Signatur Schlüssel,**
- 3. die Bezeichnung der Algorithmen, mit denen der öffentliche Schlüssel des Signatur Schlüssel-Inhabers sowie der öffentliche Schlüssel der Zertifizierungsstelle benutzt werden kann,**
- 4. die laufende Nummer des Zertifikates,**
- 5. Beginn und Ende der Gültigkeit des Zertifikates,**
- 6. den Namen der Zertifizierungsstelle und**
- 7. Angaben, ob die Nutzung des Signatur Schlüssels auf bestimmte Anwendungen nach Art und Umfang beschränkt ist.**

Angaben zur Vertretungsmacht für eine dritte Person sowie zur beruflichen oder sonstigen Zulassung können sowohl in das Signatur Schlüssel-Zertifikat als auch in ein Attribut-Zertifikat aufgenommen werden.

Weitere Angaben darf das Signaturschlüssel-Zertifikat nur mit Einwilligung der Betroffenen enthalten (vgl. § 7 SigG).

4.3 Aufnahme von Vertretungsrechten oder Zulassungen in ein Zertifikat

Die Zertifizierungsstelle hat auf Verlangen eines Antragstellers

- **Angaben über seine Vertretungsmacht für eine dritte Person sowie**
- **zur berufsrechtlichen oder sonstigen Zulassung**

in das Signaturschlüssel-Zertifikat oder ein Attribut-Zertifikat aufnehmen, soweit ihr die Einwilligung des Dritten zur Aufnahme dieser Vertretungsmacht oder die Zulassung zuverlässig nachgewiesen wird (vgl. § 5 Abs. 2 SigG).

Sollen nach § 5 Abs. 2 des Signaturgesetzes in ein Zertifikat Angaben über die Vertretungsmacht für eine dritte Person aufgenommen werden, muß die Vertretungsmacht zuverlässig nachgewiesen sein und eine schriftliche oder mit einer digitalen Signatur versehene Einwilligung der dritten Person vorliegen. Die dritte Person ist schriftlich oder in digitaler Form mit digitaler Signatur über den Inhalt des Zertifikates zu unterrichten und auf die Möglichkeit der Sperrung nach § 9 Abs. 1 hinzuweisen. Eine berufsrechtliche oder sonstige Zulassung ist insbesondere durch Vorlage der Zulassungsurkunde nachzuweisen (vgl. § 3 Abs. 2 SigV).

4.4 Gültigkeitsdauer von Zertifikaten

Die Gültigkeitsdauer eines Zertifikates darf höchstens fünf Jahre betragen und den Zeitraum der Eignung der eingesetzten Algorithmen und zugehörigen Parameter nach § 17 Abs. 2 SigV nicht überschreiten. Die Gültigkeit eines Attribut-Zertifikates endet spätestens mit der Gültigkeit des Signaturschlüssel-Zertifikates, auf das es Bezug nimmt (vgl. § 7 SigV).

- MZ 4.1 Ausstellung von Signaturschlüssel-Zertifikaten, die
- mindestens den in § 7 Abs. 1 SigG vorgeschriebenen Inhalt aufweisen und
 - deren Gültigkeitsdauer § 7 SigV entspricht.
- MZ 4.2 Einsatz von Sicherheitsvorkehrungen, die sicherstellen, daß
- die Angaben im Zertifikatsantrag und im Zertifikat übereinstimmen (z. B. durch Datenvergleich vor Übergabe des Zertifikates) und
 - aufgrund fiktiver oder unberechtigter Anträge kein Zertifikat ausgestellt wird.
- MZ 4.3 Verwendung geeigneter technischer Komponenten (s. MZ 9.2) für die Erstellung von Zertifikaten.
- MZ 4.4 Bei Vergabe eines Pseudonyms Geheimhaltung der Identität des Signaturschlüssel-Inhabers und Übermittlung der Daten über dessen Identität an Dritte nur
- unter den in § 12 Abs. 2 SigG genannten Voraussetzungen oder
 - aufgrund eines gerichtlichen Beweiserhebungsbeschlusses.
- MZ 4.5 Vor Aufnahme von Angaben über die Vertretungsmacht für eine dritte Person in ein Zertifikat Überprüfung, ob
- eine entsprechende schriftliche oder mit einer digitalen Signatur versehene Einwilligung der dritten Person vorliegt und
 - bei einer juristischen dritten Person die handelnde natürliche Person entsprechende Vertretungsmacht besitzt.
- MZ 4.6 Unterrichtung der dritten Person über
- den Inhalt des Zertifikates und
 - die Möglichkeit, das Zertifikat nach § 9 Abs. 1 SigV jederzeit sperren zu lassen,
in schriftlicher Form oder in digitaler Form mit digitaler Signatur.
- MZ 4.7 Vor Aufnahme von berufsrechtlichen oder sonstigen Zulassungen in ein Zertifikat Überprüfung der Zulassungsurkunde auf Echtheit und Unverfälschtheit.

