BSI

Spezifikation zur Entwicklung interoperabler Verfahren nach SigG / SigV Signatur-Interoperabilitätsspezifikation SigI

Gültigkeitsmodell

Version 1.1

Stand: 18. Juni 1999

Dr. Volker Hammer

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-452
Fax +49 721 6105-455

E-Mail: info@secorvo.de
http://www.secorvo.de

Inhalt

Abkürzungen und Glossar

Anker	→Sicherungsanker
ARL	Authority Revocation List; Sperrliste für Zertifizierungsinstanz-Zertifikate nach X.509
Attribut-Zertifikat	Ein Attribut-Zertifikat enthält eine Menge von Attributen, die von einer Zertifizierungsinstanz signiert werden. Ein Attribut-Zertifikat enthält allerdings keinen öffentlichen Schlüssel, wie ein →Teilnehmerzertifikat, sondern bezieht sich auf ein Teilnehmerzertifikat.
Authentikator	Als Authentikator wird ein mit dem geheimen Schlüssel des Schlüsselinhabers verschlüsselter Hash-Wert bezeichnet. Ein Authentikator ist Teil einer →digitalen Signatur.
authentische Zeitangabe	Zeitangabe, die mit der Wirklichkeit übereinstimmt, also mit Genauigkeit im Sekundenbereich den Zeitpunkt beschreibt, zu dem beispielsweise eine Signaturerzeugung stattgefunden hat (→Signaturzeitpunkt).
Bezugszertifikat	Als Bezugszertifikat wird ein Zertifikat bezeichnet, auf das sich ein Attribut-Zertifikat bezieht. Das Bezugszertifikat enthält einen öffentlichen Schlüssel, das Attribut-Zertifikat nicht.
BSI	Bundesamt für Sicherheit in der Informationstechnik
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List; Sperrliste nach X.509
CPS	Certification Practice Statement
digital signiertes Dokument	Als digital signierte Dokumente werden elektronische Dokumente bezeichnet, die mit einer digitalen Signatur versehen sind. In dieser Definition sind auch Zertifikate, Sperrlisten, Verzeichnisdienstauskünfte oder Zeitstempel als spezielle digital signierte Dokumente eingeschlossen. Zur Abgrenzung siehe →Primärdokument.
digitale Signatur	Als digitale Signatur wird der verschlüsselte Hash-Wert (→Authentikator) zu einem elektronischen Dokument gemeinsam mit den Zusatzinformationen bezeichnet, die die Prüfung des Authentikators erlauben. Solche Zusatzinformationen können beispielsweise in Form eines Zertifikats oder eines Verweises auf ein Zertifikat gegeben sein. Durch die Unterscheidung zwischen digitaler Signatur und dem Authentikator ist im Rahmen dieses Dokuments eine präzisere Beschreibung des Prüfprozesses möglich. Die Unterscheidung trägt auch der Tatsache Rechnung, daß digitale Signaturen unterschiedlich aufgebaut sein können.

explizite Informationen	Informationen, die in einem digital signierten Dokument und den zugehörigen Zertifikaten unmittelbar enthalten sind, werden als explizite Informationen bezeichnet. Zur Unterscheidung siehe auch →implizite Information.
false accept Fälle	Als "false accept Fall" wird ein Gesamtergebnis bezeichnet, das nach den Ergebnissen für die Prüfbedingungen ein digital signiertes Dokument als "technisch gültig" bewertet, obwohl es objektiv hätte abgelehnt werden müssen. Dies kann z. B. auftreten, wenn zu einem gerade gesperrten Zertifikate eine digitale Signatur im Gültigkeitszeitraum einer Sperrliste erzeugt wurde und die Prüfung erfolgt, bevor die Sperrliste aktualisiert wird.
false reject Fälle	Als "false reject Fall" wird ein Gesamtergebnis bezeichnet, das nach den Ergebnissen für die Prüfbedingungen ein digital signiertes Dokument als "technisch nicht gültig" bewertet, obwohl es objektiv hätte akzeptiert werden müssen. Dies kann z. B. auftreten, wenn zu eine (nicht SigI-konforme) Prüffunktion nach dem →Gültigkeitsmodell der Zertifizierungspfad-Gültigkeit prüft, obwohl nach der Sicherheitspolitik der Sicherungsinfrastruktur nur Zertifikat-Gültigkeit gefordert wäre..
gültige Zertifikatkette	→technisch gültige Zertifikatkette
Gültigkeitsdauer	Differenz zwischen dem Gültigkeitsbeginn und dem Gültigkeitsende eines Zertifikats.
Gültigkeitsmodelle	Für Gültigkeitsprüfungen lassen sich zwei Klassen von Akzeptanzregeln unterscheiden. Diese beiden Klassen werden hier als bezeichnet als • *Zertifizierungspfad-Gültigkeit*: Alle Zertifikate müssen zum →Signaturzeitpunkt (gleichzeitig) gültig sein. • *Zertifikat-Gültigkeit:* Die Signatur muß im Gültigkeitszeitraum des Teilnehmerzertifikats erzeugt worden sein. Der Gültigkeitsbeginn des nachgeordneten Zertifikats muß im Gültigkeitszeitraum des übergeordneten Zertifikats liegen. Die Gültigkeitszeiträume in der Zertifikatkette überlappen sich nach dieser Bedingung.
Gültigkeitspolicy	Die Menge der Annahmen und Regeln der →Gültigkeitsprüfung wird als Gültigkeitspolicy bezeichnet.
Gültigkeitsprüfung	→technische Gültigkeitsprüfung; → juristische Gültigkeitsprüfung
implizite Informationen	Informationen, die zu einem digital signierten Dokument und den zugehörigen Zertifikaten abgeleitet werden können, z. B. weil in einer Sicherungsinfrastruktur bestimmte Vorgaben als Regeln gelten oder durchgesetzt werden. Zur Unterscheidung siehe auch →explizite Information.
iVm	in Verbindung mit

juristische Gültigkeitsprüfung	Unter juristischer Gültigkeitsprüfung wird die Bewertung der Ergebnisse juristischer Prüfbedingungen für eine (digital signierte Willenserklärung) verstanden. Das Ergebnis einer juristischen Gültigkeitsprüfung kann von dem Ergebnis einer technischen Gültigkeitsprüfung abweichen, weil weitere Prüfbedingungen herangezogen und Tatbestände kontextbezogen und differenzierter geprüft werden, als dies technisch möglich ist. Beispiel: Eine digital signiertes Dokument ist im Gesamtergebnis einer technischen Signaturprüfung "technisch nicht prüfbar", wenn eine Sperrinfomation nicht vorliegt. Dennoch kann es juristisch gültig sein, wenn die Willenserklärung dem Schlüsselinhaber zuzurechnen ist.
korrespondierend	Zwei Objekte korrespondieren, z. B. digitale Signatur und öffentlicher Schlüssel oder Zeitstempel und digital signiertes Dokument, wenn die geforderte mathematische Beziehung erfüllt wird.
kp	Prüfergebnis "keine Prüfung"; die Prüfbedingung wurde durch Konfiguration nicht berücksichtigt.
mso	Prüfergebnis "mathematische Sicherheit offen"; es ist unsicher, ob die mathematische Eignung eines Algorithmus oder einer Schlüssellänge noch angenommen werden kann.
mu	Prüfergebnis "Algorithmus oder Schlüssellänge mathematisch unsicher"; Algorithmus oder Schlüssellänge ist als mathematisch unsicher eingestuft
nonce	number n once, Attribut zur Unterscheidung von Zeitstempeln.
objektiver Signaturzeitpunkt	→Signaturzeitpunkt
Primärdokument	Als Primärdokument oder Prüfobjekt erster Ordnung wird das digital signierte Dokument, bezeichnet, das der Empfänger prüfen will, z. B. eine signierte Willenserklärung. Die Bezeichnung wird verwendet, um gegenüber anderen →digital signierten Dokumenten, die ebenfalls im Rahmen eine Signaturprüfung benötigt werden, zu unterscheiden, z. B. Zertifikaten, Zeitstempeln, Sperrlisten oder Verzeichnisdienstauskünften.
Prüfobjekt erster Ordnung	Als Prüfobjekt erster Ordnung oder →Primärdokument wird die Willenserklärung des Signierenden bezeichnet.
Prüfobjekte	Als Prüfobjekte werden alle Typen von digital signierten Dokumenten bezeichnet, die in einer technischen Signaturprüfung berücksichtigt werden. Dazu zählen z. B. das Primärdokument (signierte Willenserklärung, ...) wie auch die notwendigen Zertifikate oder Verzeichnisdienstauskünfte.

Prüfobjekte dritter Ordnung	Weil Verzeichnisdienstauskünfte und Sperrlisten benötigt werden, um die technische Gültigkeit von Zertifikaten und Attribut-Zertifikaten zu bewerten, werden sie als Prüfobjekte dritter Ordnung bezeichnet.
Prüfobjekte zweiter Ordnung	Weil Zertifikate, Attribut-Zertifikate und Zeitstempel benötigt werden, um die Urheberschaft und den Signaturzeitpunkt eines Primärdokuments zu überprüfen, werden sie als Prüfobjekte zweiter Ordnung bezeichnet.
Prüfschlüssel	Als Prüfschlüssel wird der zum Prüfen eines Authentikators verwendete öffentliche Schlüssel bezeichnet.
Prüfzeitpunkt	Als Prüfzeitpunkt wird der Zeitpunkt bezeichnet, an dem die aktuelle Prüfung durchgeführt wird. Die Unterscheidung zum →Signaturzeitpunkt ist insbesondere von Bedeutung, weil im Laufe der Zeit die Sicherheit mathematischer Verfahren als unzureichend bewertet werden kann. Wenn der Prüfende sich über den Signaturzeitpunkt nicht sicher sein kann, kann er hilfsweise den Prüfzeitpunkt der ersten Prüfung als Signaturzeitpunkt annehmen.
R[x])	Regel, die im Rahmen dieser Spezifikation angenommen wird. [x] ist eine laufende Nummer im Dokument. Die Regeln bilden einerseits eine Grundlage für die Spezifikation oder Vereinfachung von Prüfbedingungen und stellen zum anderen Anforderungen an die Zertifizierungsstellen dar.
RegTP	Regulierungsbehörde für Telekommunikation und Post, Wurzel-Zertifizierungsinstanz für die Zertifizierungshierarchie nach SigI
Selbstzertifikate	Ein Selbstzertifikat liegt vor, wenn der öffentliche Schlüssel, der im Zertifikat bestätigt wird, mit dem geheimen Schlüssel korrespondiert, mit dem das Zertifikat ausgestellt wurde.
Sicherungsanker	öffentlicher Schlüssel der Wurzel-Zertifizierungsinstanz. Dieser Schlüssel liegt in der Regel in Form eines Selbstzertifikats vor (auch →Wurzelzertifikat). Der Sicherungsanker bildet bei der →technischen Gültigkeitsprüfung das Ende der →Zertifikatkette.
SigG	Signaturgesetz
SigI	Spezifikation zur Entwicklung interoperabler Verfahren nach SigG / SigV, Signatur-Interoperabilitätsspezifikation

Signaturzeitpunkt	Als Signaturzeitpunkt wird ein *angenommener* Erzeugungszeitpunkt einer digitalen Signatur bezeichnet. Der Zeitpunkt, zu dem die Signatur tatsächlich erzeugt wurde wird als objektiver Signaturzeitpunkt bezeichnet. Dieser Zeitpunkt kann von Dritten häufig nur schwer festgestellt werden. Der objektive Signaturzeitpunkt kann nur unter bestimmten Bedingungen und nur im Rahmen der technisch realisierbaren Genauigkeit durch Dritte beweissicher nachvollzogen werden, z. B. mit einer unmittelbar auf die Signaturerzeugung folgenden Zeitstempelerzeugung. Prüfende müssen in der Regel Annahmen zum Signaturzeitpunkt treffen (deshalb angenommener Erzeugungszeitpunkt). Vom Signaturzeitpunkt zu unterscheiden ist der →Prüfzeitpunkt
SigV	Signaturverordnung
Sperrinformation	Eine Sperrinformation gibt an, ob ein Zertifikat und gegebenenfalls ab welchem Zeitpunkt es als gesperrt angesehen werden muß.
Sperrzeitpunkt	Als Sperrzeitpunkt wird der Zeitpunkt bezeichnet, ab dem die Sperrung gilt. Dies ist der Zeitpunkt, den die zuständige Zertifizierungsstelle in ihrem Verzeichnis führt.
Statusprüfungen	siehe →zeitbezogene Statusprüfungen
technisch gültige Zertifikatkette	Eine Zertifikatkette, die alle Prüfbedingungen erfüllt, wird als technisch gültige Zertifikatkette bezeichnet.
technische Gültigkeit	Technische Gültigkeit ist eine Eigenschaft einer digitalen Signatur, die sich aus der Bewertung der Prüfergebnisse verschiedener Prüfbedingungen für das →Primärdokument und weiterer Prüfobjekte, z. B. der zugeordneten Zertifikatkette, ergibt.
technische Gültigkeitsprüfung	In einer technischen Gültigkeitsprüfung wird festgestellt, ob die Prüfbedingungen, die für ein digital signiertes Dokument gefordert sind, erfüllt werden.
Teilnehmerzertifikat	Zertifikat, das nach den Vorgaben des SigG für einen Teilnehmer am elektronischen Rechtsverkehr ausgestellt wurde und nicht zum Prüfen von Zertifikaten zugelassen ist. Im Kontext von SigI fallen daher auch die Zertifikate für Verzeichnisdienste, Zeitstempeldienste und Sperrlisten in die Klasse der Teilnehmerzertifikate. Siehe im Unterschied dazu →Zertifizierungsstellen-Zertifikate. Im Gegensatz zu →Attribut-Zertifikaten enthalten Teilnehmerzertifikate einen öffentlichen Schlüssel.
tg	Prüfergebnis "technisch gültig"; die Prüfbedingung ist erfüllt
tng	Prüfergebnis "technisch nicht gültig"; Prüfbedingung nicht erfüllt

tnp	Prüfergebnis "technisch nicht prüfbar"; notwendige Voraussetzungen für die Prüfung nicht gegeben (z.B. keine aktuelle Sperrliste)
Vergabekonzept für Gültigkeitszeiträume	Als Vergabekonzept für Gültigkeitszeiträume wird die Menge der Regeln bezeichnet, die bestimmen, welche Gültigkeitszeiträume eine Zertifizierungsinstanz in ein Zertifikat eintragen darf.
Verlängerungszertifikat	Von einem Verlängerungszertifikat wird gesprochen, wenn ein Zertifikat zu *einem* öffentlichen Schlüssel den folgenden Bedingungen genügt: • das Gültigkeitsende des neueren Zertifikats liegt nach dem Gültigkeitsende des ersten Zertifikats, • der Gültigkeitsbeginn des neueren Zertifikats liegt *nicht* vor dem Gültigkeitsbeginn des ersten Zertifikats, • die Seriennummern unterscheiden sich und • alle anderen Attribute sind mit identischen Werten des alten Zertifikats belegt. Die Seriennummer *muß* unterschiedlich sein, da jede Seriennummer nur ein einziges Mal von der Zertifizierungsinstanz vergeben werden darf.
Vorhandenseinsinformation	Eine Vorhandenseinsinformation gibt an, ob ein Zertifikat zu einem Zeitpunkt als vorhanden angesehen werden kann. Abweichungen zum Gültigkeitsbeginn eines Zertifikats sind möglich, wenn das Zertifikat im Rahmen organisatorischer Abläufe erst zu einem späteren Zeitpunkt "freigeschaltet" wird.
Wurzelzertifikat	Zertifikat der Wurzel-Zertifizierungsinstanz, das als Wurzel einer Zertifizierungshierarchie verwendet wird. Zertifikate, die die Wurzel-Zertifizierungsinstanz zu anderen Zwecken als zum Zertifizieren verwendet, z. B. zum Signieren von Sperrlisten oder für Zeitstempel, werden nicht als Wurzelzertifikate bezeichnet.
zeitbezogene Statusprüfungen	Unter zeitbezogenen Statusprüfungen werden die Prüfbedingungen zusammengefaßt, mit denen der Gültigkeitszeitraum, der Vorhandenseins- und der Sperrstatus eines Zertifikats geprüft wird. Als Referenzzeitpunkt für die Prüfung wird im →Gültigkeitsmodell nach SigG der Signaturzeitpunkt des Dokuments verwendet, dessen Authentikator mit dem Prüfschlüssel geprüft wird.
Zertifikat-Gültigkeit	→Gültigkeitsmodelle
Zertifizierungspfad-Gültigkeit	→Gültigkeitsmodelle

Zertifikatkette	Eine Folge von Zertifikaten [$Zert_1$] ... [$Zert_n$], für die gilt: • Authentikator des Zertifikats Z_i korrespondiert mit dem öffentlichen Schlüssel des Zertifikats [$Zert_{i-1}$] und • [$Zert_1$] ist ein Wurzelzertifikat (Sicherungsanker oder Ende der Zertifikatkette). Zwischen den Zertifikaten der Kette können weitere Konsistenzbedingungen gefordert werden, z. B. • Subject([$Zert_i$]) = Issuer([$Zert_{i+1}$])
Zertifizierungsinstanz	organisatorische Einheit, die Zertifikate ausstellt.
Zertifizierungsstelle	organisatorische Einheit, die die im Rahmen des SigG definierten Aufgaben wahrnimmt.
Zertifizierungsstellen-Zertifikate	Als Zertifizierungstellen-Zertifikate werden ausschließlich solche Zertifikate bezeichnet, deren Schlüssel zum Prüfen von Zertifikaten verwendet werden darf. Andere Zertifikate, die für Zertifizierungsstellen ausgestellt werden, z. B. nur zum Prüfen der Signaturen von Sperrlisten oder Zeitstempeln, werden in die Klasse der Teilnehmerzertifikate eingeordnet.

Notationen

Abstimmungs- und Klärungsbedarf

Für die Fertigstellung dieser Spezifikation sind noch Vorgaben anderer Dokumente aus SigI abzustimmen. Auf sie wird in diesem Dokument hingewiesen. Die entsprechenden Stellen sind in `Schreibmaschinentype` gesetzt.

Zertifizierungshierarchie und Referenzierung von Zertifikaten

Als technisch-organisatorisches Basisszenario wird eine baumartige Zertifizierungshierarchie mit drei Ebenen angenommen. Die Ebene 1 wird durch das bzw. die Selbstzertifikate der Wurzel-Zertifizierungsinstanz gebildet (auch als Wurzelzertifikate bezeichnet). Die Zertifikate, die durch die RegTP ausgestellt werden und keine Selbstzertifikate sind, bilden die Ebene 2. Teilnehmerzertifikate sind auf der Ebene 3 angesiedelt.

In dieser Zertifizierungshierarchie wird eine Zertifikatkette als Folge von Zertifikaten [$Zert_1$] ... [$Zert_n$] definiert, für die gilt: der Authentikator des Zertifikats [$Zert_i$] korrespondiert mit dem öffentlichen Schlüssel des Zertifikats [$Zert_{i-1}$] und [$Zert_1$] ist ein Wurzelzertifikat (Ebene 1).

Referenzierung von Zertifikaten und Zertifikat-Attributen

Um Angaben im Zertifikat darzustellen, wird die Schreibweise [Subject, Detail_1, ..., Detail_s] verwendet. Zur Referenzierung wird folgende Notation verwendet:

t_{sig}(Prüfobjekt)	Signaturzeitpunkt, Zeitpunkt der für die Signaturerstellung für ein digital signiertes Dokument angenommen wird. t_{sig} unterscheidet sich für die verschiedenen Prüfobjekte.

$t_{Prüf}$	Prüfzeitpunkt, Zeitpunkt, zu dem die aktuelle Signaturprüfung durchgeführt wird. $t_{Prüf}$ ist daher für alle Prüfobjekte gleich.
t_{Ref}	Referenzzeitpunkt, der für die zeitbezogenen Statusprüfungen eines Zertifikats verwendet, wird, das den Prüfschlüssel eines Prüfobjekts enthält. Als Referenzzeitpunkt wird im →Gültigkeitsmodell nach SigI immer der Signaturzeitpunkt des Prüfobjekts verwendet, dessen Authentikator mit dem Prüfschlüssel geprüft wird. Der Referenzzeitpunkt ändert sich daher für jedes Prüfobjekt. Der Begriff wird verwendet, um zwischen dem Zeitpunkt, zu dem die →zeitbezogenen Statusbedingungen für ein Zertifikat erfüllt sein müssen und dem Zeitpunkt, zu dem das Zertifikat selbst erzeugt wurde, zu unterscheiden.
$t_{StatusInfo}$	Zeitpunkt, zu dem eine Statusinformation bereitgestellt wurde.
[$Zert_{Anf}$]	Zertifikat am Anfang einer Zertifikatkette, möglich sind Zertifikate von Endteilnehmern ([$Zert_{TIn}$] oder Teilnehmerzertifikate, die für Dienste von Zertifizierungsstellen ausgestellt wurden, z. B. [$Zert_{Dir}$] oder [$Zert_{TSS}$].
[$Zert_{Attr}$]	Attributzertifikat für den Teilnehmer
[$Zert_{Dir}$]	Zertifikat zum Prüfen von OCSP-Verzeichnisdienstauskünften gemäß [BSI-DIR]. Für Sperrlisten ist eine andere Kennzeichnung vorgesehen.
[$Zert_i$, A = x]	Das Zertifikat für den Inhaber [i] enthält das Attribut [A] mit dem Wert [x].
[$Zert_{TIn}$]	Teilnehmerzertifikat, es enthält den Prüfschlüssel für das Primärdokument
[$Zert_{Ref}$]	Zertifikat, auf das im Feld **procuration** eines Attribut-Zertifikats verwiesen wird
[$Zert_{RegTP}$]	Selbstzertifikat der Wurzel-Zertifizierungsinstanz RegTP, wird nur für Wurzelzertifikate verwendet
[$Zert_{RL}$]	Zertifikat zum Prüfen von Revocation Lists
[$Zert_{TSS}$]	Zertifikat zum Prüfen von Zeitstempeln
[$Zert_{ZS}$]	Zertifikat einer Zertifizierungsstelle zum Prüfen von Zertifikaten
t_B ([$Zert_i$])	Gültigkeitsbeginn des Zertifikats für [i]
t_E ([$Zert_i$])	Gültigkeitsende des Zertifikats für [i]
t_{Sperr} ([$Zert_i$])	Sperrzeitpunkt des Zertifikats für [i]
t_{Vorh} ([$Zert_i$])	Zeitpunkt des Einstellens des Zertifikats für [i] in das Verzeichnis als vorhanden
GD_{max}	maximale Gültigkeitsdauer eines Zertifikats; ist im Rahmen des SigG auf 5 Jahre festgelegt (implizite Information)
Attribut([$Zert_i$])	liefert den Wert des durch [Attribut] bezeichneten Attributs aus dem Zertifikat.

Attribut.Teilattibut ([$Zert_i$])	liefert den Wert des durch [Teilattribut] bezeichneten Teil des [Attributs] aus dem Zertifikat.
[$Zert_x$, Attribut(e)]	Zeigt Inhalte des Zertifikats auf. z. B. steht [$Zert_{Dir}$, RegTP] für ein Zertifikat des Verzeichnisdienstes der RegTP

Geforderte und abgeleitete Voraussetzungen werden in Regeln formuliert.

Rx)	Regel mit der laufenden Nummer [x]. Die Regeln definieren Rahmenbedingungen, anhand derer Prüfbedingungen bestimmt oder vereinfacht werden können.

Konformitätsanforderungen

In Anforderungen an SigI-konforme Prüffunktionen wird der Stellenwert von Konformitätsanforderungen durch Worte verdeutlicht , die in KAPITÄLCHEN gesetzt sind. Insbesondere werden verwendet::

MUSS	Eine Prüffunktion, die die Anforderung nicht erfüllt, ist nicht SigI-konform.
SOLL	Es wird empfohlen, daß die Prüffunktion die entsprechende Anforderung unterstützt. Die Prüffunktion kann jedoch auch als SigI-konform eingeordnet werden, wenn die Anforderung nicht unterstützt wird.
KANN ANNEHMEN	Die Formulierung wird verwendet, wenn aufgrund des Sicherungskonzepts von SigG und SigI angenommen wird, daß eine Prüfbedingung erfüllt ist. Zur Vereinfachung von Implementierung und Prüfprozessen dürfen diese Annahmen in SigI-konformen Prüffunktionen verwendet werden, um das Prüfergebnis zu bestimmen. Eine Prüffunktion wird auch als SigI-konform eingeordnet, wenn sie die Annahmen nicht berücksichtigt und statt dessen die geforderte Bedingungen prüft.
KANN	Die spezifizierte Funktionalität ist für SigI-konforme Prüffunktionen hilfreich. Z. B. können sie dem Benutzer Optionen im Prüfprozeß anbieten, mit denen auf Störungssituationen beim Abruf von Statusinformationen reagiert werden kann.
MELDUNGSERGÄNZUNG	Die spezifizierten Angaben MÜSSEN von einer SigI-konformen Prüffunktion als Bestandteil des Gesamtergebnisses einer Prüfung angezeigt werden.