5 Öffentliche Verzeichnisse von Zertifikaten

Die Zertifizierungsstelle hat Signaturschlüssel-Zertifikate und Attribut-Zertifikate jederzeit für jeden über öffentlich erreichbare Telekommunikationsdienste

- **nachprüfbar und**
- **mit Zustimmung des Signaturschlüssel-Inhabers abrufbar**

zu halten (vgl. § 5 Abs. 1 SigG).

Die Zertifizierungsstelle hat die von ihr ausgestellten Zertifikate mindestens solange in einem solchen Verzeichnis zu führen, wie der im Zertifikat aufgeführte Algorithmus mit den zugehörigen Parametern nach § 17 Abs. 2 SigV als geeignet beurteilt wird. Nach Ablauf der genannten Frist hat die Zertifizierungsstelle eine Nachprüfung der Zertifikates bis zum Ablauf der in § 13 Abs. 2 SigV genannten Frist (35 Jahre) auf Antrag im Einzelfall zu ermöglichen (vgl. § 8 Abs. 1 und 3 SigV).

MZ 5.1 Führung eines Zertifikatverzeichnisses, in dem alle von der Zertifizierungsstelle ausgestellten Zertifikate, bei denen der im Zertifikat aufgeführte Algorithmus mit den zugehörigen Parametern nach § 17 Abs. 2 SigV noch als geeignet beurteilt ist, jederzeit (online „rund um die Uhr“, ohne unvertretbare Zeitverzögerung im Regelfall) nachgeprüft und, falls die Zustimmung des Signaturschlüssel-Inhabers vorliegt, abgerufen werden können.

MZ 5.2 Verwendung geeigneter technischer Komponenten (s. MZ 9.2) für das Führen eines Zertifikatsverzeichnisses und das Nachprüfen von Zertifikaten.

MZ 5.3 Aufnahme der Zertifikate, bei denen der aufgeführte Algorithmus mit den zugehörigen Parametern die Eignung verloren hat, in die Dokumentation (s. MZ 12.1) bis zum Ablauf von mindestens 35 Jahren ab dem Zeitpunkt der Ausstellung des jeweiligen Zertifikates und Durchführung einer Nachprüfung auf Antrag im Einzelfall.

MZ 5.4 Erstellung eines Notfallkonzeptes, das gewährleistet, daß auch in einem Katastrophenfall (z.B. Brand) mögliche Ausfallzeiten des Verzeichnisdienstes auf ein Minimum beschränkt bleiben.

6 Sperrung von Zertifikaten

6.1 Pflicht zur Sperrung

Die Zertifizierungsstelle hat ein Zertifikat zu sperren, wenn

- ein Signaturschlüssel-Inhaber oder sein Vertreter es verlangen,
- das Zertifikat aufgrund falscher Angaben zu § 7 SigG erwirkt wurde,
- sie ihre Tätigkeit beendet hat und diese nicht von einer anderen Zertifizierungsstelle fortgeführt wird oder
- die zuständige Behörde gemäß § 13 Abs. 5 Satz 2 SigG eine Sperrung anordnet.

Enthält ein Zertifikat Angaben einer dritten Person, so kann auch diese eine Sperrung dieses Zertifikates verlangen (vgl. § 8 Abs. 1 Satz 1 und Abs. 2 SigG).