1 Zusammenfassung

Mit dem Signaturgesetz (SigG) sollen die Voraussetzungen für Rechtssicherheit im elektronischen Rechtsverkehr verbessert werden. Die Reihe der Signatur-Interoperabilitätsspezifikationen (SigI) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) soll in diesem Kontext erreichen, daß Kooperationspartner unterschiedliche Systeme einsetzen können und dennoch eine gleiche, mit dem SigG übereinstimmende Funktionalität erhalten.

Dieses Dokument ist ein Teildokument dieser Reihe. Es spezifiziert die Konformitätsbedingungen für technische Gültigkeitsprüfungen digital signierter Dokumente. Dazu werden die Prüftatbestände und die Prüfbedingungen festgelegt.

Außerdem werden die vom BSI im Rahmen von SigI angenommenen Voraussetzungen dargestellt. Einige dieser Voraussetzungen müssen von Zertifizierungsstellen erfüllt werden, um die technische Signaturprüfung nach SigI zu unterstützen bzw. abzusichern.

2 Gegenstand und Grundlagen der Spezifikation

2.1 Gegenstand

Das Dokument spezifiziert die technischen Anteile von Gültigkeitsprüfungen für digital signierte Dokumente auf der Basis des SigG und der weiteren Dokumente nach SigI. Gegenstand der Spezifikation sind funktionale Eigenschaften, die von SigI-konformen Prüffunktionen erfüllt werden müssen.

SigI-konforme Prüffunktionen sollen für SigI-konforme digital signierte Dokumente interoperabel sein. Zwei unterschiedliche Prüffunktionen, die konform mit dieser Spezifikation sind, müssen dazu für das gleiche digital signierte Dokument bei gleichem angenommenen Signaturzeitpunkt zum gleichen Prüfergebnis kommen. Vorausgesetzt wird dabei, daß die Prüfobjekte den Spezifikationen [BSI-ZERT], [BSI-SIG], [BSI-TSS] und [BSI-DIR] genügen, soweit Anforderungen dort zwingend vorgeschrieben werden. Dies schließt ein, daß die Signaturen mit Schlüsseln aus der Zertifizierungshierarchie der RegTP erzeugt wurden, deren Zertifikate SigI-konform ausgestellt wurden.

Mehrfachsignaturen von digitalen Dokumenten werden in diesem Teildokument von SigI nicht behandelt. Insbesondere werden die besonderen Prüfbedingungen für "erneute digitale Signaturen" nach § 16 Nr. 7 iVm § 18 SigV nicht berücksichtigt.

Die Spezifikation konzentriert sich auf die Prüfbedingungen und gibt *keinen* Vorschlag für die algorithmische Realisierung des Prüfprozesses.[1]

Interoperabilität zu anderen Sicherungsinfrastrukturen ist nicht Gegenstand dieses Teildokuments von SigI. Dies gilt auch für den Fall, daß zu anderen Sicherungsinfrastrukturen eine Crosszertifizierung aufgebaut wird.

Die Meldungen an den Benutzer werden in Dokument [BSI-AIS] spezifiziert und sind nicht Gegenstand dieses Teildokuments von SigI.

Unterrichtungspflichten nach § 6 SigG, die sich auf die Gültigkeitsprüfung beziehen, sind nicht Gegenstand dieses Teildokuments von SigI.

2.2 Rechtliche Einordnung der technischen Prüfregeln nach SigI

2.2.1 Rechtliche Verbindlichkeit der SigI Spezifikationen

Die SigI-Konformitätsspezifikation ist eine Empfehlung und für die Betreiber von Zertifizierungsinstanzen und die Teilnehmer am elektronischen Rechtsverkehr nach SigG nicht verbindlich.

1 Die möglichen Alternativen, wie top-down oder bottom-up Prüfung der Zertifikatkette, haben zwar unterschiedliche Eigenschaften für die Implementierung, dürfen sich aber nach dem Verständnis dieser Spezifikation im Prüfergebnis nicht unterscheiden. Stärker algorithmisch orientierte Vorschläge, die sich jedoch nicht unmittelbar auf SigI übertragen lassen, finden sich in [ITU-T X.509 1997] und [RFC 2459 1999]

2.2.2 Rechtliche Bewertung von Prüfergebnissen

Technische Gültigkeitsprüfungen sind in ihrem Umfang begrenzt. Automatisch können nur solche Prüfbedingungen geprüft werden, die formalisierbar sind. Darüber hinaus können dem Benutzer nur solche Informationen zur Verfügung gestellt werden, die aus dem Aufbau und Inhalt digital signierter Dokumente abgeleitet werden können. Andere Informationen, beispielsweise über einen durch Zeugen verbürgten Aufenthaltsort, ein vorgetäuschter Verlust eines Signaturschlüssels oder Fehler in den Abläufen einer Zertifizierungsstelle, können in der technischen Gültigkeitsprüfung nicht berücksichtigt werden. Solche Informationen können aber für eine juristische Bewertung von digital signierten Willenserklärungen relevant sein. Es ist deshalb möglich, daß juristische Bewertungen von digital signierten Dokumenten zu einem anderen Ergebnis kommen, als dies das Ergebnis der rein technischen Gültigkeitsprüfung nahelegt.

2.3 Grundlagen der Entwurfsentscheidungen

SigI-Spezifikationen

Ausgangspunkt für die Spezifikation sind die Vorgaben von SigG und SigV sowie die SigI-Spezifikationen [BSI-ZERT], [BSI-SIG], [BSI-TSS] und [BSI-DIR]. Das Teildokument [BSI-DIR] wurde in der Version 2 berücksichtigt. Zum Redaktionsschluß für diese Version der technischen Gültigkeitsprüfung lag bereits die Version 3 vor, die in Verzeichnisdienstauskünften (OCSP) als Information ein Freigabedatum[2] vorsieht. Diese Änderung konnte jedoch nicht mehr berücksichtigt werden. In einer künftigen Version ist zu erwarten, daß dadurch die die Prüfbedingungen für die Eignung und Verwendung von Vorhandenseinsinformationen vereinfacht werden. Soweit im Rahmen dieser Vorgaben Gestaltungsspielräume bestanden, erfolgte die Orientierung am Standard [ITU-T X.509 1997].

Sicherheitsniveau SigI-konformer Zertifizierungsstellen

Von SigI konformen Zertifizierungsstellen wird ein hohes Sicherheitsniveau gefordert. Das BSI geht davon aus, daß durch dieses Sicherheitsniveau verschiedene technisch prüfbare Anforderungen an Zertifikate von den Zertifizierungsstellen sicher durchgesetzt werden. Aus den jeweiligen Annahmen über gewährleistete Tatbestände werden Vereinfachungen für Prüftatbestände abgeleitet, um den Implementierungs- und Prüfaufwand zu verringern. Die vom BSI im Rahmen von SigI angenommenen Voraussetzungen werden in dieser Spezifikation dargestellt.

Zertifizierungsmodell

Einige Prüfbedingungen beziehen sich auf die Zertifizierungshierarchie, aus der die Zertifikate für Signaturschlüssel stammen müssen. Für dieses Dokument wird dazu ein Zertifizierungsmodell mit drei Ebenen vorausgesetzt (vgl. oben Notation). Voraussetzung für eine ordnungsgemäßes Funktionieren der Prüffunktion sind die Regeln der Namensgebung für die Inhaber von Zertifikaten, die in Kapitel 4 definiert und begründet werden.

Skalierbarkeit von Prüfumfang und Implementierungsumfang

Es liegt in der Verantwortung der Benutzer, ob sie alle in diesem Dokument geforderten Prüfbedingungen für eine technische Signaturprüfung berücksichtigen oder auf einige Prüf-

2 Datum des Eintrags eines Zertifikats in das Verzeichnis.

bedingungen verzichten (vgl. auch den Abschnitt zu Prüftiefen in [BSI-AIS, Kap. 1]). Aus einem verringerten Prüfumfang folgt allerdings die Möglichkeit eines falschen technischen Prüfergebnisses (false accept Fälle).

Der in diesem Dokument geforderte Prüfumfang muß in SigI-konformen Prüffunktionen implementiert werden. Hersteller können aber zusätzliche Prüfbedingungen realisieren, die die als erfüllt angenommenen Prüfbedingungen untersuchen. Sind solche Prüfbedingungen nicht erfüllt, SOLL die Prüffunktion den Benutzer auffordern, diesen Tatbestand der RegTP zu melden.

Hersteller können auch zusätzliche Prüftatbestände oder Prüfbedingungen berücksichtigen, die in diesem Dokument nicht angesprochen werden. Dadurch können die Prüfergebnisse im Einzelfall von denen einer Prüfung nach dieser Spezifikation abweichen. SigI-konforme Prüffunktionen MÜSSEN diese Abweichung im Prüfergebnis darstellen.

3 Grundlagen technischer Signaturprüfungen nach SigI

Im Rahmen einer technischen Signaturprüfung nach SigI müssen mehrere digital signierte Dokumente (Prüfobjekte) daraufhin untersucht werden, ob Prüfbedingungen erfüllt werden. Aus den Ergebnissen dieser Teilprüfungen wird ein Gesamtergebnis gebildet.

3.1 Prüfobjekte

3.1.1 Klassen von Prüfobjekten

Als Prüfobjekte werden digital signierte Dokumente nach SigI aufgefaßt. Es können im Kontext von SigI die folgenden Typen von digital signierten Dokument unterschieden werden:

- Primärdokumente nach [BSI-SIG].
- Zertifikate nach [BSI-ZERT]. Zertifikate können nach folgenden Typen unterschieden werden:
  - *Wurzelzertifikate:* sind die Zertifikate der Wurzel-Zertifizierungsinstanz soweit sie als Selbstzertifikate einen Sicherungsanker der Zertifizierungshierarchie bilden,
  - *Zertifizierungsstellen-Zertifikate:* sind die Zertifikate die von der RegTP für Schlüsselpaare ausgestellt werden, die zum Signieren von Zertifikaten verwendet werden dürfen.
  - *Teilnehmerzertifikate:* sind die Zertifikate für die Schlüsselpaare, die im elektronischen Rechtsverkehr eingesetzt werden. Dazu zählen auch die Zertifikate der Zertifizierungsstellen, die nicht zum Prüfen von Zertifikaten verwendet werden dürfen. Die Zertifikate für Zertifizierungsstellen (auch die RegTP), die nur zum Prüfen der Signaturen von Verzeichnisdienstauskünfte, Sperrlisten oder Zeitstempeln vorgesehen sind, werden deshalb auch als Teilnehmerzertifikate eingeordnet.
- Attribut-Zertifikate (für Teilnehmer) nach [BSI-ZERT].
- Zeitstempel nach [BSI-TSS].
- Verzeichnisdienstauskünfte nach [BSI-DIR].
- Sperrlisten nach [BSI-DIR]

Verschiedene Prüfobjekte haben eine unterschiedliche Rolle im Prüfprozeß und können danach in die folgenden drei Klassen eingeteilt werden.

Prüfobjekt erster Ordnung

Als *Primärdokument* oder *Prüfobjekt erster Ordnung* wird die signierte elektronische Willenserklärung eines Teilnehmers bezeichnet, deren technische Gültigkeit geprüft werden soll.

Prüfobjekte zweiter Ordnung

Zertifikate, Attribut-Zertifikate und Zeitstempel werden benötigt, um die Urheberschaft, Autorisierung und den Signaturzeitpunkt eines Primärdokuments zu überprüfen. Sie werden deshalb als *Prüfobjekte zweiter Ordnung* bezeichnet.

Zu den Prüfobjekten zweiter Ordnung gehören zunächst das *Teilnehmerzertifikat,* das *Zertifizierungsstellen-Zertifikat* und das Wurzelzertifikat, die die Zertifikatkette zur Signatur des Primärdokuments bilden.

Attribut-Zertifikate werden verwendet, um zusätzliche Informationen über einen Schlüsselinhaber bereitzustellen. Sie müssen sich auf das Teilnehmerzertifikat beziehen, das den Prüfschlüssel zum Primärdokument enthält.

Zeitstempel dienen dem Nachweis, daß zu einem bestimmten Zeitpunkt bestimmte Daten zur Bestätigung bei einer Zertifizierungsstelle vorgelegt wurden. Zeitstempel werden im Rahmen dieser Spezifikation nur berücksichtigt, soweit sie sich auf ein Primärdokument beziehen.

Prüfobjekte dritter Ordnung

Verzeichnisdienstauskünfte, und Sperrlisten werden benötigt, um den Vorhandenseins- und Sperrstatus von Zertifikaten und Attribut-Zertifikaten zu bewerten. Sie und die nur zu ihrer Prüfung notwendigen Zertifikatkette werden als *Prüfobjekte dritter Ordnung* bezeichnet. Diese Unterscheidung ist darin begründet, daß Prüfobjekte dritter Ordnung als zusätzliche Information zur Prüfung benötigt werden, um die Prüfobjekte zweiter Ordnung zu bewerten. Sind sie "technisch nicht gültig", dann kann nicht entschieden werden, ob das Primärdokument als "technisch gültig" zu bewerten ist, weil die notwendigen Informationen fehlen. Im Unterschied zu Prüfobjekten erster oder zweiter Ordnung tragen "technisch nicht gültige" Prüfobjekte dritter Ordnung im Gesamtergebnis daher nur mit "technisch nicht prüfbar" bei.

Verzeichnisdienstauskünfte dienen zur Bereitstellung von Informationen darüber, ob ein Zertifikat ausgestellt und gesperrt wurde (Vorhandenseinsprüfung und Sperrprüfung). Der Sperrstatus eines Zertifikats kann auch über eine *Sperrliste* festgestellt werden. Verzeichnisdienstauskünfte bieten Statusinformationen mit sehr hoher Aktualität. Sie erfordern aber im Prüfprozeß eine Telekommunikationsverbindung, um die Informationen abzufragen. Aus Sperrlisten kann der Sperrstatus dagegen off-line entnommen werden. Da Sperrlisten für einen Zeitraum gültig sind, werden die in diesem Zeitraum vorgenommenen Sperrungen von der Liste nicht erfaßt. Die Informationen aus Listen können deshalb gegenüber aktuell abgefragten Verzeichnisdienstauskünften im Laufe der Zeit zunehmend Abweichungen aufweisen. Sie können daher unter bestimmten Bedingungen das Risiko eines fehlerhaften technischen Prüfergebnisses erhöhen, wenn für die Prüfung aktuellere Daten zu berücksichtigen wären (false accept Fälle). Welche Informationsquellen für die Prüfung berücksichtigt werden sollen, liegt in der Entscheidung des Prüfenden.

Zertifikate, die nur zur Prüfung von Verzeichnisdienstauskünften und Sperrlisten benötigt werden,[3] werden ebenfalls als Prüfobjekte dritter Ordnung eingeordnet.

3.1.2 Input der Gültigkeitsprüfung

Die Prüffunktion benötigt in Abhängigkeit von der Konfiguration als Input für die Prüfung:

- das digital signierte Primärdokument,
- gegebenenfalls einen Zeitstempel zum Primärdokument,
- die im Primärdokument referenzierten Attribut-Zertifikate,
- eine Liste von Wurzelzertifikaten,
- eine Menge von Zertifikaten, aus denen sich die Zertifikatketten zum Primärdokument, zu den Attribut-Zertifikaten und den Sperr- und Verfügbarkeitsinformationen bis zu einem Zertifikat aus der Liste der Wurzelzertifikate bilden lassen, sowie

3 Je nach Zertifizierungshierarchie können in den Zertifikatketten von Verzeichnisdienstauskünften und Sperrlisten auch Zertifizierungsstellen-Zertifikate enthalten sein, die bereits für die Prüfung des Primärdokuments benötigt werden.

- Sperr- und Verfügbarkeitsinformationen zu allen Zertifikaten, soweit dies nach der Konfiguration der Prüffunktion durch den Benutzer gefordert ist.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN in der Lage sein, Zeitstempel auf Primärdokumente zu beziehen. Dazu muß die Prüffunktion erkennen, daß ein Prüfobjekt "Zeitstempel" vorliegt und daß er sich auf das Primärdokument bezieht. Außerdem muß die Prüffunktion entscheiden können, wie sich der Zeitstempel auf das Primärdokument bezieht, also auf Grund welcher Daten die mathematische Relation zu bilden ist.

SigI-konforme Prüffunktionen MÜSSEN die Möglichkeit bieten, einem Primärdokument einen Zeitstempel zuzuordnen, der als separate Datei vorliegt. Außerdem SOLLEN SigI-konforme Prüffunktionen die Dokumentstruktur nach [BSI-TSS, Kapitel 8] interpretieren und auflösen können.

Es wird davon ausgegangen, daß die notwendigen Prüfobjekte beim Aufruf der einer SigI-konformen Prüffunktion entweder bereitstehen oder die Prüffunktion in der Lage ist, sich die notwendigen Informationen zu beschaffen. Soweit erforderlich MÜSSEN SigI-konforme Prüffunktionen die nach [BSI-ZERT], [BSI-TSS] und [BSI-DIR] dargestellten Verfahren zum Abruf der notwendigen Prüfobjekte aus der Sicherungsinfrastruktur nach SigI unterstützen. Diese Spezifikation setzt außerdem voraus, daß SigI-konforme Prüffunktionen die möglichen Störfälle, die im Rahmen der Protokolle spezifiziert sind, beherrschen.[4] Solche Protokollaspekte werden in diesem Teildokument von SigI nicht behandelt.

Falls im Verlauf der Prüfung Anfragen an Zertifizierungsstellen notwendig sind, sind die in den genannten Dokumenten eingesetzten Protokolle zu verwenden. Der Einsatz der Protokolle wird in diesem Dokument nicht weiter spezifiziert. Gegenstand dieses Dokuments sind allerdings Prüfbedingungen, durch die entschieden wird, ob Prüfobjekte dritter Ordnung die Konsistenzbedingungen erfüllen, die für ihre Verwendung in einer technischen Signaturprüfung gefordert sind. Die Ergebnisse dieser Teilprüfungen können Anlaß zum Abruf von Prüfobjekten aus der Sicherungsinfrastruktur sein.

3.2 Gesamtergebnis, Prüftatbestände und Prüfbedingungen

Der Empfänger eines digital signierten Dokuments muß prüfen und bewerten können, ob ein digital signiertes Dokument nicht verändert wurde (Unverfälschtheit), von wem es signiert wurde (Urheberschaft) und ob es für einen Anwendungszweck ausreichend autorisiert wurde (Autorisierung). Das Gesamtergebnis und die Teilergebnisse einer technischen Signaturprüfung geben dem Benutzer die Informationen, mit denen er entscheiden kann, ob und wie diese Prüfziele durch technische Maßnahmen für seinen spezifischen Kontext erfüllt sind.

Um das Gesamtergebnis einer technischen Signaturprüfung für ein digital signiertes Dokument zu bestimmen, sind eine Reihe von Fragestellungen zu überprüfen. Diese Fragestellungen strukturieren die technische Signaturprüfung inhaltlich und werden in dieser Spezifikation als *Prüftatbestände* bezeichnet. Für jeden Prüftatbestand werden eine oder mehrere *Prüfbedingungen* angegeben, mit denen der Beitrag des Prüftatbestandes zum Gesamtergebnis definiert wird. Prüfbedingungen sind in der Regel so formuliert, daß technisch entschieden werden kann, ob sie erfüllt oder nicht erfüllt sind.

4 So ist z. B. der OCSP **responseStatus** auszuwerten, wenn Verzeichnisdienstauskünfte eingeholt werden.

Manche Prüfbedingungen können allerdings nur in Abhängigkeit vom jeweiligen Anwendungskontext festgelegt werden. Die Definition solcher, auch formaler, technischer Prüfbedingungen für spezifische Anwendungskontexte ist nicht Gegenstand dieses Teildokuments von SigI. Dennoch müssen solche Prüfbedingungen gegebenenfalls vom Benutzer anhand von Informationen bewertet werden, die vom technischen Prüfprozeß an der Benutzungsoberfläche bereitgestellt werden. Solche Informationen werden in diesem Dokument benannt. Ihre Darstellung ist in [BSI-AIS] spezifiziert.

3.3 Prüfpolicy

Die Entscheidung über die technische Gültigkeit digitaler Signaturen hängt davon ab, welche Prüfbedingungen für welche Prüfobjekte untersucht werden. Für die Auswahl der Prüfobjekte und Prüfbedingungen im Rahmen dieser Spezifikation sind die folgenden Faktoren relevant:

- *Vorgaben des SigG:* Prüffunktionen müssen die Anforderungen prüfen, die nach dem SigG und der SigV zu erfüllen sind.
- *Vorgaben von SigI:* Soweit allgemeine Anforderungen aus dem SigG und der SigV in SigI präzisiert werden, werden die Prüfbedingungen darauf abgestellt.
- *Annahmen über Zusicherungen durch Sicherheitskonzepte:* Von Zertifizierungsstellen wird gefordert, daß sie Anforderungen nach SigG, SigV und SigI erfüllen und dies in ihrem Betriebs- und Sicherungskonzept nachweisen müssen. Das BSI geht davon aus, daß diese Anforderungen im Rahmen des Genehmigungsverfahrens und der Kontrollen nach SigG überprüft werden. Es erlaubt im Rahmen von SigI deshalb, daß die entsprechenden Prüfbedingungen als erfüllt angenommen werden.
- *Konfigurationsmöglichkeiten für den Prüfenden:* Das BSI geht davon aus, daß Prüfende ihren Prüfaufwand und ihre Risiken gegenüber einer vollständigen technischen Signaturprüfung nach den eigenen Risikopräferenzen steuern wollen. Daher werden von SigI-konformen Prüffunktionen eine Reihe von Konfigurationsmöglichkeiten gefordert, mit denen bestimmte Prüfobjekte oder Prüfbedingungen ausgeschaltet werden können.

Die jeweilige Prüfpolicy eines Benutzers ergibt sich aus der Menge der Prüfbedingungen, die nach diesen Regeln und seiner persönlichen Konfiguration den Umfang der technischen Signaturprüfung bestimmen. Veränderungen der Prüfpolicy durch Konfiguration oder durch Prüfbedingungen, die ein Hersteller zusätzlich implementiert, können daher das Prüfergebnis der technischen Signaturprüfung beeinflussen.

3.4 Prüfergebnisse

Das Gesamtergebnis einer technischen Signaturprüfung wird aus den Teilergebnissen über die Prüfbedingungen für das Primärdokument gebildet. In diesen sind die Prüfbedingungen für die Prüfobjekte zweiter und dritter Ordnung entweder direkt oder über Zwischenergebnisse enthalten. Der Benutzer muß die Details einer technischen Signaturprüfung feststellen können, um eine differenzierte Bewertung eines Prüfergebnisses vornehmen oder Fehler eingrenzen zu können. Außerdem sollen die Prüfergebnisse protokolliert werden.

3.4.1 Ergebnisse von Teilprüfungen

Jede Prüfbedingung liefert im Prüfprozeß ein Ergebnis. Diese Ergebnisse werden als *Teilergebnisse* bezeichnet. Für die Teilergebnisse werden in diesem Dokument die folgenden Klassen unterschieden:

Situation	Teilergebnisklasse	Abkürzung
Prüfung durch Benutzer abgebrochen	"Prüfung abgebrochen, kein Ergebnis"	pake
Prüfbedingung nicht erfüllt	"technisch nicht gültig"	tng
notwendige Voraussetzungen für die Prüfung nicht gegeben (z.B. keine aktuelle Sperrliste)	"technisch nicht prüfbar"	tnp
Algorithmus oder Schlüssellänge ist als mathematisch unsicher eingestuft	"Sicherheitsvermutung nicht gegeben: Algorithmus oder Schlüssellänge mathematisch unsicher"	mu
Es ist unsicher, ob die mathematische Eignung eines Algorithmus oder einer Schlüssellänge noch angenommen werden kann.	"mathematische Sicherheit offen"[5]	mso
Prüfbedingung durch Konfiguration nicht berücksichtigt	"keine Prüfung"	kp
Prüfbedingung erfüllt	"technisch gültig"	tg

SigI-konforme Prüffunktionen MÜSSEN mindestens diese Klassen für die Darstellung von Teilergebnissen unterscheiden. SigI-konforme Prüffunktionen SOLLEN detailliertere Meldungen von Teilergebnissen in der Detaildarstellung[6] erzeugen.

Das Ergebnis von Teilprüfungen kann außerdem Meldungsergänzungen enthalten, die im Gesamtergebnis anzuzeigen sind. Die entsprechenden Konformitätsanforderungen werden im Text durch "MELDUNGSERGÄNZUNG" hervorgehoben.

3.4.2 Zwischenergebnisse

Zwischenergebnisse werden in dieser Spezifikation verwendet, um die Teilergebnisse der Prüfbedingungen für ein Prüfobjekt, zusammenzufassen. Für einzelne Prüfobjekte sind Umsetzungsregeln erforderlich, mit denen das Zwischenergebnis auf einen anderen Wert abgebildet wird.

Beispiel: Eine Verzeichnisdienstauskunft sei mathematisch nicht korrekt signiert. Das Zwischenergebnis der technischen Signaturprüfung für die Verzeichnisdienstauskunft lautet daher "technisch nicht gültig". Die Verzeichnisdienstauskunft kann daher nicht für die Prüfung verwendet werden. Für die Gesamtprüfung fehlen daher die Informationen zur Vorhandenseins- und Sperrprüfung. Deshalb wird ein Zwischenergebnis erzeugt, das auf "technisch nicht prüfbar" lautet.

---

5 Diese Teilergebnisklasse ist erforderlich, weil gegenwärtig noch kein Austauschformat für die Eignung von Algorithmen spezifiziert ist. Eine solche Spezifikation ist für eine künftige Version von SigI geplant (vgl. Anhang 0). Als Interimslösung knüpft das BSI die Eignung von Algorithmen implizit an die Gültigkeitsdauer von Zertifikaten. Das Prüfergebnis tritt auf, wenn das Gültigkeitsende des Teilnehmerzertifikat erreicht wurde, da nach diesem Zeitpunkt keine Aussage zur Eignung des Verfahrens mehr vorliegt. Durch diese Entwurfsentscheidung des BSI soll der Implementierungsaufwand zur Verteilung und Verwaltung von Informationen zur Eignung von Algorithmen verringert werden. Die Ergebnisklasse kann beim Vorliegen solcher Informationen durch veränderte Prüfbedingungen für Teilergebnisse und das Gesamtergebnis entfallen.

6 Vgl. unten.

SigI-Konformitätsanforderungen

Ein Zwischenergebnis wird nach den gleichen Regeln gebildet, wie das Gesamtergebnis. Soweit für einzelne Prüfobjekte Umsetzungsregeln angegeben werden, sind dieses anzuwenden. Meldungsergänzungen müssen immer im Gesamtergebnis berücksichtigt werden.

3.4.3 Gesamtergebnis

Das *Gesamtergebnis der technischen Signaturprüfung* bietet dem Benutzer eine knappe Meldung, die das Ergebnis aller Prüfbedingungen einschließlich der Zwischenergebnisse für das Primärdokument zusammenfaßt. Das Gesamtergebnis setzt sich aus zwei Teilen zusammen: dem technischen Gesamtergebnis und Zusatzinformationen.

Für das technische Gesamtergebnis können folgende Situationen unterschieden werden:

- Prüfbedingungen, die technisch überprüfbar sind, werden nicht erfüllt. Ist dies für eine oder mehrere Prüfbedingungen der Fall lautet das Gesamtergebnis:
  "Signatur technisch nicht gültig"
- Bestimmte Prüfbedingungen können nicht überprüft werden, weil die dazu notwendigen Informationen nicht oder nicht ausreichend aktuell vorliegen. Sind alle anderen Prüfbedingungen erfüllt, lautet das Gesamtergebnis:
  "Signatur technisch nicht prüfbar"
- Alle technischen Prüfbedingungen können geprüft werden und sind, soweit sie nicht die Eignung von Algorithmen betreffen, erfüllt. Der Prüffunktion stehen Informationen zur Verfügung, die einen oder mehrere Algorithmen, gegebenenfalls mit Schlüssellänge, als unsicher kennzeichnen. In diesem Fall lautet das Gesamtergebnis:
  "Sicherheitsvermutung nicht gegeben: Signatur mathematisch unsicher, alle anderen technischen Prüfbedingungen werden erfüllt."
- Alle technischen Prüfbedingungen können geprüft werden und sind erfüllt. Der Signaturzeitpunkt des Primärdokuments liegt im Gültigkeitszeitraum des Teilnehmerzertifikats. Der Gültigkeitszeitraum des Teilnehmerzertifikats ist zum Prüfzeitpunkt allerdings bereits abgelaufen. Daher kann keine zuverlässige Annahme zur Eignung von Algorithmen mehr getroffen werden. Keiner der eingesetzten Algorithmen, gegebenenfalls mit Schlüssellänge, ist jedoch nach den Informationen der Prüffunktion als unsicher zu bewerten. In diesem Fall lautet das Gesamtergebnis:
  "Signatur technisch gültig, aber keine Aussage über die mathematische Sicherheit möglich"
- Alle Prüfbedingungen sind erfüllt und keine der vorgenannten Situationen ist gegeben. In diesem Fall lautet das Gesamtergebnis:
  "Signatur technisch gültig"
- Durch einen Benutzereingriff wurde der Prüfprozeß abgebrochen. In diesem Fall lautet das Gesamtergebnis:
  "Prüfung abgebrochen, kein Ergebnis"

Außerdem muß im Gesamtergebnis dargestellt werden, ob die technische Signaturprüfung vollständig durchgeführt wurde oder ob auf Grund einer Konfiguration der Prüffunktion nur ein Teil der Prüfobjekte untersucht wurde.

Zusatzinformationen beinhalten insbesondere solche Informationen, die der Prüfende benötigt, um die Signatur in ihrem rechtlichen und Kooperationskontext zu bewerten. Dazu gehören insbesondere:

- der Name des Signierenden,

- Nutzungsbeschränkungen oder Zeichnungsberechtigungen aus dem Teilnehmerzertifikat oder Attribut-Zertifikaten,
- der Name der root der geprüften Zertifikatketten und
- alle MELDUNGSERGÄNZUNGEN, die im gesamten Prüfprozeß entstanden sind.

SigI-Konformitätsanforderungen

Für das Gesamtergebnis der technischen Signaturprüfung "Signatur technisch gültig" MÜSSEN alle im folgenden als verbindlich vorgegebenen Prüfbedingungen erfüllt sein. Ansonsten muß ein einschränkendes oder ablehnendes Ergebnis gemäß der folgenden Tabelle erzeugt werden. Das Gesamtergebnis wird aus den Teilergebnissen der Prüfung des Primärdokuments gebildet. Das erste zutreffende Feld der linken Spalte (Ergebnisse der Teilprüfungen) entscheidet über das Gesamtergebnis.

Außer in den Fällen "Prüfung abgebrochen, kein Ergebnis" und "Signatur technisch nicht gültig" MUSS das Gesamtergebnis gekennzeichnet werden, wenn durch die Voreinstellungen in der Konfiguration oder durch Eingriffe während des Prüfprozesses einzelne Prüfbedingungen in der technischen Signaturprüfung nicht berücksichtigt werden (ein oder mehrere Teilergebnisse "kp"). Im Falle technisch nicht gültiger Signaturen wird keine Kennzeichnung vorgenommen. Als Kennzeichnung SOLL der Text "(bei eingeschränkter Prüfung)" verwendet werden.

SigI-konforme Prüffunktionen MÜSSEN für das Gesamtergebnis folgendes funktionale Verhalten aufweisen:

Ergebnisse der Teilprüfungen	Gesamtergebnis	"kp"-Kennzeichnung
Prüfung durch Benutzereingriff abgebrochen ("pake")	"Prüfung abgebrochen, kein Ergebnis"	nein
ein oder mehrere Prüfbedingungen "tng"	"Signatur technisch nicht gültig"	nein
keine Prüfbedingung "tng" und ein oder mehrere Prüftatbestände "tnp"	"Signatur technisch nicht prüfbar"	ja
Alle technischen Prüfbedingungen können geprüft werden und sind mit der folgenden Ausnahme "tg": Ein oder mehrere Teilergebnisse sind "mu" (Der Prüffunktion steht eine Information zur Verfügung, die einen Algorithmus, gegebenenfalls mit Schlüssellänge, als unsicher kennzeichnet.)	"Sicherheitsvermutung nicht gegeben: Signatur mathematisch unsicher, alle anderen technischen Prüfbedingungen werden erfüllt"	ja
Alle technischen Prüfbedingungen können geprüft werden und sind "tg". Ein oder mehrere Teilergebnisse sind "mso" (Dies kann der Fall sein, wenn der Gültigkeitszeitraum des Teilnehmerzertifikats bereits abgelaufen ist). Kein Teilergebnis lautet "mu" (Keiner der eingesetzten Algorithmen, gegebenenfalls mit Schlüssellänge, ist nach den Informationen der Prüffunktion als unsicher zu bewerten.)	"Signatur technisch gültig, aber keine Aussage über die mathematische Sicherheit möglich"	ja
alle Prüfbedingungen erfüllt, keine Prüfbedingung "tng", "tnp", "mu" oder "mso"	"Signatur technisch gültig"	ja

Das Gesamtergebnis MUSS außerdem um die Meldungen ergänzt werden, die für die einzelne Prüftatbestände und Prüfbedingungen festgelegt werden.

Alle Ergebnisse und Meldungen an den Benutzer sind in Übereinstimmung mit [BSI-AIS] darzustellen.

3.4.4 Detailergebnisse der technischen Signaturprüfung

Im Meldungsfenster des Gesamtergebnisses muß der Benutzer die Anzeige von Teilergebnissen veranlassen können. Die Detailangaben müssen einem kundigen Benutzer oder einem Benutzerservice die detaillierte Bewertung und Analyse eines Gesamtergebnisses erlauben.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN auf Anfrage zu jedem Prüfobjekt der aktuellen technischen Signaturprüfung die Teilergebnisse zu allen Prüfbedingungen bereitstellen. Der Umfang der zu berücksichtigenden Prüfobjekte wird bestimmt durch:

- die Konfiguration der Prüffunktion. Für Prüfobjekte, die durch Konfiguration oder Einzelentscheidung von der Prüfung ausgenommen werden, MUSS "kp" angezeigt werden, aber keine weitere Sperr- oder Vorhandenseinsprüfung durchgeführt werden. Der Benutzer MUSS erkennen können, wie er die notwendigen Teilprüfungen für das betreffende Prüfobjekt manuell oder durch Veränderung der Konfiguration anstoßen kann.
- Prüfobjekte, bei denen die mathematische Prüfung scheitert. Für sie muß "tng" angezeigt werden. Es muß keine weitere Prüfung von Zertifikaten oder Sperr- oder Vorhandenseinsprüfung durchgeführt werden.
- Prüfobjekte oder Informationen, die nicht zur Verfügung stehen, z. B. wenn notwendige Zertifikate oder Sperrlisten wegen einer Netzwerkstörung nicht aus einem Verzeichnis abgerufen werden können, oder die aus anderen Gründen nicht prüfbar sind. Für sie muß "tnp" angezeigt werden. Es muß keine weitere Prüfung von Zertifikaten oder Sperr- oder Vorhandenseinsprüfung durchgeführt werden.
- für alle anderen Prüfobjekte sind alle Prüfbedingungen zu prüfen und die Teilergebnisse darzustellen.

SigI-konforme Prüffunktionen MÜSSEN je Teilergebnis, das nicht "tg" lautet, die möglichen Ursachen für das Teilergebnis darstellen. Diese Ursachen SOLLEN so beschrieben werden, daß sie dem Anwender Hilfestellung bei der Interpretation des Teilergebnisses geben und zur Bewertung des rechtlichen Risikos genutzt werden können.

3.4.5 Protokollierung der Prüfergebnisse

Anhand protokollierter Prüfergebnisse können Benutzer nachvollziehen, welche Prüfungen sie durchgeführt haben. Dieses Protokoll soll keinen Beweiswert haben, sondern lediglich lokal zur Unterstützung und Nachvollziehbarkeit von Arbeitsabläufen dienen.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen SOLLEN eine Protokollierung von Prüfergebnissen erlauben, aus der hervorgehen:

- der Zeitpunkt der Prüfung (mit Datum und Uhrzeit),
- das geprüfte Objekt und
- das Prüfergebnis.

Die Protokollierung SOLL konfigurierbar sein bezüglich:

- der Protokollierung des Gesamtergebnisses oder der Protokollierung von Detailresultaten,
- der maximalen Größe der Logdatei und
- des Verhaltens bei Erreichen des Maximalumfangs. Als Optionen SOLLEN mindestens vorgesehen werden:
  - eine Meldung an den Benutzer mit der Möglichkeit, die bisherige Protokolldatei zu sichern, und
  - automatisches Überschreiben älterer Logsätze (first in first out) ohne Anfrage beim Benutzer.

4 Allgemeine Prüftatbestände technischer Signaturprüfungen

Dieses Kapitel stellt die Prüftatbestände dar und abstrahiert dabei von spezifischen Prüfbedingungen für die unterschiedlichen Prüfobjekte. Soweit allgemeine Funktionalitäten oder Eigenschaften formuliert werden können, die von SigI-konformen Prüffunktionen bereitzustellen sind, werden diese bereits bei den einzelnen Prüftatbeständen aufgeführt. Die Konkretisierung weiterer Prüfbedingungen für spezifische Prüfobjekte erfolgt im nächsten Kapitel.

Die Prüftatbestände werden so dargestellt, wie sie für eine vollständige Signaturprüfung nach SigG zu prüfen wären. Soweit Annahmen für Prüfbedingungen nach der durch das BSI vorgegebenen Gültigkeitspolicy getroffen werden dürfen, werden sie in den einzelnen Kapiteln benannt. Auf dieser Grundlage werden die verpflichtenden Prüfbedingungen für SigI-konforme Prüffunktionen spezifiziert. Soweit Prüfbedingungen tabellarisch angegeben werden, sind in der Regel nur die "negativen Fälle" (alle außer "tg") aufgeführt. In den Tabellen werden die Teilergebnisse in der Abkürzungsschreibweise angegeben.

4.1 Aufbau eines digital signierten Dokuments

Das Primärdokument und alle weiteren zu seiner Prüfung notwendigen Prüfobjekte müssen in ihrem Aufbau den jeweils entsprechenden Vorgaben der anderen Spezifikationen nach SigI entsprechen.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN sicherstellen, daß je nach Prüfobjekt alle in der zugehörigen Spezifikation ([BSI-ZERT], [BSI-SIG], [BSI-TSS] oder [BSI-DIR]) geforderten Attribute enthalten sind. SigI-konforme Prüffunktionen MÜSSEN insbesondere sicherstellen, daß in jedem Prüfobjekt der eindeutige Verweis auf das zur Prüfung zu verwendende Zertifikat enthalten und gemäß der Spezifikationen nach SigI in die Signatur eingeschlossen ist.

Nr.	Prüfbedingung	Fall	Teilergebnis
	Aufbau des Prüfobjekts entspricht SigI	unbekanntes Format	tnp
		geforderte Attribute fehlen	tng

SigI-konforme Prüffunktionen MÜSSEN feststellen, ob in einem digital signierten Dokument Attribute mit gesetzten criticalFlag enthalten sind, die die Funktion nicht verarbeiten kann. Wenn dies der Fall ist, kann das entsprechende Prüfobjekt nicht vollständig geprüft werden.

Nr.	Prüfbedingung	Fall	Teilergebnis
	keine unbekannten Attribute mit "**criticalFlag** = true" im Prüfobjekt enthalten	unbekannte Attribute mit "**criticalFlag** = true" sind im Prüfobjekt enthalten	tnp

SigI-konforme Prüffunktionen MÜSSEN den Benutzer außerdem mit einer MELDUNGSERGÄNZUNG informieren, wenn in einem Prüfobjekt unbekannte Attribute enthalten sind.

- In Zertifikaten, Sperrlisten und Verzeichnisdienstauskünften, müssen in der MELDUNGSERGÄNZUNG unbekannte Extensions angezeigt werden, deren **criticalFlag** = "false" gesetzt ist.
- In Nachrichten im CMS-Format[7] (Primärdokumente, Zeitstempel) müssen unbekannte Attribute ebenfalls in einer MELDUNGSERGÄNZUNG angezeigt werden.

SigI-konforme Prüffunktionen SOLLEN deshalb die nach den Spezifikationen [BSI-ZERT], [BSI-SIG], [BSI-TSS] und [BSI-DIR] optionalen Attribute unterstützen, um solche Meldungsergänzungen zu vermeiden.

4.2 Mathematische Prüfung des digital signierten Dokuments

Für alle Typen von digital signierten Dokumenten muß die mathematische Relation zwischen dem Authentikator und dem jeweiligen Prüfschlüssel erfüllt sein.

4.2.1 Eindeutige Identifikation von Zertifikaten und Prüfschlüssel

Für die technische Signaturprüfung eines Prüfobjekts nach SigI muß eindeutig bestimmt werden, welches Zertifikat für die Prüfung eines Authentikators verwendet werden soll. Der Prüfschlüssel darf nur aus diesem Zertifikat entnommen werden. Über die verschiedenen Stufen der Prüfung wird dadurch implizit sichergestellt, daß zu jedem digital signierten Dokument eine eindeutige Zertifikatkette rekonstruiert wird. Diese Zertifikatkette muß für jede Signaturprüfung - auch zu einem späten Zeitpunkt, an dem einige der Zertifikate möglicherweise bereits ausgelaufen sind - verwendet werden.

Die Voraussetzungen für die Identifikation des zum Prüfen zu verwendenden Zertifikats sind in den Formaten nach [BSI-ZERT], [BSI-SIG], [BSI-TSS] oder [BSI-DIR] gegeben.

R1) Der Prüfende kann die Zertifikatkette zum Zertifikat des Prüfschlüssels und die Attribut-Zertifikate mit den zugehörigen Zertifikatketten, durch die die Urheberschaft und die Autorisierung des digital signierten Dokuments nachgewiesen wird, anhand der Referenzen auf das jeweils übergeordnete Zertifikat eindeutig rekonstruieren. Diese Voraussetzung ist erfüllt, weil nach SigI in jedem Prüfobjekt der eindeutige Verweis auf das zur Prüfung zu verwendende Zertifikat enthalten ist.

Auch für die Prüfung des Schlüssels der Wurzel-Zertifizierungsinstanz muß das Wurzelzertifikat verwendet werden, das im Zertifikat der Zertifizierungsstelle eingetragen ist.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN folgende Informationen verwenden, um das Zertifikat mit dem Prüfschlüssel zu einem digital signierten Dokument zu bestimmen:

- in Primärdokumenten nach [BSI-SIG] und Zeitstempeln nach [BSI-TSS] aus dem Feld "**signedAttrs**" entweder das direkt angegebene Zertifikat (Attributtyp "**Certificate**") oder das über die Referenz abzuleitende Zertifikat (Attributtyp "**CertRef**" im Format Issuer und Seriennummer),
- in Zertifikaten und Attribut-Zertifikaten nach [BSI-ZERT] das Attribut "**authorityKeyIdentifier**" im Format Issuer und Seriennummer, .

7 In diesem Format ist das Konzept der Extensions mit der "critical"-Kennzeichnung nicht vorgesehen.

- in Sperrlisten [BSI-DIR] das Attribut "**authorityKeyIdentifier**" im Format Issuer und Seriennummer,
- in Verzeichnisdienstauskünften nach [BSI-DIR] durch das Attribut "**responderID**" `<?? Dieses Attribut bietet bisher nicht das Format Issuer und Seriennummer und ist deshalb nicht SigG-konform. Hier besteht Anpassungsbedarf in [BSI-DIR].??>.`

Sofern ein Zertifikat nicht über die Nachricht bereitgestellt wird und nicht lokal verfügbar ist, MÜSSEN SigI-konforme Prüffunktionen versuchen, dieses Zertifikat aus dem Verzeichnisdienst abzufragen. Sofern das Zertifikat ein Wurzelzertifikat ist, MUSS vor der Verwendung im Prüfprozeß ein Ablauf festgelegt sein, durch den der Benutzer entscheidet, ob er dieses Zertifikat als Wurzelzertifikat anerkennt. Dabei ist sicherzustellen, daß er dieses Zertifikat mit Informationen auf Unverfälschtheit und Urheberschaft prüfen kann, die ihm über einen unabhängigen Kanal zur Verfügung stehen.

Nr.	Prüfbedingung	Fall	Teilergebnis
	Zertifikat zum Prüfen eines digital signierten Dokuments liegt vor	nicht erfüllt	tnp

4.2.2 Bestimmung der Verfahren

Um Angriffe auf die mathematische Sicherheit abzuwehren, müssen für die mathematische Prüfung die richtigen Algorithmen verwendet werden.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN zur mathematischen Verifikation eines Authentikators verwenden:

- den Algorithmus des öffentlichen Schlüsselverfahrens, der im nach Kapitel 4.2.1 bestimmten Zertifikat gesichert enthalten ist;[8]
- den Algorithmus des Hash-Verfahrens, der aus den gesicherten Angaben im Padding des entschlüsselten Authentikators oder aus dem nach Kapitel 4.2.1 bestimmten Zertifikat des Prüfschlüssels abzuleiten ist.[9]

SigI-konforme Prüffunktionen MÜSSEN dabei sicherstellen, daß ungesicherte Angaben zu Algorithmen[10] mit den durch den Authentikator gesicherten Angaben übereinstimmen.

Nr.	Prüfbedingung	Fall	Teilergebnis
	ungesicherte Angaben zu kryptographischen Verfahren für die Prüfung eines Authentikators stimmen mit den gesicherten überein	nicht erfüllt	tng

8 Dies ist die Angabe für die Verwendung des Prüfschlüssels.

9 Ob die Informationen über das Hash-Verfahren direkt über den Authentikator oder im Zertifikat zur Verfügung stehen, hängt vom eingesetzten öffentlichen Schlüsselverfahren ab (vgl. dazu [BSI-SIG]).

10 Z. B. die ungesicherte Information über das Hash-Verfahren in Primärdokumenten, durch die eine Prüfung in einem Durchgang möglich wird.

4.2.3 Eignung von Verfahren und Schlüssellänge

Nach SigG / SigV werden mathematische Algorithmen (öffentliche Schlüsselverfahren und Hash-Verfahren) regelmäßig bezüglich ihrer kryptographischen Sicherheit bewertet und mit Angaben zur Mindestlänge von Schlüsseln für einen bestimmten Zeitraum als geeignet bewertet. Die Prüfung der Eignung der für eine bestimmte digitale Signatur verwendeten Algorithmen gibt dem Prüfenden daher Aufschluß, ob das nach dem SigG geforderte hohe mathematische Sicherheitsniveau für diese Signatur erreicht wird.

Für den Prüftatbestand ist festzustellen, ob die einzelnen verwendeten Verfahren und Schlüssellängen zu den im Bundesanzeiger veröffentlichten Verfahren gehören und der Eignungszeitraum noch nicht abgelaufen ist.

4.2.3.1 Verfügbarkeit von Verfahren in der Prüffunktion

Nicht alle der im Bundesanzeiger als geeignet angesehenen Algorithmen sind in SigI nach [BSI-SIG, Kapitel 3] zulässig.[11] Außerdem muß angenommen werden, daß im Laufe der Zeit bestehende Verfahren mit neuen Vorgaben für Parameter oder Schlüssellängen für geeignet erklärt werden, die von einer vorliegenden Prüffunktion nicht verarbeitet werden können. Auch können neue Verfahren für geeignet erklärt werden, die in einer vorliegenden Prüffunktion noch nicht implementiert sind, aber von Signaturfunktionen anderer Teilnehmer oder Zertifizierungsstellen bereits eingesetzt werden.[12]

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	Parameter oder Schlüssellängen zu bekanntem Verfahren mit der vorliegenden Implementierung verarbeitbar	nicht erfüllt	tnp
	öffentliches Schlüsselverfahren und Hash-Verfahren bekannt	nicht erfüllt	tnp

SigI-konforme Prüffunktionen müssen die Verfahren nach [BSI-SIG, Kapitel 3] unterstützen.

4.2.3.2 Öffentliche Schlüsselverfahren

Für welches öffentliche Schlüsselverfahren ein Schlüsselpaar geeignet ist, wird im Zertifikat eingetragen. Die Prüffunktion muß nach Kapitel 4.2.2 diese Information für die mathematische Prüfung verwenden.

11 In SigI wurde eine Beschränkung auf ein Signaturverfahren auf der Basis Elliptischer Kurven vorgenommen (ECDSA).

12 Dazu ist zwar eine Erweiterung der Spezifikation SigI erforderlich. jedoch muß in einer solchen Situation davon ausgegangen werde, daß "alte" und "neue" Komponenten parallel eingesetzt werden. Die folgenden Anforderungen sollen sicherstellen, daß Prüffunktionen in diesem Fall ein definiertes Verhalten aufweisen.

SigI-Konformitätsanforderungen

R2) Das BSI setzt voraus, daß in Zertifizierungsstellen nach SigI nur Zertifikate ausgestellt werden, deren Algorithmen und Schlüssellängen für den Gültigkeitszeitraum des Zertifikats geeignet sind. Dabei wird sichergestellt, daß die Algorithmen und Schlüssellängen, die für das Zertifikat der Zertifizierungsstelle und deren übergeordnete Zertifikate verwendet wurden, ebenfalls bis zum Ende des Gültigkeitszeitraums des Teilnehmerzertifikats geeignet sind. Diese Bedingungen sind durch das Sicherheitskonzept der Zertifizierungsstelle mit einem hohen Sicherheitsniveau durchzusetzen.

SigI-konforme Prüffunktionen KÖNNEN ZUNÄCHST DAVON AUSGEHEN, daß die Eignung des im Zertifikat des Prüfschlüssel angegebenen öffentlichen Schlüsselverfahren und der angegebenen Schlüssellänge für die Gültigkeitsdauer des Teilnehmerzertifikats gegeben ist. Mögliche Einschränkungen werden unten formuliert.

4.2.3.3 Hash-Verfahren

Im Rahmen von SigI ist vorgesehen, daß die Wahl von Hash-Verfahren und öffentlichen Schlüsselverfahren zur Bildung des Authentikators unabhängig voneinander erfolgen kann, wenn dies durch eine Angabe im Padding möglich ist. Daher können die zulässigen Hash-Verfahren nicht immer über die Informationen aus dem Zertifikat des Prüfschlüssels, sondern in einigen Fällen nur aus dem Prüfobjekt selbst entnommen werden. Die Prüffunktion benötigt daher eine Liste der zulässigen Hash-Verfahren. In dieser muß das Hash-Verfahren des Prüfobjekts enthalten sein.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN eine Liste zulässiger Hash-Verfahren führen. Sie MÜSSEN Funktionen anbieten, mit der diese Liste vom Benutzer verwaltet werden kann.