6.2 Zeitpunkt der Sperrung

Die Sperrung muß den Zeitpunkt enthalten, von dem an sie gilt. Eine rückwirkende Sperrung ist unzulässig (vgl. § 8 Abs. 1 Satz 2 und 3 SigG).

6.3 Verfahren zur Sperrung

Die Zertifizierungsstelle hat den Signaturschlüssel-Inhabern und dritten Personen, von denen Angaben zur Vertretungsmacht in ein Zertifikat aufgenommen wurden, sowie der zuständigen Behörde eine Rufnummer bekanntzugeben, unter der diese jederzeit eine unverzügliche Sperrung der Zertifikate veranlassen können und dafür ein Authentisierungsverfahren anzubieten (vgl. § 9 Abs. 1 SigV).

Die Zertifizierungsstelle hat ein Zertifikat unter den Voraussetzungen des § 8 des Signaturgesetzes zu sperren, wenn ein mit einer digitalen Signatur versehener oder schriftlicher Antrag des Signaturschlüssel-Inhabers oder seines Vertreters oder einer berechtigten dritten Person nach Absatz 1 vorliegt oder wenn ein vereinbartes Authentisierungsverfahren angewandt wurde (vgl. § 9 Abs. 2 SigV).

MZ 6.1 Bekanntgabe einer Rufnummer (Telefonanschluß) und ggf. weiterer Telekommunikationsanschlüsse (z.B. E-Mail, Fax) an

- die Signaturschlüssel-Inhaber (bei Übergabe der Zertifikate),
- dritte Personen, deren Vertretungsrechte in ein Zertifikat aufgenommen werden (mit Ausstellung des Zertifikates) und
- die RegTP (mit Aufnahme der Tätigkeit der Zertifizierungsstelle), unter denen jederzeit („rund um die Uhr,“) unverzüglich eine Sperrung von Zertifikaten veranlaßt werden kann sowie eines Authentisierungsverfahrens für die Signaturschlüssel-Inhaber und dritte Personen.

MZ 6.2 Überprüfung von Sperranträgen, ob die Voraussetzungen für eine Sperrung vorliegen (z.B. Anwendung eines vereinbarten Authentisierungsverfahrens durch den Signaturschlüssel-Inhaber oder dessen Vertreter).

MZ 6.3 Unverzügliche Durchführung der Sperrung mit Angabe ihres Zeitpunktes (Datum und Uhrzeit), wenn die Voraussetzungen für eine Sperrung vorliegen.

MZ 6.4 Erstellung eines Notfallkonzeptes für den Fall, daß mit der Sperrung eines übergeordneten Zertifikates auch die darauf basierenden nachgeordneten Zertifikate ungültig werden (s. MK 5.1 des Maßnahmenkataloges nach § 16 Abs. 6 SigV).

7 Vergabe von Zeitstempeln

Die Zertifizierungsstelle hat digitale Daten auf Verlangen mit einem Zeitstempel zu versehen (vgl. § 9 Satz 1 SigG).

MZ 7.1 Betrieb eines Zeitstempeldienstes, der jederzeit (online „rund um die Uhr“, ohne unvermeidbare Zeitverzögerung im Regelfall) zur Verfügung steht.

MZ 7.2 Verwendung geeigneter technischer Komponenten (s. MZ 9.2) für die Erzeugung von Zeitstempeln.

MZ 7.3 Erstellung eines Notfallkonzeptes für den Fall, daß der für das Signieren von Zeitstempeln eingesetzte private Signaturschlüssel kompromittiert wird.

8 Datenschutz

Die Zertifizierungsstelle darf personenbezogene Daten nur unmittelbar beim Betroffenen selbst und nur insoweit erheben, als dies für Zwecke eines Zertifikates erforderlich ist. Eine Datenerhebung bei Dritten ist nur mit Einwilligung des Betroffenen zulässig. Für andere als die in Satz 1 genannten Zwecke dürfen die Daten nur verwendet werden, wenn dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Betroffene eingewilligt hat (vgl. § 12 Abs. 1 SigG).