R3) Das BSI setzt voraus, daß von Zertifizierungsstellen nach SigI nur Zertifikate und Attribut-Zertifikate ausgestellt werden, deren Authentikatoren mit Hash-Verfahren erzeugt werden, die für den Gültigkeitszeitraum des Zertifikats geeignet sind. Dabei wird sichergestellt, daß auch die Hash-Verfahren, die für das Zertifikat der Zertifizierungsstelle und deren übergeordnete Zertifikate verwendet wurden, ebenfalls bis zum Ende des Gültigkeitszeitraums des Teilnehmerzertifikats geeignet sind. Diese Bedingungen sind durch das Sicherheitskonzept der Zertifizierungsstelle mit einem hohen Sicherheitsniveau durchzusetzen.

SigI-konforme Prüffunktionen KÖNNEN daher für Prüfobjekte, die von Zertifizierungsstellen signiert wurden, ZUNÄCHST DAVON AUSGEHEN, daß das verwendete Hash-Verfahren für die Gültigkeitsdauer des Zertifikats zum Prüfschlüssel erfüllt ist.[13]

4.2.3.4 Bewertung der Eignung zum Prüfzeitpunkt

Die Eignung der kryptographischen Verfahren wird im Laufe der Zeit unterschiedlich bewertet. Durch besondere Erkenntnisse in der Kryptanalyse können öffentliche Schlüsselverfahren und Hash-Verfahren auch vorzeitig ungeeignet werden. Diese Information wird von der RegTP ebenfalls veröffentlicht. Im Rahmen des Prüfprozesses ist festzustellen, ob

13 Die Unterscheidung zwischen Primärdokumenten und Prüfobjekten, die von Zertifizierungsstellen signiert wurden, erscheint aufwendiger, als die hier spezifizierte Prüfbedingung auf alle Prüfobjekte anzuwenden. Auf die Differenzierung der Fälle wurde deshalb in der folgenden Tabelle verzichtet.

ein verwendetes Verfahren *nicht* zu den als ungeeignet bewerteten Verfahren gehört. Um diesen Fall zu beherrschen, müssen Anwender die Algorithmen und Parameter in der Prüffunktion konfigurieren können.

SigI-Konformitätsanforderungen "Verwaltung von Verfahren"

SigI-konforme Prüffunktionen müssen eine Möglichkeit zur Verwaltung von ungeeigneten öffentlichen Schlüsselverfahren mit ihren Parametern und Schlüssellängen bieten.

Auch in der Liste der Hash-Verfahren muß es möglich sein, Verfahren, die inzwischen als ungeeignet erklärt wurden, zu verwalten. Die Liste muß Informationen zum Anfangszeitpunkt der Eignung und zum Endzeitpunkt der Eignung bereitstellen.

SigI-Konformitätsanforderungen "Zeitpunkt der Eignungsbewertung"

Da der Signaturzeitpunkt weit zurückliegen kann, aber die aktuelle Stärke der Mechanismen berücksichtigt werden muß, muß in der Prüfung als Zeitpunkt für die Bewertung der Eignung der aktuelle Zeitpunkt (*Prüfzeitpunkt*) verwendet werden,[14] soweit dies in dieser Spezifikation nicht anders bestimmt wird.

SigI-Konformitätsanforderungen "Gesicherte Zertifikate in Verzeichnisdienstauskünften"

Im Rahmen von Verzeichnisdienstanfragen können auch Zertifikate abgefragt werden. Diese werden, soweit der Inhaber ihrer Bereitstellung zugestimmt hat, mit der Antwort übermittelt. Dazu nimmt das BSI an:

R4) Das BSI setzt voraus, daß von Zertifizierungsstellen nach SigI Verzeichnisdienstauskünfte nur mit aktuell geeigneten Verfahren signiert werden. Da die Zertifikate in der Zertifizierungsstelle mit geprüften Komponenten verwaltet werden und insofern gegen Verfälschung geschützt sind, werden durch die Signatur der Verzeichnisdienstauskunft auch die (alten) Zertifikate selbst gegen Verfälschung gesichert. Die Anforderungen an die Zertifizierungsstelle sind durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchzusetzen.

Dadurch können mit Hilfe von Verzeichnisdienstauskünften auch "alte" Zertifikate verwendet werden, die mit nicht mehr geeigneten Verfahren oder Schlüssellängen erzeugt wurden. SigI-konforme Prüffunktionen dürfen unter diesen Bedingungen allerdings nur auf solche Zertifikate vertrauen, die in der Verzeichnisdienstauskunft als vollständiges Zertifikat enthalten waren. Für diese in der Verzeichnisdienstauskunft enthaltenen Zertifikate müssen die Bedingungen aus Kapitel 4.2.1 geprüft werden.

SigI-Konformitätsanforderungen "Eignungsprüfung von Hash-Verfahren"

Für die Prüfung der Eignung von Hash-Verfahren MÜSSEN SigI-konforme Prüffunktionen folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	Hash-Verfahren zum Prüfzeitpunkt geeignet?	Hash-Verfahren nicht in der Liste geeigneter Hash-Verfahren	tng

14 Wie oben in der Bestimmung des Gegenstands bereits erwähnt, werden "erneute digitale Signaturen" nach § 16 Nr. 7 iVm § 18 SigV in dieser Spezifikation nicht berücksichtigt.

Nr.	Prüfbedingung	Fall	Teilergebnis
		Hash-Verfahren in der Liste geeigneter Hash-Verfahren, aber Eignung zum Prüfzeitpunkt bereits abgelaufen	mu
		Hash-Verfahren in der Liste geeigneter Hash-Verfahren und Eignung zum Prüfzeitpunkt gegeben	tg

SigI-Konformitätsanforderungen "Eignungsprüfung von öffentlichen Schlüsselverfahren"

Für die Prüfung der Eignung von öffentlichen Schlüsselverfahren MÜSSEN SigI-konforme Prüffunktionen folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	öffentliches Schlüsselverfahren mit vorliegenden Parametern und Schlüssellängen zum Prüfzeitpunkt geeignet	ist ungeeignet gemäß vorliegender Informationen	mu
		es liegt keine Information vor, nach der gilt "Verfahren ist ungeeignet", aber $t_{Prüf} < t_E([Zert_{Tln}])$	tg
		es liegt keine Information vor, nach der gilt "Verfahren ist ungeeignet", aber $t_{Prüf} > t_E([Zert_{Tln}])$	mso
		sofern das Prüfobjekt ein Zertifikat aus einer technisch gültigen Verzeichnisdienstauskunft aus der Sicherungsinfrastruktur nach SigI ist, wobei insbesondere die Eignung der Algorithmen für die Verzeichnisdienstauskunft zum Prüfzeitpunkt gegeben ist, gilt für das Teilergebnis:[15]	tg

Unterstützung der Verwaltung kryptographischer Verfahren

Zur Verwaltung der Eignung kryptographischer Funktionen benötigt der Benutzer den Bundesanzeiger. Um dem Benutzer die Verwaltung der kryptographischen Verfahren zu erleichtern, SOLLEN SigI-konforme Prüffunktionen eine download-Möglichkeit oder einen WWW-Zugang zum Bundesanzeiger anbieten. SigI-konforme Prüffunktionen MÜSSEN beim Abruf jedoch darauf hinweisen, daß die elektronisch abgerufene Information nicht gegen Manipulation oder Maskerade gesichert ist und unter Sicherheitsaspekten deshalb das Printmedium nicht ersetzen kann.

15 Das Teilergebnis "bestätigt" in diesem Fall die Eignung der Algorithmen, mit denen das Prüfobjekt, in diesem Fall das ursprüngliche Zertifikat, durch die Verzeichnisdienstauskunft bestätigt wurde. Durch die Annahme des BSI ist die Eignung der ursprünglichen Algorithmen nicht mehr von Bedeutung.

HINWEIS: Das BSI plant die Definition eines Austauschformats für Eignungsinformationen, durch die die Verwaltungsaufgaben des Prüfenden technisch unterstützt werden können (vgl. Anhang 3).

4.2.4 Mathematische Korrektheit

Der Authentikator des Prüfobjekts muß mit dem Prüfschlüssel aus dem nach Kapitel 4.2.1 bestimmten Zertifikat die geforderte mathematische Relation aufweisen.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen müssen zur mathematischen Verifikation eines Authentikators verwenden:

- den Prüfschlüssel aus dem Zertifikat, das nach Kapitel 4.2.1 bestimmt wird,
- die Verfahren, wie sie nach Kapitel 4.2.2 bestimmt werden.

Nr.	Prüfbedingung	Fall	Teilergebnis
	mathematische Korrektheit gemäß der vorgenannten Bedingungen gegeben	nicht erfüllt	tng

4.3 Prüfung des Namens des Signierenden

Für digital signierte Dokumente kann gefordert sein, daß sie von einem bestimmten Schlüsselinhaber signiert werden. Diese Prüfung ist notwendig, wenn Maskerade verhindert werden soll. Die Prüfung des Signierenden ist beispielsweise für Zertifikate oder Sperrlisten notwendig.

Eine Angabe zum Namen des Signierenden im jeweils signierten Dokument wird vom Signierenden selbst eingetragen. Sie wird daher von ihm kontrolliert. Als Name des Signierenden muß deshalb die Angabe zum **subject** aus dem Zertifikat verwendet werden, das den Prüfschlüssel enthält. Diese Information ist gegen eine Referenzinformation zu prüfen. Die Referenzinformation, gegen die geprüft werden muß, unterscheidet sich nach den Prüfobjekten. Die Prüfbedingungen werden daher in Kapitel 5 spezifiziert.

Für die Sicherungsinfrastruktur nach SigI muß sichergestellt werden, daß die in der Prüfung geforderten Konsistenzbedingungen beim Ausstellen der Zertifikate beachtet werden. Daher sind für die Zertifizierungshierarchie folgende Regeln einzuhalten:

R5) Die Namensgebung für Zertifikate, die von Zertifizierungsstellen eingesetzt werden, muß die folgenden automatisierten Abläufe und Prüfbedingungen in Prüfprozessen berücksichtigen: Der distinguished name von Zertifizierungsstellen entspricht implizit der "Adresse", unter der im Directory die aktuellen Sperrlisten abgefragt werden können. Außerdem wird dieser Name verwendet, um zu entscheiden, ob der Signierende überhaupt eine bestimmte Statusinformation bereitstellen darf. Um einfache Implementierungen der Prüffunktionen zu erlauben, wird auf die Grundregeln aus [ITU-T X.509 1997] zurückgegriffen. Danach muß der Name des Signierenden einer Standard-Sperrliste[16] mit dem Namen des Ausstellers des zu prüfenden Zertifikats übereinstimmen. Eine entsprechende Annahme wird in dieser Spezifikation für den Namen des Signierenden von Verzeichnisdienstauskünften getroffen.
Um einen geordneten Betrieb aufrecht zu erhalten, dürfen SigI-konforme Zertifizierungsstellen ihren distinguished name mit neuen Zertifikaten daher nicht wechseln, auch wenn sie neue Schlüsselpaare verwenden. Die Zertifikate, die zum Zertifizieren und zum Signieren von Verzeichnisdienstauskünften und Sperrlisten Zertifizierungsstelle ausgestellt werden, müssen den identischen distinguished name als Inhaber (subject) enthalten.

4.4 Zulässigkeit von Zertifikatketten

Durch den Aufbau der Zertifizierungshierarchie nach SigG können Zertifikatketten nur eine bestimmte Länge haben. Zertifikatketten sind außerdem nur dann zulässig, wenn sie in einem Wurzelzertifikat der RegTP enden.

4.4.1 Länge von Zertifikatketten

Durch Prüfbedingungen, die auf die Länge der Zertifikatkette abheben, wird erkannt, ob in einer nachgeordneten Zertifizierungsstelle unzulässigerweise ein Zertifikat für eine Zertifizierungsstelle ausgestellt wurde. Die maximale Länge von Zertifikatketten wird durch die Vorgabe des SigG bestimmt. Dabei wird grundsätzlich vorausgesetzt, daß Zertifikate nur mit Hilfe von Zertifizierungsstellen-Zertifikaten ausgestellt werden dürfen.

R6) Die Zertifizierungshierarchie nach SigG hat genau 3 Ebenen (Ebene 1 = RegTP, Ebene 2 = Zertifizierungsstellen, Ebene 3 = Teilnehmer-Zertifikate und Attribut-Zertifikate). Das BSI geht davon aus, daß eine SigI-konforme Zertifizierungsstelle auf Ebene 2 keine weiteren Zertifikate zum Ausstellen von Zertifikaten erzeugt. Implizit gilt für Zertifikatketten daher, daß sie maximal 3 Zertifikate enthalten dürfen. Das Attribut **pathLenConstraint** kann jedoch eingesetzt werden, um größerer Längen freizugeben.[17] Es darf von SigI-konformen Zertifizierungsstellen nur mit Zustimmung der Wurzel-Zertifizierungsinstanz verwendet werden. Die Anforderungen an die einzelne Zertifizierungsstelle sind durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchzusetzen.

---

16 Indirekte Sperrlisten, Sperrlisten über Distribution Points oder andere neuere Formen der Bereitstellung sind keine Standard-Sperrlisten. Jedoch werden nur Standard-Sperrlisten im Rahmen dieser Spezifikation von SigI-konformen Prüffunktionen gefordert und in den Prüfbedingungen berücksichtigt. SigI-konforme Prüffunktionen KÖNNEN andere Bereitstellungsformen unterstützen. In diesem Fall müssen die Prüfbedingungen entsprechend angepaßt werden.

17 Die implizite Maximallänge "3" muß von SigI-konformen Prüffunktion geprüft werden, wenn **pathLenConstraint** nicht enthalten ist. Die "Freigabe" entsteht daher relativ zur impliziten Grenze. Das Attribut wird in diesem Sinne zur kontrollierten Öffnung der Zertifizierungshierarchie einge-

SigI-konforme Prüffunktionen KÖNNEN DAHER ANNEHMEN, daß die Längenbegrenzung von Zertifikatketten eingehalten werden. Allerdings können sie sich erst auf dieses Annahme stützen, wenn sie die Zertifikatkette als SigI-konform geprüft haben.

Nach [BSI-ZERT] kann in Zertifikaten von Zertifizierungsstellen optional das Attribut **pathLenConstraint** enthalten sein. Der enthaltene Wert gibt an, wieviele Zertifizierungsstellen-Zertifikate noch maximal bis zum Wurzelzertifikat auftreten dürfen.[18]

Im allgemeinen Fall ergibt die Zertifizierungsrelation einen beliebigen Zertifizierungsgraphen. In diesem Fall sind Schleifen in Zertifikatketten möglich. Durch geeignete Prüfbedingungen für Zertifikate muß daher sichergestellt werden, daß Schleifen erkannt werden, damit die Prüfung terminiert. In einer strengen der Zertifizierungshierarchie nach SigG sind Schleifen in Zertifikatketten nicht möglich. Crosszertifikate führen allerdings bereits zu einer bidirektionalen Zertifizierungsrelation zwischen zwei Zertifizierungsstellen. Da die RegTP Crosszertifikate zwischen den Zertifizierungsschlüsseln zur Unterstützung des Schlüsselwechsels bereitstellen will, können dadurch Schleifen in Zertifikatketten auftreten. Crosszertifikate können auch für die Zertifizierung ausländischer Zertifizierungsstellen mit gleichem Sicherheitsniveau eingesetzt werden. Schließlich können Angreifer versuchen, den Prüfprozeß durch lange Zertifikatketten oder Schleifen in Zertifikatketten "außerhalb" von SigI zu stören.

SigI-Konformitätsanforderungen

Prüffunktionen MÜSSEN so implementiert werden, daß "Schleifen" erkannt werden und der Prüfprozeß terminiert.

SigI-konforme Prüffunktionen MÜSSEN die Länge von Zertifikatketten auf Übereinstimmung mit dem Zertifizierungsmodell nach SigG prüfen. Abweichend sind längere Zertifikatketten mit **pathLenConstraint** möglich. SigI-konforme Prüffunktionen SOLLEN dieses Attribut unterstützen. In diesem Fall MÜSSEN SIE die Bedingungen überprüfen, die an **pathLenConstraint** geknüpft sind, falls das Attribut im Zertifikat enthalten ist. Wenn das Attribut nicht unterstützt wird, ist es Bestandteil eines als "critical" gekennzeichneten Felds. Solche Zertifikate MÜSSEN als "tnp" abgelehnt werden, wenn **pathLenConstraint** nicht unterstützt wird.

Die Prüfbedingungen werden in Kapitel 5 formuliert.

4.4.2 Prüfung des Sicherungsankers

Zertifikatketten nach SigI müssen in einem Wurzelzertifikat der RegTP enden. Die Wurzel-Zertifizierungsinstanz (RegTP) kann zu beliebigen Zeitpunkten neue Schlüssel erzeugen und dafür Selbstzertifikate ausstellen. Solange ein Schlüsselpaar für die vorgesehene Gültigkeitsdauer eines Zertifikats geeignet ist, kann die RegTP auch ein neues Selbstzertifikat für einen bestehenden Schlüssel mit neuem Gültigkeitszeitraum ausstellen. Jedes dieser Selbstzertifikate (Wurzelzertifikate) bildet einen Sicherungsanker, der eine unabhängige Zertifizierungshierarchie aufspannt.

R7) Alle Selbstzertifikate der RegTP, die als Sicherungsanker für SigI verwendet werden sollen, genügen den Formatanforderungen von [BSI-ZERT]. Diese Anforderungen an die RegTP sind durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchzusetzen.

---

setzt. Für die Prüfbedingungen für **pathLenConstraint** ergeben sich jedoch keine Abweichungen gegenüber der Definition in [ITU-T X.509 1997].

18 Vgl. auch [ITU-T X.509 1997]

Im Laufe der Zeit wird die RegTP eine Reihe von Selbstzertifikaten erzeugen, die jeweils die Funktion eines Sicherungsankers für eine Teilhierarchie der Zertifizierungshierarchie nach SigI übernehmen werden.

Die Übermittlung und Prüfung neuer Wurzelzertifikate ist nicht Gegenstand dieses Teildokuments von SigI. Allerdings müssen die Benutzer mit SigI-konformen Prüffunktionen die Möglichkeit haben, den Inhalt und den Fingerprint von Wurzelzertifikaten festzustellen. Die Benutzer müssen sicherstellen, daß jeder Sicherungsanker mit Daten, die sie über einen vertrauenswürdigen Kanal erhalten, geprüft wird.

SigI-Konformitätsanforderungen

Für die Prüffunktion nach SigI werden unverknüpfte Selbstzertifikate der Wurzel-Zertifizierungsinstanz angenommen. Daher MÜSSEN SigI-konforme Prüffunktionen eine Liste von unabhängigen Wurzelzertifikaten verwalten können. Sie müssen Funktionen anbieten, mit der diese Liste vom Benutzer verwaltet werden kann. SigI-konforme Prüffunktionen MÜSSEN so gestaltet sein, daß Wurzelzertifikate nur mit Zustimmung des Benutzers in die Liste aufgenommen werden. Hinweise zu Prüfbedingungen für Erstprüfung von Wurzelzertifikaten werden in Kapitel 5 gegeben.

SigI-konforme Prüffunktionen MÜSSEN sicherstellen, daß jede Zertifikatkette in einem Wurzelzertifikat der RegTP endet, das in der Liste der Wurzelzertifikate enthalten ist. Wann diese Bedingung gefordert ist, wird in Kapitel 5 spezifiziert.

4.5 Zeitbezogene Statusprüfungen für Prüfschlüssel

Mit Statusprüfungen wird für ein Prüfobjekt festgestellt, ob

- der Signaturzeitpunkt im Gültigkeitszeitraum des Zertifikats liegt, in dem der Prüfschlüssels enthalten ist. Die erforderlichen Statusinformationen sind durch die Angaben zum Gültigkeitszeitraum statisch im Zertifikat enthalten.
- das Zertifikat zum Signaturzeitpunkt vorhanden und bereits freigegeben war. Die erforderlichen Vorhandenseinsinformationen können über eine Verzeichnisdienstauskunft abgefragt werden.
- das Zertifikat zum Signaturzeitpunkt gesperrt war. Die erforderlichen Sperrinformationen können über eine Verzeichnisdienstauskunft oder eine Sperrliste beschafft werden.

Alle zeitbezogenen Statusprüfungen beziehen sich auf das Zertifikat, das den Prüfschlüssel enthält. Dieses Kapitel stellt daher nur die Grundlagen der zeitbezogenen Statusprüfungen dar. Außerdem werden einige funktionale Voraussetzungen SigI-konformer Prüffunktionen formuliert. Die zeitbezogenen Prüfbedingungen werden dagegen in Kapitel 5.3 spezifiziert.

4.5.1 Grundlagen der zeitbezogenen Statusprüfungen

Damit eine Signatur als technisch gültig akzeptiert wird, muß auch überprüft werden, ob der Erzeugungszeitpunkt zulässig ist. Für die technische Bewertung des Signaturzeitpunktes eines Prüfobjekts wird gefragt, ob eine Zeitangabe in einen zulässigen Zeitraum fällt. Dieser Zeitraum wird zunächst statisch bestimmt durch den Gültigkeitszeitraum, der im Zertifikat angegeben ist. Durch zusätzliche Maßnahmen kann das Zertifikat gegenüber dem Gültigkeitsbeginn zu einem späteren Zertifikat freigegeben und gegenüber dem Gültigkeitsende zu einen früheren Zeitpunkt gesperrt werden.

Für die Statusprüfungen ist zum ersten der Signaturzeitpunkt notwendig, bezüglich dessen die Prüfbedingungen auszuwerten sind. Zum zweiten müssen die Statusinformationen des

Zertifikats vorliegen, gegen die geprüft werden muß. Drittens muß eine Prüfpolicy festgelegt werden, die durch die zeitbezogenen Prüfbedingungen abzubilden ist.

Authentizität und Wahl des Signaturzeitpunktes

Für die Zeitangaben in Prüfobjekten müssen unterschiedliche Annahmen zur Authentizität getroffen werden. Die Regeln zur Wahl des Signaturzeitpunktes können das Prüfergebnis beeinflussen, weil das Zertifikat eines Prüfschlüssels für verschiedene Signaturzeitpunkte einen unterschiedlichen Status aufweisen kann.

Quellen für Statusinformationen

Gültigkeitszeiträume sind in Zertifikaten enthalten. Sie müssen daher nicht extra beschafft werden.

Anders ist dies für die Vorhandenseins- und Sperrinformationen. Für sie stehen die Quellen nach Tabelle 1 zur Verfügung.

Statusinformation	Verzeichnisdienst-auskunft	Sperrliste
Sperrinformation	ja	ja
Vorhandenseinsinformation	ja	nein

Tabelle 1: Quellen für Statusinformationen zum Vorhandensein und zur Sperrung

Bewertungsregeln

Für die Bewertung des Signaturzeitpunktes bezüglich der Statusinformationen eines Zertifikates können unterschiedliche Bewertungsregeln herangezogen werden. Diese Bewertungsregeln hängen ab von:

- den zur Verfügung stehenden *Zeitangaben* und den Annahmen zu ihrer *Authentizität*: Welche Zeitangaben stehen als Input für die Prüfung zur Verfügung? Welche Zeitangaben in Prüfobjekten sind authentisch? Auf welche Tatbestände kann daraus geschlossen werden?
- dem zugrundegelegten *Gültigkeitsmodell für Gültigkeitszeiträume:* Wird Zertifizierungspfad-Gültigkeit oder Zertifikat-Gültigkeit gefordert?
- dem *Vergabekonzept der Gültigkeitszeiträume* durch die Zertifizierungsinstanzen,
- der *Gültigkeitspolicy:* Welche Konsistenzbedingungen und Interpretationsregeln werden im Rahmen des jeweiligen Gültigkeitsmodells gefordert?
- dem Konzept *Schlüsselwechsel und Zertifikatwechsel von Zertifizierungsinstanzen* in der Sicherungsinfrastruktur*:* Zu welchen Zeitpunkten und mit welchen Gültigkeitsrelationen sollen Schlüssel und Zertifikate der Zertifizierungsinstanzen gewechselt werden?
- der *Interpretation von Vorhandenseinsinformationen:* ist der Zeitpunkt der Freigabe relevant oder nicht?
- der *Interpretation von Sperrungen* für nachfolgende Zertifikate: wird der nachfolgende Teilbaum implizit mitgesperrt oder nicht? Haben verschiedene Sperrgründe unterschiedliche Reichweiten?

Dieser Gestaltungsraum wird durch diese Spezifikation auf ausgewählte Lösungen eingegrenzt.

4.5.2 Authentizität und Wahl des Signaturzeitpunktes

Der Zeitpunkt, zu dem eine Signatur tatsächlich erzeugt wurde, wird als *objektiver Signaturzeitpunkt* bezeichnet. Er kann nur unter bestimmten Bedingungen und nur im Rahmen der technisch realisierbaren Genauigkeit durch einen Prüfenden beweissicher nachvollzogen

werden, z. B. mit einer unmittelbar auf die Signaturerzeugung folgenden Erzeugung eines Zeitstempels. Da der objektive Signaturzeitpunkt vom Prüfenden in der Regel nicht mit Sicherheit festgestellt werden kann, muß er eine Annahme auf der Basis der ihm vorliegenden Informationen treffen. Statt des objektiven Signaturzeitpunktes wird daher im Prüfprozeß von einem *angenommenen* Erzeugungszeitpunkt als Signaturzeitpunkt ausgegangen.

Damit aus der Prüfung des Erzeugungszeitpunkts einer digitalen Signatur gegenüber dem Gültigkeitszeitraum des korrespondierenden Zertifikats und Vorhandenseins- und Sperrinformationen eine verwertbare Aussage abgeleitet werden kann, muß für den Erzeugungszeitpunkt eine ausreichend authentische Zeitangabe zur Verfügung stehen. Die Zeitangaben in den verschiedenen Prüfobjekten weisen allerdings eine unterschiedliche Qualität auf. Der für die Prüfung anzunehmende Signaturzeitpunkt unterscheidet sich daher je nach vorliegendem Prüfobjekt und Kontextbedingungen. An dieser Stelle werden die grundlegenden Regeln erläutert, nach denen der Signaturzeitpunkt (t_{sig}) eines Prüfobjekts zu wählen ist. Die genauen Auswahl- und Prüfregeln werden im Kapitel 5 dargestellt.

Zur Prüfung werden vorrangig solche Zeitangaben herangezogen, die als authentisch anzusehen und durch Signatur gegen Veränderung gesichert sind. Falls für das Primärdokument kein Zeitstempel zur Verfügung steht, kann der Prüfende Zeitangaben verwenden, die ihm als gesichert bekannt sind. Wenn er sichergehen will, daß eine digitale Signatur nicht rückdatiert wurde, kann er die Prüfung auf den *Eingangszeitpunkt* des digital signierten Dokuments abstellen. Um zu einem späteren Zeitpunkt false reject oder false accept Fälle zu vermeiden, ist es sinnvoll, in Wiederholungsprüfungen auf den *Zeitpunkt der Erstprüfung* abzustellen.

Grundsätzlich ist es sinnvoll, den objektiven Signaturzeitpunkt für die Prüfung heranzuziehen. Da der Prüfende diesen nur bedingt feststellen kann, muß er von Annahmen für den Erzeugungszeitpunkt einer digitalen Signatur ausgehen:

- Für die Zeitangaben *innerhalb des Primärdokuments* hat der Prüfende im allgemeinen keine Zusicherungen, da diese Zeitangaben vom Signierenden bestimmt werden können. Insbesondere könnte gegebenenfalls ein Angreifer versucht haben, einen gegebenenfalls im Dokument angegebenen Erzeugungszeitpunkt (**signingTime**) rückzudatieren, um eine Sperrung oder ein Gültigkeitsende des Zertifikats zu unterlaufen. Gemäß der folgenden Annahmen kann der Prüfende aber auf einen Zeitstempel zurückgreifen, falls dieser mitgeliefert wird. Andernfalls ist ein für ihn sinnvoller Zeitpunkt der Eingangszeitpunkt des digital signierten Dokuments oder der Zeitpunkt der Erstprüfung.
- Zertifizierungsstellen genießen ein implizites Vertrauen, stets korrekt Zeitangaben zu verwenden. Für Zeitangaben, die von Zertifizierungsstellen für Signaturerzeugungen angegeben werden, kann der Prüfende daher annehmen, daß die Zeitangabe authentisch ist. Authentisch meint in diesem Fall, daß die Angabe nur im Sekundenbereich vom objektiven Signaturzeitpunkt abweicht. In diesem Fall kann die Zeitangabe aus dem jeweiligen Prüfobjekt als Signaturzeitpunkt für die Prüfung herangezogen werden.

Für die Zeitangaben von Zertifizierungsstellen ergeben sich damit folgenden Regeln:

R8) Das BSI setzt voraus, daß Zertifizierungsstellen für die folgenden Attribute im oben beschrieben Sinn authentische Zeitangaben eintragen. Der Signaturzeitpunkt wird eingetragen in Zertifikaten und Attribut-Zertifikaten in "**dateOfCertGen**" [BSI-ZERT], in Zeitstempeln in "**tstTime**"; in Verzeichnisdienstauskünften in "**producedAt**" und in Sperrlisten und Zertifikatlisten in "**thisUpdate**". Diese Bedingungen sind durch das Sicherheitskonzept und die relevanten Technikkomponenten mit einem hohen Sicherheitsniveau durchzusetzen.

R9) Das Ende der Zertifikatkette bildet das Wurzelzertifikat. Für diesen Schlüssel liegt ein Selbstzertifikat $Zert_{RegTP}$ mit Gültigkeitszeitraum vor. Der Erzeugungszeitpunkt muß gegebenenfalls im Rahmen der Übernahme dieses Zertifikats in die Menge der Wurzelzertifikate geprüft werden. Diese Prüfung muß über andere Mechanismen, z. B. per Augenschein, erfolgen und ist nicht Gegenstand dieses Teildokuments von SigI.

SigI-Konformitätsanforderungen

Die Auswahl des Signaturzeitpunktes wird für die verschiedenen Prüfobjekte in Kapitel 5 spezifiziert

4.5.3 Prüfung des Gültigkeitszeitraums des Prüfschlüssels nach SigI

4.5.3.1 Gültigkeitsmodell

Für die Zulässigkeit des Erzeugungszeitpunktes einer digitalen Signatur wird im Rahmen dieser Spezifikation als Gültigkeitsmodell "Zertifikat-Gültigkeit" festgelegt.

R10) Unter der Gültigkeitsregel *Zertifikat-Gültigkeit* ist ein Signaturzeitpunkt genau dann technisch gültig, wenn er im Gültigkeitszeitraum des bestätigenden Zertifikats liegt. Die Kette der Zertifikate ist gültig, wenn jedes Zertifikat [$Zert_i$] im Gültigkeitszeitraum des übergeordneten Zertifikats [$Zert_{i-1}$] ausgestellt wurde.

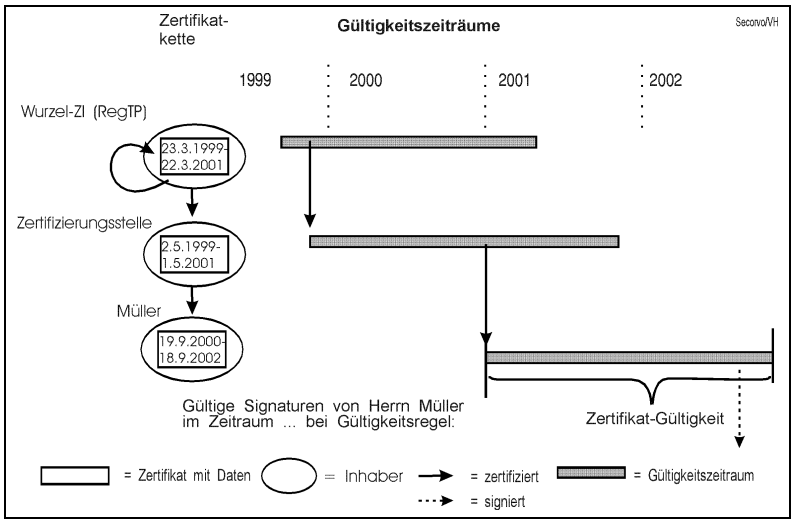

Abb. 1: Für Zertifikat-Gültigkeit muß jede Signatur im Gültigkeitszeitraum des jeweils bestätigenden Zertifikats liegen.

SigI-Konformitätsanforderungen

Die Prüfbedingungen für die Prüfung des Gültigkeitszeitraums werden in Kapitel 5 definiert.

4.5.3.2 Vergabekonzepte für Gültigkeitszeiträume für Zertifikate und Attribut-Zertifikate

In einem Vergabekonzept für Gültigkeitszeiträume werden die zulässigen Werte für Gültigkeitszeiträume in Zertifikaten festgelegt. Aus diesen Regeln können Prüfbedingungen oder

Anforderungen an Zertifizierungsstellen abgeleitet werden. Im Rahmen dieser Spezifikation werden folgende Regeln angenommen:

R11) Zertifikate mit rückdatiertem Gültigkeitsbeginn sind nicht zulässig. Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingung durch das Sicherheitskonzept und die Technikausstattung mit einem hohen Sicherheitsniveau durchgesetzt wird. Dadurch soll es Angreifern erschwert werden, rückdatierte Zertifikate auszustellen.

R12) Zertifikate mit vordatiertem Gültigkeitsbeginn sind zulässig. Das BSI setzt voraus, daß die Zertifizierungsstellen auch für vordatierte Zertifikate sicherstellen, daß der Gültigkeitszeitraum den Zeitraum der Eignung von Algorithmus und Schlüssellänge nicht überschreitet. Diese Bedingung ist durch das Sicherheitskonzept von Zertifizierungsstellen mit einem hohen Sicherheitsniveau durchzusetzen.

R13) Zertifizierungsstellen dürfen Zertifikate erst ab Gültigkeitsbeginn ihres Zertifikats zum Zertifizierungsstellen-Schlüssel ausstellen. Daraus folgt auch, daß der früheste Gültigkeitsbeginn eines nachgeordneten Zertifikats nach dem Gültigkeitsbeginn des übergeordneten Zertifikats liegen muß. Das BSI setzt voraus, daß die Zertifizierungsstellen diese Forderungen auch dann mit einem hohen Sicherheitsniveau sicherstellen, wenn sie Inhaber vordatierter Zertifikate sind.

R14) Zertifikate mit vordatiertem Gültigkeitsbeginn dürfen bereits vor dem Gültigkeitsbeginn gesperrt werden.

R15) Die maximale Gültigkeitsdauer (GD_{max}) von Zertifikaten und Attribut-Zertifikaten beträgt 5 Jahre (§ 7 SigV). Eine kürzere Gültigkeitsdauer ist zulässig (§ 7 SigV). Das BSI setzt voraus, daß Zertifizierungsstellen keine Zertifikate ausstellen, deren Gültigkeitsdauer > GD_{max} ist. Diese Bedingungen ist durch das Sicherheitskonzept der Zertifizierungsstellen mit einem hohen Sicherheitsniveau durchzusetzen.

R16) Attribut-Zertifikate sind nicht länger gültig als das Bezugszertifikat (§ 7 SigV). Das BSI setzt voraus, daß Zertifizierungsstellen keine Attribut-Zertifikate ausstellen, deren Gültigkeitsbeginn vor dem des Bezugszertifikats oder deren Gültigkeitsende nach dem des Bezugszertifikats liegt. Diese Bedingungen sind durch das Sicherheitskonzept der Zertifizierungsstellen mit einem hohen Sicherheitsniveau durchzusetzen.

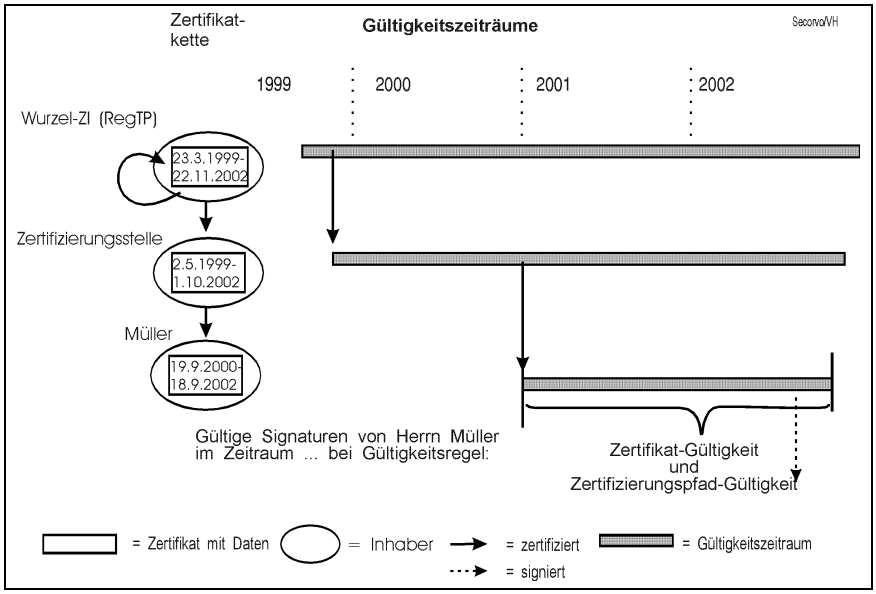

Abb. 2: Überdeckende Gültigkeitszeiträume nach dem Konzept der RegTP.

Für die Vergabe von Gültigkeitszeiträumen empfiehlt die RegTP, daß der Gültigkeitszeitraum des jeweils übergeordneten Zertifikats die Gültigkeitszeitraum aller nachgeordneten Zertifikate überdecken soll. Bei dieser Vergabestrategie für Gültigkeitszeiträume entspricht das Ergebnis einer Gültigkeitsprüfung nach dem Gültigkeitsmodell „Zertifikat-Gültigkeit“ dem Ergebnis einer Prüfung nach dem Gültigkeitsmodell „Zertifizierungspfad-Gültigkeit“, das beispielsweise in Sicherungsinfrastrukturen nach PEM oder PKIX verwendet wird. Diese Empfehlung hat keine jedoch Auswirkungen auf das Gültigkeitsmodell nach SigI und wird daher im Rahmen der technischen Signaturprüfung nach SigI nicht berücksichtigt.

SigI-Konformitätsanforderungen

Das Vergabekonzept für Gültigkeitszeiträume steht unter der Kontrolle der Zertifizierungsstellen. Die genannten Vorgaben werden nach der Annahme des BSI durch die Sicherungskonzepte und deren Überprüfungen durchgesetzt. SigI-konforme Prüffunktionen KÖNNEN DESHALB DAVON AUSGEHEN, daß die Vorgaben stets eingehalten werden und nicht geprüft werden müssen. Es entstehen daher keine weiteren Prüfbedingungen für technische Signaturprüfungen.

4.5.3.3 Schlüssel- und Zertifikatwechsel für Zertifizierungsinstanzen

Da nach Kapitel 4.2.1 die Zertifikatkette eindeutig rekonstruiert werden muß und dafür auch die technischen Voraussetzungen gegeben sind, haben Schlüssel- und Zertifikatwechsel keinen Einfluß auf die technische Signaturprüfung. Insbesondere werden abgelaufene Zertifikate in einer Zertifikatkette im Rahmen der technischen Signaturprüfung nach SigI nicht durch Verlängerungszertifikate ersetzt. Dies gilt auch für die Wurzelzertifikate, die im Rahmen der Prüfung verwendet werden.

SigI-Konformitätsanforderungen

Da die Zertifikatketten für technische Signaturprüfungen nach SigI eindeutig rekonstruiert werden, sind Schlüssel- und Zertifikatwechsel von Zertifizierungsinstanzen für die technische Signaturprüfung nach SigI nicht relevant. Es ergeben sich keine zusätzlichen Prüfbedingungen.

4.5.4 Vorhandenseinsprüfung von Zertifikaten

Das SigG sieht vor, daß Prüfende Zertifikate und Attribut-Zertifikate über öffentliche Telekommunikationsverbindungen jederzeit bei der Zertifizierungsstelle nachprüfen können.

Dabei erhalten sie eine Auskunft, ob das angefragte Zertifikat "vorhanden" ist (Vorhandenseinsinformation). Die Prüfung des Signaturzeitpunktes gegen die Vorhandenseinsinformation wird im weiteren als Vorhandenseinsprüfung bezeichnet.

Mit der Verzeichnisdienstauskunft erhält der Prüfende gleichzeitig auch den Sperrzeitpunkt, wenn das Zertifikat gesperrt wurde. Diese Information kann als Sperrinformation ausgewertet werden (vgl. unten). Verzeichnisdienstauskünfte haben daher eine Doppelfunktion für die Bereitstellung von Statusinformationen.

4.5.4.1 Interpretation von Vorhandenseinsinformationen

Mit der Vorhandenseinsprüfung soll überprüft werden, ob ein Zertifikat wirklich von einer Zertifizierungsstelle ausgestellt und für die Nutzung freigegeben wurde. Das Zertifikat ist vorhanden, wenn der Verzeichnisdienst für den angefragten Zeitpunkt das Vorhandensein (Wert von **certStatus** = "good") oder die Sperrung (**certStatus** = "revoked") zurückliefert.[19] Diese beiden Fälle werden als *positive Vorhandenseinsinformation* interpretiert. Sie sagen aus, daß das Zertifikat von der Zertifizierungsstelle ausgestellt wurde. Eine ablehnende Auskunft (Wert von **certStatus** = "unknown") sagt dagegen aus, daß das Zertifikat zum angefragten Zeitpunkt noch nicht freigeschaltet war oder nicht existiert.

Das BSI setzt voraus, daß in Zertifizierungsstellen die folgenden Bedingungen durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt werden:

R17) Rückwirkende Freigaben von Zertifikaten sind nicht zulässig.

R18) Freigaben von Zertifikaten werden in keinem Fall aufgehoben.

Für die Prüffunktion ergeben sich damit die folgenden Regeln:

R19) Aus der Information, daß ein Zertifikat zu einem Zeitpunkt vorhanden war, kann der Prüfende ableiten, daß es zu jedem Zeitpunkt nachher vorhanden ist.

R20) Aus der Information, daß ein Zertifikat zu einem Zeitpunkt "nicht vorhanden" war, kann der Prüfende ableiten, daß es zu jedem Zeitpunkt vorher ebenfalls "nicht vorhanden" war.

Der Prüfende kann sich jedoch nicht darauf verlassen, daß ein "nicht vorhandenes" Zertifikat nicht zu einem späteren Zeitpunkt freigeschaltet wird. Die Information "nicht vorhanden" bedeutet daher nicht zwingend einen Mißbrauchsfall.

4.5.4.2 Vorhandenseinsinformationen

Vorhandenseinsinformationen kann der Prüfende über Verzeichnisdienstauskünfte erhalten. Vorhandenseinsinformationen können sowohl für den Prüfzeitpunkt als auch für einen zurückliegenden Zeitpunkt abgefragt werden.

Eine Zusicherung für die Bereitstellung von Statusinformationen zum automatischen Abruf über Verzeichnisdienstauskünfte ergibt sich aus den Dokumentationspflichten für Zertifizierungsstellen nach SigG / SigV nur bis zum Ende der mathematischen Eignung der verwen-

19 Die beiden Tatbestände "wurde erzeugt" und "freigeschaltet" werden in Verzeichnisdienstauskünften nicht unterschieden. Positive Vorhandenseinsinformationen werden erst ab einer Freischaltung zurückgegeben.

deten Algorithmen.[20] Um hier eine einheitliche Vorgabe mit geringerer Komplexität zu erreichen, wird folgende Voraussetzung gefordert:

R21) Das BSI fordert von SigI-konformen Zertifizierungsstellen, daß sie Verzeichnisdienstauskünfte nach [BSI-DIR] mindestens für einen Zeitraum von 10 Jahren ab dem Ausstellungszeitpunkt bereitstellen, auch wenn die verwendeten Algorithmen zu diesem Zeitraum bereits ungeeignet sind. Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingung durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt wird.

In Zusammenhang mit der von der RegTP vorgesehene Vergabestrategie von Gültigkeitszeiträumen wird dadurch sichergestellt, daß automatische Verzeichnisdienstauskünfte zu allen Zertifikaten einer Zertifikatkette bis 5 Jahre nach Ende des Gültigkeitszeitraums des Teilnehmerzertifikats verfügbar sind.

Ob der Prüfende die Vorhandenseinsprüfung durchführt, obliegt seiner Entscheidung.

Verzeichnisdienstauskünfte müssen einer technischen Signaturprüfung unterworfen werden, um ihre Urheberschaft und Integrität sicherzustellen. Erst dann dürfen die enthaltenen Statusinformationen verwendet werden.

SigI-Konformitätsanforderungen

Konfigurationsmöglichkeiten der Prüffunktion:
SigI-konforme Prüffunktionen KÖNNEN die Möglichkeit bieten, Wurzelzertifikate, Zertifizierungsstellen-Zertifikate oder Teilnehmerzertifikate von der Vorhandenseinsprüfung auszunehmen. Die Konfigurationsmöglichkeiten sind so anzubieten, daß sie die zusätzlichen Risiken einer solchen Prüfpolicy erläutern.

Umfang der Vorhandenseinsinformation
SigI-konforme Prüffunktionen MÜSSEN so ausgelegt sein, daß sie für jedes Zertifikat, für das eine Vorhandenseinsprüfung konfiguriert ist, auch eine Vorhandenseinsprüfung durchführen.

Technische Signaturprüfung von Verzeichnisdienstauskünften
Diese Vorhandenseinsinformationen MÜSSEN von der Prüffunktion auf technische Korrektheit geprüft werden. Dies schließt rekursiv die Prüfung der Zertifikate und deren Vorhandenseinsinformationen ein, die die Signatur der Sperrinformation bestätigen. Verzeichnisdienstauskünfte, die nicht "technisch gültig" geprüft werden, werden als nicht vorhanden interpretiert.

Die detaillierten Prüfbedingungen für

- die technische Signaturprüfung von Verzeichnisdienstauskünften,
- die Bewertung der Eignung von Vorhandenseinsinformationen und
- die zeitbezogene Bewertung der Vorhandenseinsinformation im Rahmen der Statusprüfung

werden im Kapitel 5 spezifiziert.

---

20 Nach § 8 SigV müssen Zertifizierungsstellen die von ihnen ausgestellten Zertifikate mindestens für die Dauer der mathematischen Eignung der verwendeten Algorithmen abrufbar halten. Darüber hinaus muß die Dokumentation von ausgestellten Zertifikaten nach § 13 SigV zwar bis 35 Jahre nach Ausstellung aufbewahrt werden. Für diesen Zeitraum wird jedoch nur eine "Nachprüfung der Zertifikate [...] auf Antrag im Einzelfall" (§ 8 SigV) gefordert. Von einer technischen Unterstützung durch eine Verzeichnisdienst kann dann nicht mehr ausgegangen werden.

4.5.5 Prüfung des Sperrstatus

Das SigG sieht vor, daß Zertifikate und Attribut-Zertifikate gesperrt werden können. Sperrinformationen werden über Verzeichnisdienstauskünfte oder im Rahmen von SigI über Sperrlisten bereitgestellt (vgl. [BSI-DIR]).

4.5.5.1 Interpretation von Sperrungen

Um auf Veränderungen in der Realität gegenüber den Angaben in einem Zertifikat, auf Fehler oder auf Mißbrauch vor dem Auslaufen des Gültigkeitszeitraums reagieren zu können, können Zertifikate gesperrt werden. Sperrungen sind im Kontext des SigG wie folgt zu interpretieren:

- Zum einen sollen Sperrungen ab dem Sperrzeitpunkt gelten. Dadurch soll Mißbrauch durch eine künftige Verwendung eines Signatur- oder Zertifizierungsschlüssels unterbunden werden. Diese Anforderung wird so interpretiert, daß Signaturen, die vor einem Sperrzeitpunkt erzeugt wurden, hinsichtlich des Sperrstatus "technisch gültig" sind. Signaturen, die nach einem Sperrzeitpunkt erzeugt wurden, werden dagegen im Rahmen technischen Signaturprüfung abgelehnt.
- Zum zweiten dürfen gesperrte Zertifikate nicht wieder freigegeben werden (§ 9 SigV). Dadurch kann angenommen werden, daß ein zu einem späten Zeitpunkt nicht gesperrtes Zertifikat auch vorher nicht gesperrt war. Wenn ein Zertifikat bezüglich des Signaturzeitpunktes nicht gesperrt war, kann es nach dieser Vorgabe auch keinen vorherigen Zeitpunkt geben, zu dem es gesperrt war. Eine Sperrprüfung bezogen auf den Signaturzeitpunkt ist daher im Rahmen der technischen Gültigkeitsprüfung nach SigI ausreichend, um Signaturen zu erkennen, die durch ein gesperrtes Zertifikat bestätigt werden.

Das BSI setzt voraus, daß in Zertifizierungsstellen die folgenden Bedingungen durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt werden:

R22) Rückwirkende Sperrungen sind nicht zulässig (§ 8 (1) SigG).

R23) Sperrungen werden in keinem Fall aufgehoben (§ 9 SigV).

Für die Prüffunktion ergeben sich damit die folgenden Regeln:

R24) Aus der Information, daß ein Zertifikat zu einem Zeitpunkt nicht gesperrt war, kann der Prüfende ableiten, daß es zu keinem Zeitpunkt vorher gesperrt war.

R25) Aus der Information, daß ein Zertifikat zu einem Zeitpunkt gesperrt war, kann der Prüfende ableiten, daß es jedem Zeitpunkt nachher ebenfalls gesperrt ist.

Für die Interpretation von Sperrungen sind folgende Regeln anzuwenden:

R26) Die Sperrung eines Zertifizierungsstellen-Zertifikats wird genauso interpretiert, wie die eines Teilnehmerzertifikats. Sie führt insbesondere nicht zur Sperrung des gesamten nachgeordneten Teilbaums. Lediglich Zertifikate, die nach dem Sperrzeitpunkt ausgestellt wurden, werden als "technisch nicht gültig" bewertet.

R27) Sperrgründe werden bei der Auswertung von Sperrinformationen nicht berücksichtigt. Relevant für den Status eines Zertifikats "gesperrt" ist ausschließlich der Eintrag in der Sperrliste.