Bei einem Signaturschlüssel-Inhaber mit Pseudonym hat die Zertifizierungsstelle die Daten über dessen Identität auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder des Zollkriminalamtes erforderlich ist. Die Auskünfte sind zu dokumentieren (vgl. § 12 Abs. 2 SigG).

MZ 8.1 Aufnahme der für Zwecke eines Zertifikates erforderlichen Daten (z.B. auch für Zwecke der Kostenabrechnung) in den Zertifikatsantrag, der vom Antragsteller zu unterzeichnen ist.

MZ 8.2 Einholung der Einwilligung des Betroffenen (schriftlich oder mit digitaler Signatur) für eine erforderliche Datenerhebung bei Dritten (z.B. für Zwecke der Identifikation, wenn kein geeigneter Ausweis vorgelegt werden kann).

MZ 8.3 Vor Verwendung der personenbezogenen Daten für andere Zwecke, als sie das Signaturgesetz vorsieht, Überprüfung, ob

- eine andere Rechtsvorschrift dies erlaubt oder
- der Betroffene eingewilligt hat.

MZ 8.4 Dokumentation (s. MZ 12.1) von Auskünften an die Sicherheitsbehörde mit Angabe

- der ersuchenden Behörde,
 - des Pseudonyms und der Personalien der betroffenen Person, über die Auskunft erteilt wird, sowie des Umfangs der Auskunft,
 - des Zeitpunktes der Auskunft und
 - der auskunfterteilenden Person
- mit Unterschrift oder digitaler Signatur der für die Auskunftserteilung verantwortlichen Person.

9 Infrastruktur

9.1 Personal

Die Zertifizierungsstelle hat für die Ausübung der Zertifizierungstätigkeit und die Ausstellung von Zeitstempeln zuverlässiges Personal einzusetzen (vgl. §§ 5 Abs. 5 Satz 1 und 9 Satz 2 SigG).

Die Zertifizierungsstelle hat sich von der Zuverlässigkeit von Personen, die am Zertifizierungsverfahren oder an der Ausstellung von Zeitstempeln mitwirken, zu überzeugen. Sie kann hierzu insbesondere die Vorlage eines Führungszeugnisses nach § 30 Abs. 1 des Bundeszentralregistergesetzes

verlangen. Unzuverlässige Personen sind vom Zertifizierungsverfahren und der Ausstellung von Zeitstempeln auszuschließen (vgl. § 10 SigV).

Das Personal muß über die für den Betrieb der Zertifizierungsstelle erforderlichen Kenntnisse, Erfahrungen und Fertigkeiten verfügen (vgl. § 4 Abs. 3 Satz 2 SigG).

9.2 Technische Komponenten

Die Zertifizierungsstelle hat für

- **das Bereitstellen von Signaturschlüsseln,**
- **das Erstellen von Zertifikaten,**
- **das Nachprüfen von Zertifikaten nach § 5 Abs. 1 Satz 2 und**
- **das Ausstellen von Zeitstempeln**

technische Komponenten gemäß § 14 SigG einzusetzen (vgl. § 5 Abs. 5 Satz 2, 3 und § 9 Satz 2 SigG).

Die Zertifizierungsstelle hat Vorkehrungen zu treffen, um private Signaturschlüssel und die zum Erstellen der Zertifikate und Zeitstempel sowie zum Nachprüfbarhalten der Zertifikate eingesetzten technischen Komponenten vor unbefugtem Zugriff zu schützen (vgl. § 11 SigV).

MZ 9.1 Sorgfältige Auswahl des Personals, das für die Ausübung der Zertifizierungstätigkeit oder die Ausstellung von Zeitstempeln eingesetzt werden soll, im Hinblick auf dessen

- Zuverlässigkeit (unter Beiziehung eines Führungszeugnisses nach § 30 Abs. 1 Bundeszentralregistergesetz) und Ausschluß unzuverlässiger Personen, sowie
- Fachkunde (ggf. unter Beiziehung von Zeugnissen, die die erforderlichen Kenntnisse, Erfahrungen oder Fertigkeiten nachweisen) und Ausschluß ungeeigneter Personen.