4.5.5.2 Sperrinformation

Sperrinformationen kann der Prüfende über Verzeichnisdienstauskünfte oder in Sperrlisten erhalten. Als "technisch gültig" geprüfte Verzeichnisdienstauskünfte garantieren eine Information über den Sperrstatus zum abgefragten Zeitpunkt, auch wenn dies der Prüfzeitpunkt

ist. Da Sperrlisten für einen Zeitraum gelten, ist diese Bedingung für den aktuellen Sperrstatus von Zertifikaten nur unmittelbar nach der Bereitstellung einer neuen Sperrliste erfüllt. Eine "tolerante" Prüfung mit höherer false accept Wahrscheinlichkeit kann allerdings zu einem geringerem Telekommunikationsaufwand führen. Auf welche Informationsquelle der Prüfende zurückgreift, obliegt seiner Entscheidung.

Sowohl Verzeichnisdienstauskünfte als auch Sperrlisten müssen einer technischen Signaturprüfung unterworfen werden, um die Urheberschaft und Integrität von Sperrinformationen sicherzustellen.

SigI-Konformitätsanforderungen

Konfigurationsmöglichkeiten der Prüffunktion:
SigI-konforme Prüffunktionen MÜSSEN die Möglichkeit bieten, als Quelle für Sperrinformationen "Verzeichnisdienstauskunft" oder "Sperrliste" voreinzustellen. Die Konfigurationsmöglichkeiten sind so anzubieten, daß sie nach den Ebenen der Zertifizierungshierarchie, Teilnehmerzertifikaten und Attribut-Zertifikaten unterschiedlich voreingestellt werden können. SigI-konforme Prüffunktionen KÖNNEN die Möglichkeit bieten, Zertifizierungsstellen-Zertifikate oder Wurzelzertifikate von der Sperrprüfung auszunehmen. Die Konfigurationsmöglichkeiten sind so anzubieten, daß sie die zusätzlichen Risiken einer solchen Prüfpolicy erläutern.

Umfang der Sperrinformationen
Für eine technische Signaturprüfung müssen Sperrinformationen für alle Prüfobjekte vorliegen, für die dies nach der Konfiguration gefordert ist.

Technische Signaturprüfung der Quelle von Sperrinformationen
Die Quellen für Sperrinformationen (Verzeichnisdienstauskunft, Sperrliste) MÜSSEN von der Prüffunktion auf technische Gültigkeit geprüft werden. Dies schließt rekursiv die Prüfung der Zertifikate und deren Sperrinformationen ein, die die Signatur der Sperrinformation bestätigen. Sperrlisten, die nicht "technisch gültig" geprüft werden, werden als nicht vorhanden interpretiert.

Die detaillierten Prüfbedingungen für

- die technische Signaturprüfung von Sperrlisten,
- die Bewertung der Eignung von Sperrinformationen und
- die zeitbezogene Bewertung der Sperrinformationen im Rahmen der Statusprüfung

werden im Kapitel 5 spezifiziert.

4.5.5.3 Umfang von Sperrlisten

Gemäß [BSI-DIR] werden Möglichkeiten zur Kennzeichnung von ARLs nicht unterstützt. Zertifizierungsstellen dürfen daher nur CRLs erzeugen, um das mißbräuchliche Unterschieben von ARLs auszuschließen. Die Seriennummern gesperrter Attribut-Zertifikate müssen ebenfalls in Sperrlisten gepflegt werden. Besondere Sperrlisten für Attribut-Zertifikate werden nach dieser Spezifikation nicht gefordert und unterstützt.

Für den Kontext von SigI werden die folgenden Vorgaben getroffen:

R28) Jede Zertifizierungsstelle darf jede Seriennummer nur einmal vergeben, unabhängig davon, ob sie einem Zertifizierungsstellen-Zertifikate, einem Teilnehmerzertifikate oder Attribut-Zertifikat zugeordnet wird.[21] Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingungen durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt wird. Damit können alle Zertifikate unabhängig von ihrem Typ eindeutig über Issuer und Seriennummer referenziert werden.

R29) Die "normale" CRL einer Zertifizierungsstelle enthält grundsätzlich die Seriennummern aller Typen von Zertifikaten (Zertifizierungsstellen-Zertifikate, Teilnehmerzertifikate und Attribut-Zertifikate), die gesperrt wurden.[22] Die Seriennummer eines gesperrten Zertifikats darf nach dem Gültigkeitsende des Zertifikats aus der CRL nur in Übereinstimmung mit den Regeln dieser Spezifikation entfernt werden. Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingungen durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt wird.

R30) Zertifizierungsstellen stellen sicher, daß sie nur CRLs bereitstellen. Die jeweils aktuelle CRL ist im X.500-Directory identisch in den beiden Attributen "**authorityRevocationList**" und "**certificateRevocationList**" im Directory-Eintrag der Zertifizierungsstelle abzulegen. Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingungen durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt wird.

Bereitstellungszeitraum von Sperrinformationen in Sperrlisten

Nach X.509 wird als Minimalanforderung für Sperreinträge nur gefordert, daß die Seriennummer eines gesperrten Zertifikats bis zum Ende seiner Gültigkeitsdauer in der Sperrliste geführt wird.[23] Um Sperrlisten im Gültigkeitsmodell "Zertifikat-Gültigkeit" effizient einsetzen zu können, ist eine längere Pflege der Zertifizierungsstellen-Zertifikate in Sperrlisten erforderlich.

R31) Die Seriennummern gesperrter Zertifizierungsstellen-Zertifikate werden in den zugehörigen Sperrlisten geführt, bis das Gültigkeitsende des letzten Zertifikats des nachgeordneten Teilbaums erreicht wurde. Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingung durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt wird.

4.5.6 Lokale Statusinformationen

Anfragen an den Verzeichnisdienst oder an ein Directory zur Abfrage von Verzeichnisdienstauskünften oder Sperrlisten sind nur notwendig, wenn die notwendigen Statusinformationen lokal nicht verfügbar sind.

Um aus der Sicherungsinfrastruktur abgefragte Statusinformationen wiederverwenden zu können, sollten SigI-konforme Prüffunktionen eine lokale Verwaltung von Statusinformationen unterstützen. Dazu muß im Prüfprozeß bewertet werden, ob die lokalen Statusinforma-

---

21 Eine "Zertifizierungsstelle" wird dabei durch den technischen Namen bestimmt, der im Feld **issuer** in den Zertifikaten angegeben wird. Nur so kann die Eindeutigkeit von Aussteller und Seriennummer für jedes Zertifikat erreicht werden. Werden einer Zertifizierungsstelle zwei unterschiedliche technische Namen zugeordnet, dann darf je Name jede Seriennummer einmal vergeben werden.

22 Ein abweichender Umfang kann z. B. für spezifische Sperrlisten oder für Distribution Points festgelegt werden. Solche Varianten werden hier jedoch nicht spezifiziert und von SigI-konformen Prüffunktionen nicht gefordert.

23 [ITU-T X.509 1997, Kap. 8].

tionen geeignet sind. Die in Kapitel 5 spezifizierten Prüfbedingungen berücksichtigen dieses Modell. Verzeichnisdienstauskünfte oder Sperrlisten werden in diesem Fall nur abgefragt, wenn lokal keine geeignete Information verfügbar ist (vgl. Abb. 3).

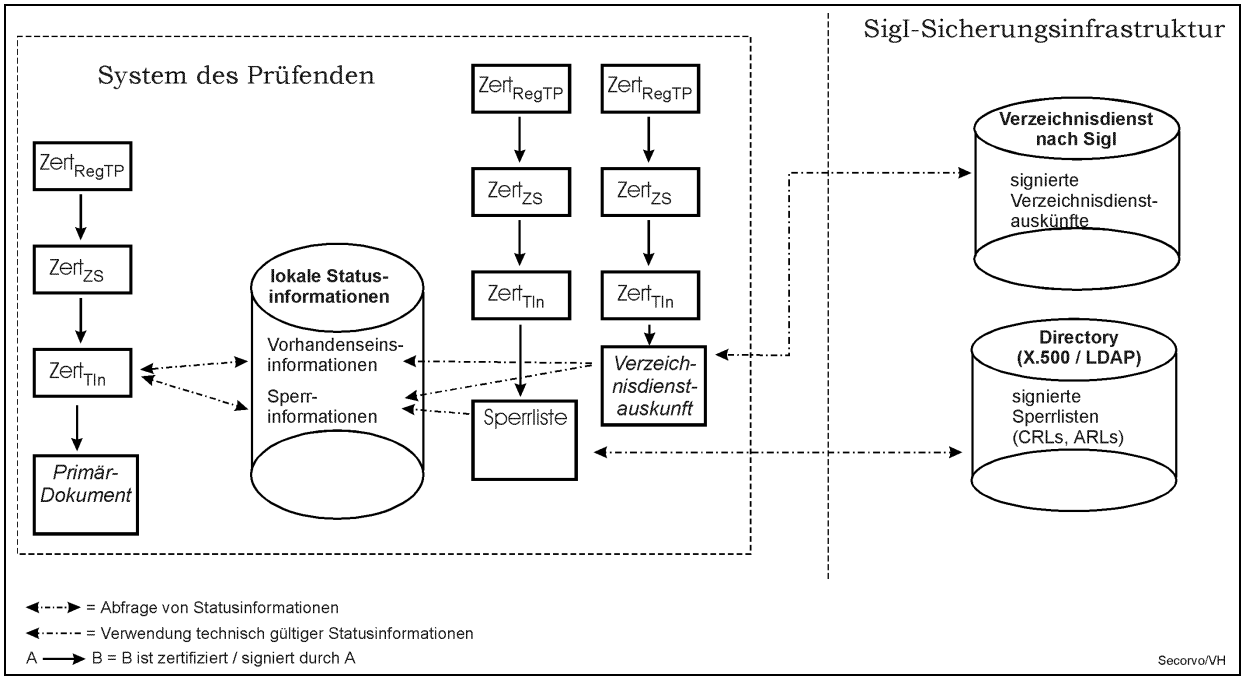

Abb. 3: Bereitstellung von Statusinformationen. In der Abbildung wird beispielhaft die Statusinformation des Teilnehmerzertifikats zum Primärdokuments verwendet. Inhaber der Teilnehmerzertifikate zur Verzeichnisdienstauskunft und zur Sperrliste ist die Zertifizierungsstelle.

4.6 Zweck- und Autorisierungsprüfung von digital signierten Dokumenten

Digital signierte Dokumente können für einen bestimmten Zweck vorgesehen sein. Einige digital signierte Dokumente sollen auch nur dann als technisch gültig anerkannt werden, wenn sie von entsprechend autorisierten Schlüsselinhabern signiert wurden. Da sich die Prüfbedingungen der Prüftatbestände "Zweckprüfung" und "Autorisierungsprüfung" überschneiden, werden sie in diesem Kapitel zusammengefaßt.

4.6.1 Zweckprüfung

Für digital signierte Dokumente kann gefordert sein, daß sie für einen bestimmten Zweck erzeugt werden. Die Prüfung auf den Zweck eines digital signierten Dokuments ist notwendig, wenn der versehentliche oder mißbräuchliche Austausch von digital signierten Dokumenten verhindert werden soll. Die Prüfung des Zwecks ist beispielsweise für Sperrlisten oder Zeitstempel notwendig.

Für die Angabe des Zwecks stehen in digital signierten Dokumenten unterschiedliche Attribute zur Verfügung. Zur Kennzeichnung können dienen (soweit jeweils vorhanden):

- der OID, der den Datentyp des digital signierten Dokuments kennzeichnet,
- der Aufbau des jeweiligen digital signierten Dokuments,
- Zweckangaben im digital signierten Dokument, z. B. zur Unterscheidung von CRL und ARL,

- Zweckangaben des Zertifikates, das den Prüfschlüssel bestätigt, z. B. die Angabe im Attribut **keyUsage** oder **basicConstraints**.

SigI-Konformitätsanforderungen

Soweit ein Zweckprüfung gefordert ist, MÜSSEN SigI-konforme Prüffunktionen die Informationen über den Zweck eines digital signierten Dokuments aus den durch Signatur gesicherten Daten der Prüfobjekte entnehmen. Die Referenzinformation, gegen die geprüft werden muß, unterscheidet sich je nach den Prüfobjekt. Die Prüfbedingungen werden daher in Kapitel 5 spezifiziert.

4.6.2 Autorisierungsprüfung

Mit der Autorisierungsprüfung wird geprüft, ob ein Signierender im Rahmen des Gesamtkonzepts von SigI auch die Berechtigung hatte, eine bestimmte Signatur auszustellen, soweit eine solche Prüfung technisch möglich ist. Zwei Merkmale können dabei unterschieden werden. Zum einen ist zu prüfen, ob die Signatur unter Berücksichtigung von Nutzungsbeschränkungen technisch gültig ist. Zum zweiten kann geprüft werden, ob eine Signatur im Rahmen des Sicherungskonzepts von SigI autorisiert wurde (Policy-Prüfung).

4.6.2.1 Prüfung von Nutzungsbeschränkungen

In digital signierten Dokumenten können Nutzungsbeschränkungen angegeben werden. Der Prüfende muß in der Lage sein, diese Nutzungsbeschränkungen festzustellen und zu bewerten. Die Prüffunktion muß die Darstellung und Bewertung von Nutzungsbeschränkungen unterstützen. Für eine automatische Auswertung sind im Rahmen von SigI allerdings nur Nutzungsbeschränkungen relevant, die in Zertifikaten oder Attribut-Zertifikaten angegeben werden. Nur diese Daten sind auch durch die Signatur der jeweils ausstellenden Zertifizierungsstelle gegen Manipulation durch einen Angreifer oder den Schlüsselinhaber gesichert.

Für die Angabe von Nutzungsbeschränkungen und -erlaubnissen stehen in Zertifikaten und Attribut-Zertifikaten unterschiedliche Attribute zur Verfügung. Zur Kennzeichnung können dienen (soweit jeweils vorhanden, vgl. BSI-ZERT)

- **keyUsage**
- **extKeyUsage**
- **liabilityLimitationFlag** (Kennzeichnung einer Beschränkung über ein Attribut eines Attribut-Zertifikats)
- **procuration** (Vertretungsmacht)
- **admission** (Zulassung)
- **monetaryLimit** (Monetäre Beschränkung)
- **declarationOfMajority** (Volljährigkeit)
- **restriction** (Sonstige Einschränkungen)

SigI-konforme Prüffunktionen MÜSSEN die Informationen über Nutzungserlaubnisse und -beschränkungen eines digital signierten Dokuments aus den Zertifikaten der Prüfschlüssel und aus Attribut-Zertifikaten entnehmen. Die Verarbeitung der Attribute und Referenzinformationen, gegen die gegebenenfalls geprüft werden muß, unterscheidet sich je nach den Prüfobjekt. Die Prüfbedingungen werden daher in Kapitel 5 spezifiziert.

4.6.2.2 Prüfung der Policy-Angabe in Zertifikaten und Attribut-Zertifikaten

SigI-konforme Zertifikate werden im Attribut **certificatePolicies** gekennzeichnet. Diese Kennzeichnung drückt zunächst die Konformität zu den Vorgaben der Spezifikation von [BSI-ZERT] aus. Für Zertifizierungsstellen-Zertifikate kann ein Prüfender aber auch annehmen, daß damit die Berechtigung verbunden ist, SigI-konforme Zertifikate auszustellen.

Für die Wurzelzertifikate der RegTP wird eine Policy-Prüfung aus zwei Gründen nicht vorgesehen. Zum einen definiert die RegTP für ihre Selbstzertifikate die Inhalte selbst. Die Prüfung des Policy-Attributs würde damit keinen wesentlichen Sicherungsbeitrag schaffen. Zum zweiten sollte die Zahl gleichzeitig existierender Wurzelzertifikate gering gehalten werden. Da es erforderlich sein könnte, daß die RegTP Selbstzertifikate ohne oder mit anderer Policy-Angabe erzeugt, schafft der Verzicht auf die Policy-Prüfung für die RegTP größere Flexibilität.

SigI-Konformitätsanforderungen

Die Prüfbedingungen werden in Kapitel 5 spezifiziert.

5 Spezifische Prüfbedingungen

In diesem Kapitel werden spezifische Prüfbedingungen je Prüfobjekt beschrieben, die von SigI-konformen Prüffunktionen zusätzlich zu den Bedingungen nach Kapitel 4 geprüft werden müssen. Das Gesamtergebnis wird durch Verknüpfung aller Teilergebnisse für das Primärdokument nach Kapitel 3.4 gebildet.

Die Gliederung folgt der Reihenfolge Primärdokument, Prüfobjekt zweiter und Prüfobjekt dritter Ordnung. Für Zertifikate werden die allgemeinen Prüfbedingungen zusammenfassend dargestellt. Lediglich die jeweils besonderen Prüfbedingungen je Zertifikattyp werden in spezifischen Unterkapiteln spezifiziert.[24] Die Prüfbedingungen für Statusinformationen wurden aufgeteilt in die Prüfung der Eignung von Statusinformationen, die Prüfung von Verzeichnisdienstauskünften und die Prüfung von Sperrlisten. Diese Gliederung unterstützt das Konzept der lokalen Verwaltung aus Kapitel 4.

Soweit Prüfbedingungen tabellarisch angegeben werden, sind in der Regel nur die "negativen Fälle" (alle außer "tg") aufgeführt. In den Tabellen werden die Teilergebnisse in der Abkürzungsschreibweise angegeben.

5.1 Prüfbedingungen für das Primärdokument

5.1.1 Aufbau des Primärdokuments

SigI-Konformitätsanforderungen

Für den Aufbau des Primärdokuments sind die Prüfbedingungen nach Kapitel 4.1 zu überprüfen.

5.1.2 Mathematische Prüfung des Primärdokuments

SigI-Konformitätsanforderungen

Für die mathematische Prüfung des Primärdokuments sind die Prüfbedingungen nach Kapitel 4.2 zu überprüfen.

Wie dort beschrieben, ist als Teilnehmerzertifikat entweder das im Dokument enthaltene Zertifikat (**signedAttr.cert** in **signerInfo**) oder das über die Referenz (**signedAttr.crtRef** in **signerInfo**) adressierte Zertifikat zu verwenden. Ein dem Primärdokument beigefügtes Zertifikat, das nicht mitsigniert ist (im Feld **certificates**) darf für die Prüfung nur verwendet werden, wenn es in **crtRef** referenziert wurde.

Das Zertifikat, das den Prüfschlüssel enthalten soll,[25] wird im weiteren mit [$Zert_{Tln}$] bezeichnet.

24 Wie oben bereits gesagt, muß die Implementierung einer SigI-konformen Prüffunktion nicht dieser Strategie folgen. Relevant ist nur, daß je Zertifikattyp alle relevanten Prüfbedingungen im Prüfprozeß berücksichtigt werden.

25 Diese Annahme wird erst durch die mathematische Prüfung des Primärdokuments bestätigt.

5.1.3 Prüfung des Namens des Signierenden

SigI-Konformitätsanforderungen

Für die Prüfung des Namens des Signierenden bestehen keine Konsistenzbedingungen. Formale Prüfbedingungen für die technische Signaturprüfung von Primärdokumenten können daher im Rahmen von SigI nicht angegeben werden. SigI-konforme Prüffunktionen MÜSSEN den Namen des Signierenden des Primärdokuments im Rahmen des Gesamtergebnisses anzeigen. In dieser MELDUNGSERGÄNZUNG muß der Name des Signierenden aus $Zert_{TIn}$ verwendet werden.

Konfigurationsmöglichkeiten:
SigI-konforme Prüffunktionen MÜSSEN für die Meldungsergänzung folgende alternativen Konfigurationsmöglichkeiten anbieten:

- Anzeige von [$Zert_{TIn}$**.subject**] (im Format des technischen Namens, wie in [BSI-ZERT] spezifiziert),
- Anzeige von [$Zert_{TIn}$**.subjectAltName.otherName**] (im Format von **PersonalData**, wie in [BSI-ZERT] spezifiziert),
- Anzeige von [$Zert_{TIn}$**.subject**] und [$Zert_{TIn}$**.subjectAltName.otherName**]

Für die Anzeige von technischen Namen (**subject**) MÜSSEN SigI-konforme Prüffunktionen mindestens die folgenden Attributtypen nach [X.521] unterstützen:

- CommonName (CN),
- Surname (S)=Name,
- Titel (T),
- Serialnumber (SN),
- Street (ST),
- Locality (L),
- Organisation (O),
- OrganisationalUnit (OU) und
- Country (C).

Für die Anzeige von **PersonalData** MÜSSEN SigI-konforme Prüffunktionen alle nach [BSI-ZERT] für dieses Feld spezifizierten Attributtypen unterstützen. Wenn der dort enthaltene Name ein Pseudonym ist, MUSS in allen Anzeigevarianten als MELDUNGSERGÄNZUNG eine entsprechende Kennzeichnung erfolgen.

5.1.4 Signaturzeitpunkt

Für den Signaturzeitpunkt ist gefordert, daß er im Gültigkeitszeitraum des Teilnehmerzertifikats liegt. Außerdem muß dieses Zertifikat zum Signaturzeitpunkt vorhanden und ungesperrt sein. Zunächst muß jedoch je nach den vorliegenden Informationen und Präferenzen des Prüfenden der Signaturzeitpunkt, der zum Prüfen herangezogen werden soll (*angenommener Signaturzeitpunkt*), bestimmt werden.

5.1.4.1 Wahl des Signaturzeitpunktes

Für die Wahl des Signaturzeitpunktes des Primärdokuments stehen prinzipiell die in der folgenden Tabelle aufgeführten Zeitangaben im oder zum digital signierten Dokument zur Verfügung:

Attribut	Bedeutung und Authentizität	Quelle für die Information (beim Prüfenden), [Literaturverweis]
Erzeugungszeitpunkt der digitalen Signatur	vom Signierenden eingetragen, ohne besondere Maßnahmen keine Authentizität erzwungen	**signingTime** [BSI-SIG]
Zeitstempel	Erstellungszeitpunkt des Zeitstempels, Im Zeitstempel bestätigte Daten haben zum Erstellungszeitpunkt beim Zeitstempeldienst vorgelegen, Authentizität gemäß SigG gesichert.	**tstTime** [BSI-TSS]
Eingangszeitpunkt	Zeitpunkt, zum dem der Erklärungsempfänger ein digital signiertes Dokument erhalten hat.	lokal verwaltete Zeitangabe
Zeitpunkt der Erstprüfung	Zeitpunkt, zu dem der Erklärungsempfänger das digital signierte Dokument zum ersten Mal prüft	lokal verwaltete Zeitangabe
Prüfzeitpunkt	Zeitpunkt, zu dem ein Prüfender das digital signierte Dokument (aktuell) prüft.	aktuelle Systemzeit

Der angenommene Signaturzeitpunkt muß aus der Sicht des Prüfenden so bestimmt werden können, daß er seine Risiken im elektronischen Rechtsverkehr kontrolliert. Sofern kein Zeitstempel zur Verfügung steht, ist ein angenommener später Signaturzeitpunkt aus seiner Sicht mit geringeren Mißbrauchsmöglichkeiten behaftet, weil dadurch eine Signatur, die ein Angreifer mißbräuchlich vor einen Sperrzeitpunkt datiert hat, ausgeschlossen werden kann.

Der Prüfende sollte auf einen Zeitstempel zurückgreifen, wenn dem Primärdokument ein solcher beigefügt wurde. Falls kein Zeitstempel vorliegt, kann der Prüfende Zeitangaben heranziehen, deren Authentizität ihm bekannt ist. Je größer die Abweichung vom objektiven Signaturzeitpunkt ist, desto eher wird allerdings ein digital signiertes Dokument fälschlicherweise als "technisch nicht gültig" eingestuft (false reject Fall). Daher sollte er einen Zeitpunkt wählen, der möglichst nahe am objektiven Signaturzeitpunkt liegt. Wenn er sichergehen will, daß eine digitale Signatur nicht rückdatiert wurde, kann er die Prüfung auf den *Eingangszeitpunkt* oder notfalls den Prüfzeitpunkt abstellen. Falls eine Prüfung wiederholt wird, sollte die Möglichkeit bestehen, den *Zeitpunkt der Erstprüfung* erneut zu verwenden.

Optional kann der Prüfende auch auf den vom Signierenden angegebenen Signaturzeitpunkt zurückgreifen. Problematisch ist diese Wahl jedoch, weil der Signierende diese Zeitangabe selbst einträgt und deshalb auch rückdatieren kann. Wenn ein Angreifer den Signaturzeitpunkt vor einer Sperrung angibt, kann dadurch für den Prüfenden ein false accept Fall eintreten.

SigI-Konformitätsanforderungen "Konfiguration des Signaturzeitpunktes des Primärdokuments"

SigI-konforme Prüffunktionen MÜSSEN folgende Optionen bieten, mit denen die Wahl des angenommen Signaturzeitpunktes bestimmt wird. Der Prüfende kann voreinstellen, daß als Signaturzeitpunkt verwendet wird:

- der durch *Zeitstempel* bestätigte Zeitpunkt, falls dem Primärdokument ein technisch gültiger Zeitstempel zugeordnet ist.

- der *aktuelle Prüfzeitpunkt*, der aus einer Quelle für Zeitangaben des lokalen Systems abgefragt wird.
- ein *aktueller Zeitstempel*, der von der Prüffunktion zum Primärdokument beantragt wird. Der Abruf von neuen Zeitstempeln MUSS so konfiguriert werden können, daß er nur erfolgt, wenn noch kein Zeitstempel vorhanden oder dieser ungültig ist. Es SOLL eine Konfigurationsmöglichkeit vorgesehen werden, mit der ein neuer Zeitstempel für jedes neu geprüfte Dokument abgefragt wird.[26] Es MUSS eine Konfigurationsmöglichkeit vorgesehen werden, mit der der Benutzer die Anfrage von Fall zu Fall starten kann (halbautomatisch).
- ein vom Benutzer *anzugebender Zeitpunkt*. SigI-konforme Prüffunktionen KÖNNEN entsprechend der vorgenannten Alternativen einen Vorschlag für diesen Zeitpunkt machen, wenn sie die Quelle der Zeitangabe darstellen und erläutern.

SigI-konforme Prüffunktionen SOLLEN für die Wahl des Signaturzeitpunktes des Primärdokuments folgende zusätzliche Optionen bieten:

- den *Empfangszeitpunkt* des digital signierten Dokuments. Dazu ist eine entsprechende Unterstützung der lokalen Verwaltung von digital signierten Dokumenten notwendig (siehe auch unten).
- eine andere lokal verwaltete Zeitangabe, z. B. der Zeitpunkt der Erstprüfung.
- den *Signaturzeitpunkt im digital signierten Dokument*.

SigI-konforme Prüffunktionen SOLLEN die Möglichkeit bieten, bei der Konfiguration des Signaturzeitpunktes eine halbautomatische Abfolge für verschiedene Alternativen festzulegen. Falls ein Zeitstempel nicht bereits zu Beginn der Prüfung zur Verfügung steht, soll bei entsprechender Voreinstellung nach Bestätigung des Benutzers eine andere Option verwendet werden.

SigI-konforme Prüffunktionen MÜSSEN den Benutzer bei der Konfiguration auf die Konsequenzen der einzelnen Optionen für die Prüfergebnisse hinweisen.

SigI-Konformitätsanforderungen "*Bestimmung des Signaturzeitpunktes*"

t_{Sig}(Primärdokument) MUSS entsprechend der vom Prüfenden gewählte Option bestimmt werden. t_{Sig}(Primärdokument) wird für die zeitbezogenen Statusprüfungen des Teilnehmerzertifikats und eventuell vorhandener Attribut-Zertifikate verwendet (vgl. unten).

SigI-Konformitätsanforderungen "*Wahl eines alternativen Signaturzeitpunktes*"

Der Benutzer MUSS für jede Prüfung im Einzelfall entscheiden können, welchen Zeitpunkt er wählt. Die Anforderung ist ausreichend erfüllt, wenn er bei der Anzeige eines Prüfergebnisses eine zusätzliche Prüfung mit einem von der Voreinstellung abweichenden angenommenen Signaturzeitpunkt veranlassen kann.

5.1.4.2 Signaturzeitpunkt aus Zeitstempel

Die Vorgaben dieses Abschnittes sind anzuwenden, wenn t_{Sig}(Primärdokument) aus einem Zeitstempel bestimmt werden soll.

---

26 Diese Option bietet dem Prüfenden die Möglichkeit, den Prüfzeitpunkt als t_{sig}(Primärdokument) zu verwenden und gesichert festzuhalten. Soweit dies bisher zu übersehen ist, bietet ein zusätzlicher Zeitstempel aus der Sicht des SigG allerdings keinen Gewinn für eine Beweisführung. Der größere Abstand zum objektiven Signaturzeitpunkt führt dazu, daß "späte" Sperrungen berücksichtigt werden. Andererseits kann dies aber auch zu false reject Fällen führen.

Die Zeitangabe aus einem Zeitstempel kann nur als Signaturzeitpunkt angenommen werden, wenn der Zeitstempel technisch gültig ist und sich auf das Primärdokument bezieht. Die folgenden Prüfbedingungen gelten auch, wenn der Zeitstempel vom Prüfenden im Rahmen des Prüfprozesses selbst angefordert wird.

5.1.4.2.1 Technische Gültigkeit des Zeitstempels

Der Zeitstempel muß ein technisch gültiges digital signiertes Dokument sein und in der Sicherungsinfrastruktur von SigI ausgestellt worden sein. Fällt die Prüfung für den Zeitstempel negativ aus, kann aus Sicht der technischen Signaturprüfung der darin bestätigte Zeitpunkt nicht als gesichert für t_{sig} angenommen werden. Falls das Zwischenergebnis nicht "technisch gültig" lautet, können dem Benutzer Alternativen angeboten werden, um einen anderen Signaturzeitpunkt für die Prüfung auszuwählen.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Zwischenergebnis für den Zeitstempel	Verhalten bei [Zwischenergebnis]	Teilergebnis für das Primärdokument
	Durchführung der technische Signaturprüfung für das Prüfobjekt "Zeitstempel". Gefordert wird daß er gemäß der unten beschriebenen Prüfbedingungen "technisch gültig" ist und von einer Zertifizierungsstelle aus der Sicherungsinfrastruktur nach aus SigI ausgestellt wurde.	"tnp" oder "tng"	Zeitstempel wird als "nicht vorhanden" interpretiert. Gemäß der Vorgaben des letzten Abschnitts ist vom Benutzer die Wahl eines anderen Signaturzeitpunktes vorzugeben	Teilergebnis wird durch die Prüfung der neuen Quelle für t_{sig} ersetzt.
		mu	Bestätigung vom Benutzer anfordern, daß t_{sig} trotz "mu" aus dem Zeitstempel bestimmt werden soll oder daß ein anderer Zeitpunkt gewählt werden soll	mu; Teilergebnis wird ggf. durch die Prüfung der neuen Quelle für t_{sig} ersetzt.
		mso	Bestätigung vom Benutzer anfordern, daß t_{sig} trotz "mso" aus dem Zeitstempel bestimmt werden soll oder daß ein anderer Zeitpunkt gewählt werden soll.	mso; Teilergebnis wird ggf. durch die Prüfung der neuen Quelle für t_{sig} ersetzt.
		tg		tg
		kp		kp
		pake		pake

5.1.4.2.2 Bezug des Zeitstempels zum Primärdokument

Falls die Prüfung des Prüfobjekts "Zeitstempel" mit "tg" endet oder er bei "mu" oder "mso" durch Benutzerentscheidung weiterverwendet werden soll, muß der mathematische Bezug zwischen dem Zeitstempel und dem Primärdokument überprüft werden. Die Bedingung ist erfüllt, wenn der Hash-Wert im Zeitstempel und der Hash-Wert über das Primärdokument übereinstimmen. Dabei muß das Hash-Verfahren für die Prüfung verwendet werden, daß in **messageImprint.hashAlgorithm** in die Signatur des Zeitstempeldienstes eingeschlossen ist.[27] Das Hash-Verfahren muß außerdem zum Prüfzeitpunkt geeignet sein.

SigI-Konformitätsanforderungen "mathematische Korrektheit des Hash-Wertes"

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	messageImprint.hashAlgorithm ist auch in **digestAlgorithms** enthalten	nicht erfüllt (zwei Angaben zum Hash-Verfahren sind inkonsistent) => Zeitstempel wird als "nicht vorhanden" interpretiert. Gemäß der Vorgaben des letzten Abschnitts ist vom Benutzer die Wahl eines anderen Signaturzeitpunktes vorzugeben	tng; Teilergebnis wird ggf. durch die Prüfung der neuen Quelle für t_{sig} ersetzt.
	Hash(Primärdokument) = **messageImprint.hashedMessage**	nicht erfüllt => Zeitstempel wird als "nicht vorhanden" interpretiert. Gemäß der Vorgaben des letzten Abschnitts ist vom Benutzer die Wahl eines anderen Signaturzeitpunktes vorzugeben	tng; Teilergebnis wird ggf. durch die Prüfung der neuen Quelle für t_{sig} ersetzt.

SigI-Konformitätsanforderungen "Eignung des Hash-Verfahrens"

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Zwischenergebnis für das Hash-Verfahren	Verhalten bei [Zwischenergebnis]	Teilergebnis für das Primärdokument
	Hash-Verfahren aus **messageImprint.hashAlgorithm** ist zum Prüfzeitpunkt gemäß Kapitel 4 geeignet	tng	Zeitstempel wird als "nicht vorhanden" interpretiert. Gemäß der Vorgaben des letzten Abschnitts ist vom Benutzer die Wahl eines anderen Signaturzeitpunktes vorzugeben	Teilergebnis wird durch die Prüfung der neuen Quelle für t_{sig} bestimmt

27 Dieses Verfahren wird nur in **messageImprint.hashAlgorithm angegeben,** so daß dieses Attribut zunächst auszuwerten ist.

		mu	Bestätigung vom Benutzer anfordern, daß t_{sig} trotz "mu" aus dem Zeitstempel bestimmt werden soll oder daß ein anderer Zeitpunkt gewählt werden soll	mu; ggf. durch Prüfung der gewählten Variante
		tg		tg
		pake		pake

5.1.4.2.3 Bestimmen des Signaturzeitpunktes aus Zeitstempel

SigI-Konformitätsanforderungen

Sind die Prüfbedingungen für "Verwendung des Zeitstempels" erfüllt oder hat der Benutzer Warnhinweise entsprechend quittiert, wird t_{sig}(Primärdokument) durch **TSTInfo.tstTime** bestimmt.

Sind einem digital signierten Dokument mehrere technisch gültige Zeitstempel zugeordnet, wird der erste ("älteste") Zeitpunkt verwendet.[28] Dies gilt nicht, wenn der Benutzer "Abruf eines neuen Zeitstempels" voreingestellt hat oder durch manuellen Eingriff in den Prüfprozeß dieses Variante bestimmt hat. In diesen Fällen wird t_{sig}(Primärdokument) aus dem neu abgerufenen Zeitstempel bestimmt.

5.1.4.2.4 Abruf eines neuen Zeitstempels

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen müssen in der Lage sein, einen aktuellen Zeitstempel zum digital signierten Dokument zu beantragen, falls dem Dokument bisher kein Zeitstempel zugeordnet ist. Sie müssen diesen Zeitstempel dem digital signierten Dokument zuordnen können.

Für den neu abgerufenen Zeitstempel müssen die SigI-Konformitätsanforderungen "Signaturzeitpunkt aus Zeitstempel" einschließlich der mathematischen Korrelation zum Primärdokument überprüft werden, bevor tsig(Primärdokument) bestimmt wird.[29]

Zusätzlich MUSS geprüft werden, ob der Zeitstempel von der Stelle ausgestellt wurde, bei der er beantragt wurde und ob die "**nonce**" aus dem Antrag mit der "**nonce**" im Zeitstempel übereinstimmt.

Nr.	Prüfbedingung	Fall	Teilergebnis
	Zeitstempel von der gewünschten Stelle ausgestellt	nicht erfüllt	tng

28 Werden Kompromittierungsszenarien ausgeschlossen, ist dies der Zeitstempel, der am nächsten am objektiven Signaturzeitpunkt liegt.

29 Da der **msgImpring** in einem Zeitstempelantrag vom Antragsteller berechnet wird, genügt für die mathematische Korrelation, daß dieser **msgImprint** und das gewählte Hash-Verfahren auch im ausgestellten Zeitstempel enthalten ist. Der Hash-Wert des Primärdokuments muß in diesem Fall also nicht erneut bestimmt werden. Die übrigen Prüfbedingungen müssen jedoch sichergestellt werden.

	Wert von **Nonce** im Zeitstempel stimmt mit dem Wert von **Nonce** im Antrag überein	nicht erfüllt	tng

SigI-konforme Prüffunktionen SOLLEN die Möglichkeit bieten, einen neu abgerufenen Zeitstempel, der den genannten Bedingungen genügt, mit dem Primärdokument abzuspeichern.

5.1.4.3 Lokal verwaltetet Zeitpunkte

Im Kontext von Telekooperation kann der Erklärungsempfänger vermuten, daß die digitale Signatur in zeitlicher Nähe zum Eingang des in seinen Herrschaftsbereich erzeugt wurde. Ersatzweise, allerdings mit größerer zeitlicher Abweichung, könnte er als angenommenen Signaturzeitpunkt auch den aktuellen Prüfzeitpunkt heranziehen. Im Rahmen der lokalen Anwendung können auch weitere Verfahren eingesetzt werden, um den angenommenen Signaturzeitpunkt für das Primärdokument zu bestimmen. Schließlich wird es bei wiederholter Prüfung eines digital signierten Dokuments häufig sinnvoll sein, auf den Zeitpunkt der Erstprüfung als angenommenen Signaturzeitpunkt zurückzugreifen,[30] wenn nicht der Signaturzeitpunkt selbst Gegenstand der Prüfung ist. *Soll beweissicher nachgewiesen werden, daß das digital signierte Dokument zum Zeitpunkt der Erstprüfung vorlag, muß ein Zeitstempel zum Dokument zur Verfügung stehen oder ein neuer abgefragt werden, auf den bei wiederholten Signaturprüfungen zurückgegriffen werden sollte.*

Anforderungen an die lokale Anwendung

Der angenommene Signaturzeitpunkt für die erste technische Gültigkeitsprüfung in der jeweiligen Umgebung ist als "Zeitpunkt der Erstprüfung" anzusehen.

Es ist Aufgabe der lokalen Anwendungen, die Speicherung eines Eingangszeitpunkts oder eines Zeitpunktes der Erstprüfung zu einem Primärdokument zu unterstützen. Die lokale Verwaltung von Zeitangaben MUSS sicherzustellen, daß vom Prüfenden keine ungesicherten Zeitangaben aus dem Herrschaftsbereich eines anderen Anwenders (von Dritten) als Eingangszeitpunkt oder Zeitpunkt der Erstprüfung verwendet werden, sofern der Benutzer dies nicht ausdrücklich will. Sollen Zeitangaben Dritter aufbewahrt werden, MUSS sichergestellt werden, daß der Prüfende zur Bestimmung des t_{sig}(Primärdokument) Zeitangaben aus seinem Herrschaftsbereich verwendet oder im Prüfprozeß der Verwendung von Zeitangaben Dritter zustimmt und dies im Gesamtergebnis geeignet feststellen kann. Diese funktionalen Anforderungen sind nicht Bestandteil der SigI-Konformitätsanforderungen für Prüffunktionen, da sie nur anwendungsspezifisch realisiert werden können.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen SOLLEN die Möglichkeit bieten, gemäß den oben beschriebenen Konfigurationsmöglichkeiten durch den Benutzer einen Eingangszeitpunkt, den Prüfzeitpunkt oder eine andere lokal verwaltete Zeitangabe aus der lokalen Anwendung abzufragen und zu verwenden.

30 Die Wiederverwendung lokaler Zeitangaben kann beispielsweise innerhalb eines Workflow-Systems sinnvoll sein, wenn an verschiedenen Arbeitsplätzen das von extern eingegangene digital signierte Dokument auf den Eingangszeitpunkt geprüft werden soll. Die Abstimmung einer solchen Vorgehensweise mit einem lokalen Sicherheitskonzept ist nicht Gegenstand dieser Spezifikation.

Wenn eine solche Zeitangabe zur Verfügung steht und vom Benutzer als priorisiert konfiguriert wurde, ist t_{sig}(Primärdokument) durch die entsprechende Zeitangabe zu bestimmen. Sofern eine solche Zeitangabe nicht zur Verfügung steht, MÜSSEN SigI-konforme Prüffunktionen dem Benutzer vorschlagen, als t_{sig}(Primärdokument) den Prüfzeitpunkt (aktuelle Systemzeit) zu verwenden.

Damit ergibt sich für die Wahl eines lokalen t_{sig}(Primärdokument) folgende Funktionalität der Prüffunktion:

Nr.	Prüfbedingung	Fall	Teilergebnis
	konfigurierte lokale Zeitquelle steht zur Verfügung	erfüllt	tg
		nicht erfüllt, aber Benutzer bestätigt einen anders gewählten t_{sig}(Primärdokument)	tg
		nicht erfüllt und Benutzer bricht ab	pake

Falls die Speicherung des Zeitpunktes der Erstprüfung von der lokalen Anwendung unterstützt wird, kann diese Zeitangabe von der Prüffunktion eingetragen werden. SigI-konforme Prüffunktionen SOLLEN daher die Möglichkeit bieten, im Falle der Prüfung anhand des Prüfzeitpunktes diesen als Zeitpunkt der Erstprüfung mit Hilfe der lokalen Anwendung abzuspeichern, falls dieser noch nicht mit einem Wert belegt ist.

Unabhängig von der Konfiguration zur "Abfrage neuer Zeitstempel" MÜSSEN SigI-konforme Prüffunktionen auch bei der Voreinstellung lokaler Zeitangaben die Möglichkeit bieten, für ein Primärdokument im Einzelfall einen Zeitstempel abzufragen. Die Anforderung ist ausreichend erfüllt, wenn der Benutzer bei der Anzeige eines Prüfergebnisses einen neuen Zeitstempel zum Primärdokument anfordern und speichern kann. Dabei MÜSSEN die Anforderungen bei "Abruf eines neuen Zeitstempels" eingehalten bzw. überprüft werden.

5.1.4.4 Signaturzeitpunkt bei Wiederholung der Signaturprüfungen

Zertifikate können auch nach der ersten Prüfung eines digital signierten Dokuments gesperrt werden oder auslaufen. Um ein mit der Erstprüfung vergleichbares Prüfergebnis zu erhalten, sollten Prüfungen sollten daher ebenfalls auf den bei der Erstprüfung verwendeten Zeitpunkt abgestellt werden. Andernfalls kann die zeitlichen Abweichung zwischen der Erzeugung der Signatur und der Prüfung sehr groß werden. Durch diese Abweichung können z. B. sowohl der Gültigkeitszeitraum von Zertifikaten überschritten als auch ein falscher Sperrstatus berücksichtigt werden und zu "false reject"-Fällen führen.

Eine weitere Abweichung in Prüfergebnissen ist möglich, wenn die Eignung von Algorithmen inzwischen anders bewertet wird.

Allerdings kann der Prüfende im Einzelfall auch feststellen wollen, wie das Prüfergebnis für ein digital signiertes Dokument mit einem anderen angenommen Signaturzeitpunkt lautet.

SigI-Konformitätsanforderungen "Wahl des Signaturzeitpunktes"

SigI-konforme Prüffunktionen SOLLEN bei wiederholten Signaturprüfungen den angenommenen Signaturzeitpunkt gemäß der vom Benutzer getroffenen Voreinstellung aus der Zeitangabe aus einem Zeitstempel oder einer lokalen Zeitangabe so ableiten, daß der in der Erstprüfung gewählte Zeitpunkt verwendet wird.

SigI-konforme Prüffunktionen MÜSSEN eine Möglichkeit bieten, um Prüfungen von Primärdokumenten mit der Angabe des anzunehmenden Signaturzeitpunktes anzustoßen.

SigI-Konformitätsanforderungen "Eignung der Algorithmen"

SigI-konforme Prüffunktionen SOLLEN bei wiederholten Signaturprüfungen in einer MELDUNGSERGÄNZUNG auf die zeitliche Differenz zwischen angenommenen Signaturzeitpunkt und Prüfzeitpunkt als Ursache für Teilergebnisse der Klassen "mu" oder "mso" hinweisen, falls sich die Eignung der Algorithmen in diesem Zeitraum geändert hat.

5.1.4.5 Ergebnis der Wahl des Signaturzeitpunktes

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN sicherstellen, daß nach Abschluß der Prüfungen des Kapitels 5.1.4.1 ein Signaturzeitpunkt t_{sig}(Primärdokument) gemäß der Vorgaben des Benutzers bestimmt oder die Prüfung des Primärdokuments abgebrochen wurde.

Transparenz:
SigI-konforme Prüffunktionen MÜSSEN im Gesamtergebnis den von der Prüffunktion für das Primärdokument bestimmten Signaturzeitpunkt darstellen. Die MELDUNGSERGÄNZUNG muß sowohl die Zeitangabe als auch die Quelle der Information, z. B. "aus Zeitstempel" oder "Eingangszeitpunkt", beinhalten.

5.1.5 Prüfung des Teilnehmerzertifikats

Mit der Prüfung des Teilnehmerzertifikats wird implizit die Prüfung der Zertifikatkette angestoßen. Daher ist eine zusätzliche explizite Prüfung der Zertifikatkette nicht erforderlich.

SigI-Konformitätsanforderungen

Das Zertifikat, in dem der Prüfschlüssel enthalten ist, muß ein Teilnehmerzertifikat sein. Die Statusprüfungen für das Teilnehmerzertifikat MÜSSEN auf den angenommenen Signaturzeitpunkt des Primärdokuments bezogen werden.

Nr.	Prüfbedingung	Fall	Teilergebnis
	[$Zert_{Tln}$] ist ein technisch gültiges Teilnehmerzertifikat aus der Zertifizierungshierarchie von SigI. Als Referenzzeitpunkt für die zeitbezogenen Statusprüfungen ist t_{sig}(Primärdokument) zu verwenden.		Zwischenergebnis für das Prüfobjekt

5.1.6 Zweck- und Autorisierungsprüfung

Die Anzeige von Beschränkungen und Berechtigungen aus dem Teilnehmerzertifikat wird beim Prüfobjekt "Teilnehmerzertifikat" beschrieben.

Zweck- und Autorisierungsinformationen zum Primärdokument können außer im Teilnehmerzertifikat auch in einem oder mehreren Attribut-Zertifikaten enthalten sein. Im Rahmen der Prüfung des Primärdokuments muß daher sichergestellt werden, daß:

- im Primärdokument enthaltene oder referenzierte Attribut-Zertifikate technisch gültig sind,

- zum Signaturzeitpunkt des Primärdokuments auch die zeitbezogenen Statusprüfungen von jedem enthaltenen Attribut-Zertifikat erfüllt werden,
- sich enthaltene Attribut-Zertifikate auf das Teilnehmerzertifikat beziehen und
- die Zweck- und Autorisierungsinformationen enthaltener oder referenzierter Attribut-Zertifikate angezeigt werden.

Anwendungsspezifische Prüfbedingungen für Attribut-Zertifikate sind nicht Gegenstand ist nicht Gegenstand dieses Teildokuments von SigI.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN *für jedes* im Primärdokument enthaltene oder referenzierte Attribut-Zertifikat die unten für dieses Prüfobjekt beschriebene technische Gültigkeitsprüfung durchführen. Jedes Zwischenergebnis für das Attribut-Zertifikat wird als Teilergebnis für Prüfung des Primärdokuments übernommen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	[$Zert_{Attr}$] ist ein technisch gültiges Attribut-Zertifikat aus der Zertifizierungshierarchie von SigI und referenziert [$Zert_{Tln}$]. Als Referenzzeitpunkt für die zeitbezogenen Statusprüfungen ist t_{sig}(Primärdokument) zu verwenden.		Zwischenergebnis für das Prüfobjekt

Die Anzeige von Beschränkungen und Berechtigungen aus dem Attribut-Zertifikat wird beim Prüfobjekt "Attribut-Zertifikat" beschrieben.

5.2 Prüfbedingungen für Zeitstempel

Ein Zeitstempel muß ein digital signiertes Dokument sein. Der Prüfschlüssel muß in einem zweckspezifischen Zertifikat für einen Zeitstempeldienst bestätigt werden. Das Zertifikat muß aus der Zertifizierungshierarchie nach SigI stammen.

5.2.1 Aufbau des Zeitstempels

SigI-Konformitätsanforderungen

Für den Aufbau des Zeitstempels sind die Prüfbedingungen nach Kapitel 4.1 zu überprüfen.

5.2.2 Mathematische Prüfung des Zeitstempels

SigI-Konformitätsanforderungen

Für die mathematische Prüfung des Zeitstempels sind die Prüfbedingungen nach Kapitel 4.2 zu überprüfen.

Wie dort beschrieben, ist als Teilnehmerzertifikat entweder das im Zeitstempel enthaltene Zertifikat (**signedAttr.cert** in **signerInfo**) oder das über die Referenz (**signedAttr.crtRef** in **signerInfo**) adressierte Zertifikat zu verwenden. Ein dem Zeitstempel beigefügtes Zertifikat, das nicht mitsigniert ist (im Feld **certificates**) darf für die Prüfung nur verwendet werden, wenn es in **crtRef** referenziert wurde.

Das Zertifikat, das den Prüfschlüssel enthalten soll,[31] wird im weiteren mit [$Zert_{TSS}$] bezeichnet.

5.2.3 Prüfung des Namens des Signierenden

Prinzipiell besteht für Zeitstempel nur die Anforderung, daß sie von einer Zertifizierungsstelle aus der Sicherungsinfrastruktur ausgestellt worden sein müssen. Besondere Bedingungen für den Namen des ausstellenden Instanz müssen nicht vorgegeben werden.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen SOLLEN bei selbst beantragten Zeitstempeln überprüfen, ob die ausstellende Zertifizierungsstelle mit der angefragten Zertifizierungsstelle übereinstimmt. Ist diese Bedingung nicht erfüllt, muß der Benutzer mit einer Fehlermeldung auf den Tatbestand hingewiesen werden. Ein Prüfprozeß unter Verwendung dieses Zeitstempels darf nur nach ausdrücklicher Bestätigung des Benutzers fortgesetzt werden.