MZ 9.2 Einsatz von technischen Komponenten für die in § 5 Abs. 5 Satz 2, 3 und § 9 Satz 2 SigG genannten Aufgaben,

- für die eine Sicherheitsbestätigung nach § 14 Abs. 4 SigG vorliegt und

- die im Rahmen der in den Sicherheitsbestätigungen genannten Einsatzbedingungen eingesetzt werden.

MZ 9.3 Schutz der technischen Komponenten vor unbefugtem Zugriff durch

- Zugangskontrollen bei den Betriebsräumen und Sicherung nicht besetzter Betriebs- oder Lagerräume der technischen Komponenten vor unbemerktem Zutritt Unbefugter und
 - Transport der technischen Komponenten durch zuverlässiges Personal oder in einer Verpackung, die einen Zugriff Unbefugter auf die technischen Komponenten erkennen lässt,
- sowie Wartung und Instandsetzung der technischen Komponenten durch fachkundiges und zuverlässiges Personal.

MZ 9.4 Veranlassung einer technischen Überprüfung von technischen Komponenten, wenn ein Manipulationsverdacht vorliegt, durch das BSI oder eine andere von der RegTP anerkannte Prüfstelle.

10 Sicherheitskonzept

Die Zertifizierungsstelle hat die Maßnahmen zur Erfüllung der Sicherheitsanforderungen des Signaturgesetzes und der Signaturverordnung in einem Sicherheitskonzept aufzuzeigen (vgl. § 4 Abs. 3 Satz 3 SigG).

Das Sicherheitskonzept hat alle Sicherheitsmaßnahmen sowie insbesondere eine Übersicht über die eingesetzten technischen Komponenten und eine Darstellung der Ablauforganisation der Zertifizierungstätigkeit zu enthalten. Im Falle sicherheitserheblicher Veränderungen ist das Konzept unverzüglich anzupassen (vgl. § 12 Abs. 1 SigV).

MZ 10.1 Erstellung eines Sicherheitskonzeptes, aus dem

- alle Sicherheitsmaßnahmen,
- die eingesetzten technischen Komponenten und
- die Ablauforganisation (von der Annahme eines Zertifikatantrages über die Ausstellung eines Zertifikates bis zur Dokumentation)

hervorgehen.

MZ 10.2 Im Falle sicherheitserheblicher Veränderungen unverzügliche

- Anpassung des Sicherheitskonzeptes und
- Veranlassung einer erneuten Sicherheitsüberprüfung und -bestätigung (s. MZ 11.1 ff).

MZ 10.3 Aufnahme aller gültigen Fassungen des Sicherheitskonzeptes oder der jeweiligen Veränderungen in die Dokumentation (s. MZ 12.1).

11 Sicherheitsbestätigungen und Kontrollen

Eine von der zuständigen Behörde anerkannte Stelle hat das Sicherheitskonzept und dessen Umsetzung daraufhin zu prüfen, ob die Sicherheitsanforderungen des Signaturgesetzes und der Signaturverordnung erfüllt sind (vgl. § 4 Abs. 3 Satz 3 SigG).

Die Zertifizierungsstelle hat eine solche Prüfung

- vor Betriebsaufnahme,
- nach sicherheitserheblichen Veränderungen sowie
- regelmäßig im Abstand von zwei Jahren

zu veranlassen und der zuständigen Behörde einen Prüfbericht und eine Bestätigung darüber vorzulegen, daß sie die Vorgaben aus dem Signaturgesetz und der Signaturverordnung erfüllt (vgl. § 15 Abs. 1 SigV).

Die Zertifizierungsstelle hat daneben der zuständigen Behörde zum Zwecke von Kontrollen

- das Betreten von Geschäfts- und Betriebsräumen während der üblichen Betriebszeiten zu gestatten,
- auf Verlangen in Betracht kommende Bücher, Aufzeichnungen, Belege, Schriftstücke und sonstige Unterlagen zur Einsicht vorzulegen,
- Auskunft zu erteilen und
- erforderliche Unterstützung zu gewährleisten

(vgl. § 13 Abs. 2 Satz 1 SigG).

MZ 11.1 Veranlassung von Überprüfungen der Zertifizierungsstelle durch eine nach § 4 Abs. 3 Satz 3 SigG anerkannte Prüf- und Bestätigungsstelle in den in § 15 Abs. 1 SigV genannten Fällen.

MZ 11.2 Vorlage der Prüfberichte und der Sicherheitsbestätigungen bei der RegTP.

MZ 11.3 Aufnahme der Prüfberichte und der Sicherheitsbestätigungen in die Dokumentation (s. MZ 12.1).

MZ 11.4 Umfassende Unterstützung der RegTP bei der Durchführung von Kontrollen.

12 Dokumentation

Die Zertifizierungsstelle hat

- **die Sicherheitsmaßnahmen zur Einhaltung des Signaturgesetzes und der Signaturverordnung sowie**
- **die ausgestellten Zertifikate**

so zu dokumentieren, daß die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind (vgl. § 10 SigG).

12.1 Umfang der Dokumentation

Die Dokumentation hat sich auf

- **das Sicherheitskonzept einschließlich der Änderungen,**
- **die Prüfberichte und Bestätigungen nach § 15 Abs. 1 SigV,**
- **die vertraglichen Vereinbarungen mit den Antragstellern und**
- **die von der zuständigen Behörde erhaltenen Zertifikate**

zu erstrecken (vgl. § 13 Abs. 1 Satz 1 SigV).

Zu den eingegangenen Anträgen auf Zertifikate und Vereinbarungen mit den Antragstellern sind

- **eine Ablichtung des vorgelegten Ausweises oder eines anderen Identitätsnachweises,**
- **die für die Aufnahme von Angaben dritter Personen erforderlichen Unterlagen,**
- **die Vergabe eines Pseudonyms,**
- **der Nachweis über die vorgeschriebene Unterrichtung des Antragstellers und dritter Personen,**
- **die erteilten Zertifikate mit dem jeweiligen Zeitpunkt der Ausstellung und der Übergabe,**
- **die Sperrung von Zertifikaten und**
- **Auskünfte nach § 12 Abs. 2 SigG**

zu dokumentieren. Soweit die Zertifizierungsstelle Signaturschlüssel oder Identifikationsdaten nach § 5 Abs. 2 SigV bereitstellt, sind der Zeitpunkt der Übergabe und die Übergabebestätigung zu dokumentieren. In digitaler Form geführte Aufzeichnungen müssen digital signiert sein (vgl. § 13 Abs. 1 Satz 2, 3 und 4 SigV).

12.2 Aufbewahrungsfristen

Die Dokumentation nach Absatz 1 ist mindestens 35 Jahre ab dem Zeitpunkt der Ausstellung des Signaturschlüssel-Zertifikates aufzubewahren und so zu sichern, daß sie innerhalb dieses Zeitraumes verfügbar bleibt. Die Dokumentation von Auskünften nach § 12 Abs. 2 Satz 2 des Signaturgesetzes ist zwölf Monate aufzubewahren (vgl. § 13 Abs. 2 SigV).

MZ 12.1 Führen einer Dokumentation über die in Abschnitt 12.1 genannten Aufzeichnungen.

MZ 12.2 Sicherstellung der Verfügbarkeit der Dokumentation (d.h. auch der Lesbarkeit digitaler Dokumente) über die in Abschnitt 12.2 genannten Zeiträume.

MZ 12.3 Schutz der Dokumentation vor dem Zugriff Unbefugter.

Ergänzende Hinweise

1 Anerkannte Prüf- und Bestätigungsstellen

Die von der RegTP anerkannten Prüf- und Bestätigungsstellen für die Sicherheit von Zertifizierungsstellen (vgl. § 4 Abs. 3 Satz 3 SigG) werden im Bundesanzeiger bekanntgegeben (s. Bundesanzeiger vom 14. Februar 1998, S. 1787). Sie können auch unter der nachstehenden elektronischen Adresse der RegTP aktuell abgerufen werden.

2 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>

Abkürzungsverzeichnis

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