5.2.4 Bestimmen des Signaturzeitpunktes

Für den Signaturzeitpunkt, zu dem der Zeitstempel erzeugt wurde, ist gefordert, daß er im Gültigkeitszeitraum des Teilnehmerzertifikats des Zeitstempeldienstes liegt. Außerdem muß dieses Zertifikat zum Signaturzeitpunkt vorhanden, gültig und ungesperrt sein.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN als Signaturzeitpunkt des Zeitstempels den Wert aus dem Attribut "**tstTime**" verwenden. Dieser Zeitpunkt wird im weiteren als t_{sig}(Zeitstempel) bezeichnet.

5.2.5 Prüfung des Teilnehmerzertifikats

Mit der Prüfung des Teilnehmerzertifikats der Zeitstempeldienstes wird implizit auch die Prüfung der Zertifikatkette angestoßen.

SigI-Konformitätsanforderungen

Das Zertifikat, in dem der Prüfschlüssel enthalten ist, muß ein Teilnehmerzertifikat für einen Zeitstempeldienst sein. Die Sperrprüfung und die Prüfung des Gültigkeitszeitraums müssen auf den Signaturzeitpunkt des Zeitstempels bezogen werden.

Nr.	Prüfbedingung	Fall	Teilergebnis
	[$Zert_{TSS}$] ist ein technisch gültiges Teilnehmerzertifikat aus der Zertifizierungshierarchie von SigI. Als Referenzzeitpunkt für die zeitbezogenen Statusprüfungen von [$Zert_{TSS}$] ist t_{sig}(Zeitstempel) zu verwenden. Das Zertifikat muß für einen Zeitstempeldienst ausgestellt sein.		Zwischenergebnis für das Prüfobjekt [$Zert_{TSS}$]

Die Prüfbedingungen für das Zertifikat sind in Kapitel 5.3 angegeben.

31 Diese Annahme wird erst durch die mathematische Prüfung des Primärdokuments bestätigt.

5.2.6 Zweck- und "Granted"-Prüfung für Zeitstempel

Zeitstempel können für unterschiedliche Zwecke ausgestellt werden. Für SigI-konforme Zeitstempel wird gefordert, daß sie als "gewährt" ("granted" Kennzeichnung) und unter der Policy von SigI ausgestellt wurden.

5.2.6.1 "Granted" Kennzeichnung

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	TSTInfo.status enthält den Wert "granted"	nicht erfüllt	tng

5.2.6.2 Policy-Prüfung für Zeitstempel

Da über unbekannte Policies keine Aussage getroffen werden kann, wird von Zeitstempeln SigI-Konformität gefordert.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	TSTInfo.policy enthält den Wert "Id-sigi-sigts-sigconform"	nicht erfüllt	tng

5.2.7 Bildung des Zwischenergebnisses

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN das Zwischenergebnis für die technische Gültigkeitsprüfung des Zeitstempels nach den Regeln für die Bildung eines Gesamtergebnisses zusammenfassen.

5.3 Prüfbedingungen für Zertifikate

Notationen

- Das Zertifikat, das aktuell Gegenstand der Prüfung ist (aktuelles Prüfobjekt), wird mit $[Zert_i]$ bezeichnet. Das zu $[Zert_i]$ übergeordnete Zertifikat wird mit $[Zert_{i-1}]$ bezeichnet.
- Der *Signaturzeitpunkt* $t_{sig}([Zert_i])$ bezeichnet den Zeitpunkt, zu dem $[Zert_i]$ erzeugt wurde.
- Als *Referenzzeitpunkt* t_{Ref} wird der Zeitpunkt bezeichnet, für den die Statusprüfungen für $[Zert_i]$ durchgeführt werden, zu dem also $[Zert_i]$ gültig und vorhanden sein muß und nicht gesperrt sein darf. Nur in diesem Fall wird eine mit dem in $[Zert_i]$ enthaltenen öffentlichen Schlüssel geprüfte Signatur, z. B. die eines Primärdokuments, als technisch gültig anerkannt. Der Begriff Referenzzeitpunkt wird zur Unterscheidung vom Signaturzeitpunkt $t_{sig}([Zert_i])$ verwendet. Der für die Prüfung zu verwendende Referenzzeitpunkt ergibt sich aus dem Signaturzeitpunkt des Prüfobjekts, das mit dem Prüfschlüssel aus $[Zert_i]$ ma-

thematisch geprüft wird. Der Signaturzeitpunkt von [$Zert_i$] wird dagegen für die Statusprüfungen des übergeordneten Zertifikats ([$Zert_{i-1}$]) herangezogen.

Das aktuelle Prüfobjekt [$Zert_i$] kann sowohl ein Teilnehmerzertifikat, ein Attribut-Zertifikat als auch ein Zertifizierungsstellen-Zertifikat sein.

Struktur der Darstellung

Die "allgemeinen Prüfbedingungen für Zertifikate" müssen von allen Zertifikaten, auch Attribut-Zertifikaten, mit Ausnahme von Wurzelzertifikaten erfüllt werden.

Spezifische Prüfbedingungen werden zusätzlich zu den "allgemeinen Prüfbedingungen für Zertifikate" für Attribut-Zertifikate angegeben.

Die Entscheidung über die Eigenschaft "zulässiges Wurzelzertifikat" wird alleine anhand der "spezifischen Prüfbedingungen für Wurzelzertifikat" getroffen. Hinweise zur "Erstprüfung von Wurzelzertifikaten" finden sich im Anhang.

Die "spezifischen Zweck- und Autorisierungsprüfungen" müssen für Zertifikate je nach Anwendungszweck des Prüfschlüssels und Zertifikattyps durchgeführt werden. Sie unterscheiden sich nach

- Teilnehmerzertifikaten für Endanwender und Attribut-Zertifikate
- Teilnehmerzertifikaten für Dienste von Zertifizierungsstellen und
- Zertifizierungsstellen-Zertifikaten.

5.3.1 Allgemeine Prüfbedingungen für Zertifikate

Die Prüfbedingungen dieses Abschnitts gelten für Teilnehmerzertifikate, Attribut-Zertifikate und Zertifizierungsstellen-Zertifikate. Für Wurzelzertifikate sind die Prüfbedingungen dieses Abschnitts nicht relevant. Für sie müssen die Prüfbedingungen aus Kapitel 5.3.6 angewandt werden.

5.3.1.1 Aufbau des Zertifikats

SigI-Konformitätsanforderungen

Für den Aufbau des Zertifikats sind die Prüfbedingungen nach Kapitel 4.1 zu überprüfen.

5.3.1.2 Mathematische Prüfung des Zertifikats und Terminierung der Zertifikatkette

Für die mathematische Prüfung des Zertifikats sind die Prüfbedingungen nach Kapitel 4.2 zu überprüfen. Zunächst muß jedoch das Zertifikat mit dem Prüfschlüssel bestimmt werden. für dieses Zertifikat ist die technische Gültigkeitsprüfung anzustoßen. An dieser Stelle werden außerdem die Prüfbedingungen angegeben, mit denen die Prüffunktion sicherstellt, daß die Forderung nach Terminierung der Zertifikatkette erfüllt ist.

5.3.1.2.1 Bestimmen des übergeordneten Zertifikats

Wie im Kapitel 4.2 beschrieben, ist in Zertifikaten und Attribut-Zertifikaten nach [BSI-ZERT] das Attribut "**authorityKeyIdentifier**" im Format Issuer und Seriennummer zu verwenden, um das übergeordnete Zertifikat mit dem Prüfschlüssel zu bestimmen. Dieses Zertifikat muß in allen Fällen ein Zertifizierungstellen-Zertifikat sein.

Das Zertifikat, das den Prüfschlüssel zum aktuell geprüften Zertifikat enthalten soll,[32] wird im weiteren mit [$Zert_{i-1}$] bezeichnet.

5.3.1.2.2 Terminierungsforderung für Zertifikatketten

In einer streng SigG-konformen Zertifizierungshierarchie darf in einer Zertifikatkette zwischen dem Wurzelzertifikat und einem Teilnehmerzertifikat höchstens ein Zertifizierungstellen-Zertifikat enthalten sein. Das aktuell geprüfte Zertifizierungstellen-Zertifikat kann aber bereits das Wurzelzertifikat sein, z. B. wenn ein Zertifikat für einen Zeitstempeldienst direkt von der RegTP ausgestellt wird.

SigI-Konformitätsanforderungen "Terminierung"

SigI-konforme Prüffunktionen MÜSSEN für die Terminierung der Zertifikatkette und die Prüfung des referenzierten Sicherungsankers das Zertifizierungsmodell des SigG beherrschen.

Nr.	Prüfbedingung	Fall	Teilergebnis und Verhalten
	Länge der Zertifikatkette ist SigG-konform und endet in Wurzelzertifikat	[$Zert_i$] ist ein Teilnehmerzertifikat oder ein Attribut-Zertifikat und [$Zert_{i-1}$] ist ein "technisch gültiges" Zertifizierungsstellen-Zertifikat aus SigI.	tg; die Prüfung von [$Zert_{i-1}$] wird angestoßen[33]
		[$Zert_i$] ist ein Teilnehmerzertifikat oder Attribut-Zertifikat und [$Zert_{i-1}$] ist ein Wurzelzertifikat gemäß der Bedingungen des Kapitels 5.3.6.[34]	tg
		[$Zert_i$] ist ein Zertifizierungstellen-Zertifikat und [$Zert_{i-1}$] ist ein Wurzelzertifikat gemäß der Bedingungen des Kapitels 5.3.6.	tg
		sonst	tng, außerdem wird die Prüfung dieser Zertifikatkette beendet

Die Entscheidung über die Eigenschaft "ist Wurzelzertifikat" fällt gemäß der in Kapitel 5.3.6 beschriebenen spezifischen Prüfbedingung.

SigI-konforme Prüffunktionen KÖNNEN die Prüfung der Terminierung von Zertifikatketten über das Attribut **pathLenConstraint** unterstützen. In diesem Fall sind die aufgeführten Prüfbedingungen geeignet zu ergänzen. Das Attribut **pathLenConstraint** darf nur in Zertifikaten

32 Diese Annahme wird erst durch die mathematische Prüfung des Primärdokuments bestätigt.

33 Siehe dazu unten.

34 Gemäß des Zertifizierungsmodells der RegTP entsteht diese Situation nur für Teilnehmerzertifikate, die von Diensten von Zertifizierungsstellen eingesetzt werden, z. B. zum Signieren von Verzeichnisdienstauskünften. Dazu gehören auch die Zertifikate für die Dienste der RegTP. Teilnehmerzertifikate für Endanwender sollen auf dieser Ebene nicht ausgestellt werden.

von Zertifizierungsstellen vorhanden sein. Von der Prüffunktion wird folgendes funktionales Verhalten gefordert:

Nr.	Prüfbedingung	Fall	Teilergebnis
	[$Zert_i$] ist ein Zertifizierungsstellen-Zertifikat. Falls **pathLenConstraint** im Zertifikat enthalten ist, dürfen zwischen dem aktuellen Zertifizierungsstellen-Zertifikat und dem Teilnehmerzertifikat maximal **pathLenConstraint** Zertifizierungsstellen-Zertifikate in der Kette enthalten sein.	mehr Zertifizierungsstellen-Zertifikate in der Zertifikatkette enthalten	tng
	Zertifikatkette endet in einem Wurzelzertifikat gemäß der Bedingungen des Kapitels 5.3.6	nicht erfüllt	tng

Um Angriffe zu erschweren, SOLLEN SigI-konforme Prüffunktionen, die die Terminierung mit **pathLenConstraint** unterstützen, sicherstellen, daß das Benutzer eine maximale Anzahl von Zertifikaten in einer Zertifikatkette konfigurieren kann, nach der die Prüfung abbrechen soll.

5.3.1.2.3 Mathematische Prüfung des Zertifikat-Authentikators

SigI-Konformitätsanforderungen

Für die mathematische Prüfung des Zertifikats sind die Prüfbedingungen nach Kapitel 4.2 zu überprüfen.

5.3.1.3 Prüfung des Namens des Signierenden

Für Zertifikate besteht die Anforderung, daß der distinguished name des Ausstellers gleich dem distinguished name des Inhabers des übergeordneten Zertifikats sein muß.

SigI-Konformitätsanforderungen

R32) Das BSI nimmt an, daß in der Zertifizierungshierarchie nach SigG nur Zertifikate ausgestellt werden, die die genannte Verkettung von **subject** und **issuer** aufweisen. Diese Bedingung ist durch das Sicherheitskonzept der Zertifizierungsstelle mit einem hohen Sicherheitsniveau durchzusetzen.

SigI-konforme Prüffunktionen KÖNNEN DESHALB DAVON AUSGEHEN, daß diese Prüfbedingung erfüllt ist, wenn die Zertifikatkette in einem Wurzelzertifikat der RegTP endet.

SigI-konforme Prüffunktionen KÖNNEN die Prüfung mit folgender Funktionalität durchführen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	issuer([$Zert_i$])=**subject**([$Zert_{i-1}$])	nicht erfüllt	tng

5.3.1.4 Bestimmen des Signaturzeitpunktes

[$Zert_i$] darf nur anerkannt werden, wenn der Signaturzeitpunkt, zu dem [$Zert_i$] erzeugt wurde, im Gültigkeitszeitraum von [$Zert_{i-1}$] liegt. Außerdem müssen die anderen Statusprüfungen für [$Zert_{i-1}$] zum Signaturzeitpunkt erfolgreich verlaufen.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN als Signaturzeitpunkt des Zertifikats [$Zert_i$] den Wert aus dem Attribut "**dateOfCertGen**" verwenden. Dieser Zeitpunkt wird im weiteren als $t_{sig}([Zert_i])$ bezeichnet.

5.3.1.5 Prüfung des übergeordneten Zertifizierungstellen-Zertifikats

Das Zertifikat, in dem der Prüfschlüssel zu [$Zert_i$] enthalten ist, muß nach dem Zertifizierungsmodell des SigG ein Zertifizierungstellen-Zertifikat sein. Die Prüfungen zur Terminierung und zum Sicherungsanker wurden bereits oben definiert.

Falls [$Zert_{i-1}$] als Wurzelzertifikat identifiziert wurde, müssen nur die Statusprüfungen für [$Zert_{i-1}$] zum Zeitpunkt $t_{sig}([Zert_i])$ durchgeführt werden.

Andernfalls muß eine volle technische Gültigkeitsprüfung für [$Zert_{i-1}$] erfolgen.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	[$Zert_{i-1}$] ist ein technisch gültiges Zertifizierungstellen-Zertifikat aus der Zertifizierungshierarchie von SigI. Als Referenzzeitpunkt für die zeitbezogenen Statusprüfungen von [$Zert_{i-1}$] ist t_{sig}([$Zert_i$]) zu verwenden.	[$Zert_{i-1}$] ist kein Wurzelzertifikat	Zwischenergebnis für das Prüfobjekt [$Zert_{i-1}$]
		[$Zert_{i-1}$] ist ein Wurzelzertifikat gemäß der Bedingungen des Kapitels 5.3.6	Zwischenergebnis für die Statusprüfungen gemäß Kapitels 5.3.6

Für die Prüfung von [$Zert_{i-1}$] sind die Prüfbedingungen dieses Kapitels anzuwenden.

5.3.1.6 Statusprüfungen

Das aktuelle Zertifikat [$Zert_i$] soll die Signatur eines nachgeordneten Prüfobjekts bestätigen. Dazu muß geprüft werden, ob der dort bestimmte Referenzzeitpunkt t_{Ref} für die zeitbezogenen Prüfungen:

- im Gültigkeitszeitraum des aktuell geprüften Zertifikats liegt,
- nach einem Vorhandenseinszeitpunkt des aktuell geprüften Zertifikats liegen und
- vor einem eventuellen Sperrzeitpunkt des aktuell geprüften Zertifikats liegen.

Es müssen nur solche Prüfungen durchgeführt werden, die vom Benutzer gemäß der Voreinstellung der Prüffunktion (vgl. Kapitel 4) gefordert sind.

Da Statusinformationen nur für einen bestimmten Zeitraum in den Diensten der Sicherungsinfrastruktur nach SigI gepflegt werden, ist nicht jede abgerufene Statusinformation für diese Prüfung geeignet. Die lokal vorliegenden oder abgerufenen Statusinformationen zu einem Zertifikat müssen daher zunächst auf ihre Eignung geprüft werden.[35] Die dazu notwendigen Prüfbedingungen sind in Kapitel 5.4 formuliert. Dort wird auch der Abruf von Statusinformationen und deren Prüfung angestoßen, falls dies notwendig ist.

5.3.1.6.1 Statusprüfung "Gültigkeitszeitraum"

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN für die Prüfung von t_{Ref} die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	$t_B([Zert_i]) < t_{Ref} < t_E([Zert_i])$	erfüllt	tg
		nicht erfüllt	tng

35 Nicht zu verwechseln mit der Eignung kryptographischer Algorithmen.

5.3.1.6.2 Vorhandenseinsprüfung

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN für eine gemäß Konfiguration geforderte Vorhandenseinsprüfung des aktuell geprüften Zertifikats die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	[$Zert_i$] ist gemäß geeigneter Vorhandenseinsinformation zum Zeitpunkt t_{Ref} vorhanden	gemäß Konfiguration *keine* Prüfung	kp
		es liegt *keine* für t_{Ref} geeignete Vorhandenseinsinformation für [$Zert_i$] vor	tnp
		[$Zert_i$] ist zu t_{Ref} vorhanden	tg
		[$Zert_i$] ist zu t_{Ref} *nicht* vorhanden	tng

Für die Bewertung der Eignung von Vorhandenseinsinformationen sind die Prüfbedingungen aus Kapitel 5.4 zu verwenden.

5.3.1.6.3 Sperrprüfung

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN für die gemäß Konfiguration geforderte Sperrprüfung des aktuell geprüften Zertifikats die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	[$Zert_i$] ist gemäß geeigneter Sperrinformation zum Zeitpunkt t_{Ref} nicht gesperrt	gemäß Konfiguration *keine* Prüfung	kp
		es liegt *keine* für t_{Ref} geeignete Sperrinformation für [$Zert_i$] vor	tnp
		$t_{Ref} < t_{Sperr}([Zert_i])$	tg
		$t_{Ref} >= t_{Sperr}([Zert_i])$	tng

Für die Bewertung der Eignung von Sperrinformationen sind die Prüfbedingungen aus Kapitel 5.4 zu verwenden.

5.3.1.7 Allgemeine Zweck- und Autorisierungsprüfung für Zertifikate

Für Zertifikate und Attribut-Zertifikat

- muß sichergestellt werden, daß sie aus der Zertifizierungshierarchie nach SigI stammen,
- müssen Nutzungsbeschränkungen und -berechtigungen angezeigt werden und
- muß auf ein gegebenenfalls gefordertes Attribut-Zertifikat geprüft werden.

Die dazu erforderlichen Prüfbedingungen werden in diesem Abschnitt spezifiziert. Zusätzlich müssen für Teilnehmerzertifikate von Endanwendern, Teilnehmerzertifikate für Dienste von Zertifizierungsstellen, Zertifizierungsstellen-Zertifikate und Attribut-Zertifikate spezifische Prüfbedingungen aus den folgenden Abschnitten geprüft werden.

5.3.1.7.1 Zertifizierungshierarchie "SigI"

Die Prüfbedingung stellt sicher, daß alle Zertifikate aus der Zertifizierungshierarchie nach SigI stammen.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	certificatePolicies von [$Zert_i$] enthält den OID *id-sigi-cp-sigconform*[36]	nicht erfüllt	tng

5.3.1.7.2 Nutzungsbeschränkungen und -berechtigungen

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN in Zertifikaten die folgenden Attribute im Feld **subjectDirectoryAttributes** oder als eigenständige Erweiterung erkennen (vgl. [BSI_ZERT]):

- **admission** (Zulassung)
- **monetaryLimit** (Monetäre Beschränkung)
- **declarationOfMajority** (Volljährigkeit)
- **restriction** (Sonstige Einschränkungen)

SigI-konforme Prüffunktionen müssen diese Erweiterungen gemäß [BSI-ZERT] interpretieren und alle inhaltlichen Attribute der Erweiterungen als MELDUNGSERGÄNZUNG im Gesamtergebnis anzeigen, wenn sie im Zertifikat enthaltenen sind.

5.3.1.7.3 procuration

Eine Besonderheit tritt für die Erweiterung **procuration** auf. In ihr wird eine Vertretungsmacht für eine oder mehrere dritte Personen bekanntgegeben. In die Erweiterung wird entweder der Namen der vertretenen Person oder ein Verweis auf deren Teilnehmerzertifikat aufgenommen.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN in Zertifikaten im Feld **subjectDirectoryAttributes** die Erweiterung **procuration** (Vertretungsmacht) erkennen. SigI-konforme Prüffunktionen müssen die Erweiterungen gemäß [BSI-ZERT] interpretieren und alle inhaltlichen Attribute der Erweiterungen als MELDUNGSERGÄNZUNG im Gesamtergebnis anzeigen, wenn sie im Zertifikat enthaltenen ist

Für den Verweis auf die vertretene Person kann die Variante **signingFor.certRef** gewählt werden, die über Issuer und Seriennummer auf ein Zertifikat verweist. Dieses Zertifikat wird als [$Zert_{Ref}$] bezeichnet. Diese Variante ist technisch so zu interpretieren, daß die Vertretungsmacht nur dann ausgeübt werden darf, wenn auch das Zertifikat des Vertretenen technisch gültig ist. Daher MUSS [$Zert_{Ref}$] mit der zugehörigen Zertifikatkette geprüft werden.

36 Siehe [BSI-ZERT].

Nr.	Prüfbedingung	Fall	Teilergebnis
	[$Zert_{Ref}$] ist ein technisch gültiges Teilnehmerzertifikat aus der Zertifizierungshierarchie von SigI. Als Referenzzeitpunkt für die zeitbezogenen Prüfungen ist t_{Ref} zu verwenden.		Zwischenergebnis für das Prüfobjekt [$Zert_{Ref}$]

Im Gesamtergebnis ist die Prüfung für [$Zert_{Ref}$] abzugrenzen. dazu ist eine abgeschlossen MELDUNGSERGÄNZUNG vorzusehen. Folgendes Verhalten wird von SigI-konformen Prüffunktionen gefordert:

Nr.	Zwischenergebnis für die Prüfung von [$Zert_{Ref}$]	Verhalten der Prüffunktion	
	"tg", "mso" oder "mu"	in die MELDUNGSERGÄNZUNG für das Gesamtergebnis ist der Name des Vertretenen aufzunehmen, wie er in [$Zert_{Proc}$] angegeben ist. Für die Anzeige des Namens gelten die Regeln der Konfiguration aus Kapitel 5.1.3. Das Zwischenergebnis ist ebenfalls anzugeben.	
	"tng" oder "tnp"	Die MELDUNGSERGÄNZUNG für das Gesamtergebnis weist darauf hin, daß [$Zert_{Ref}$] den geforderten Prüfbedingungen nicht genügt. Das Zwischenergebnis ist ebenfalls anzugeben.	
	"kp" Kennzeichnungen	"kp" Kennzeichnungen werden in der MELDUNGSERGÄNZUNG für [$Zert_{Ref}$] berücksichtigt	
	pake	pake	

Über die MELDUNGSERGÄNZUNG hinaus wird das Zwischenergebnis *nicht* im Gesamtergebnis des Primärdokuments berücksichtigt!

5.3.1.7.4 liabilityLimitationFlag

Ein im Teilnehmerzertifikat enthaltenes **liabilityLimitationFlag** zeigt an, daß das Zertifikat nur mit einem ergänzenden Attribut-Zertifikat verwendet werden darf. Im Primärdokument muß also auf ein Attribut-Zertifikat verwiesen werden, das auf das Teilnehmerzertifikat verweist.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN im Falle eines im Zertifikat enthaltenen **liabilityLimitationFlag** die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis

Nr.	Prüfbedingung	Fall	Teilergebnis
	liabilityLimitationFlag([$Zert_{Tln}$]) ist gesetzt und im Primärdokument ist gemäß Kapitel 5.1.6 ein technisch gültiges Attribut-Zertifikat ([$Zert_{Attr}$]) enthalten. [$Zert_{Attr}$] muß [$Zert_{Tln}$] referenzieren.[37]	erfüllt	tg
		nicht erfüllt	tng

5.3.1.8 Bildung des Zwischenergebnisses für Zertifikate

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN das Zwischenergebnis für die technische Gültigkeitsprüfung eines Zertifikats nach den Regeln für die Bildung eines Gesamtergebnisses zusammenfassen. Dabei sind die allgemeinen Prüfbedingungen für Zertifikate aus diesem Kapitel sowie die spezifischen Prüfbedingungen zu berücksichtigen, soweit sie nach den folgenden Abschnitten für den jeweiligen Zertifikattyp oder Verwendungszweck gefordert werden.

5.3.2 Spezifische Zweck- und Autorisierungsprüfungen für Zertifikate von Endanwendern

Die Prüfbedingungen dieses Abschnitts gelten für Teilnehmerzertifikate von Endanwendern. Die spezifischen Prüfbedingungen für Teilnehmerzertifikate für Dienste von Zertifizierungsstellen werden im nächsten Teilkapitel beschrieben.

Zertifikate von Endanwendern sind Signatur-Zertifikate, deren bestätigtes Schlüsselpaar *nicht* zum Zertifizieren verwendet werden darf. Sie sind deshalb von Zertifizierungsstellen-Zertifikaten zu unterscheiden. In Zertifikate von Endanwendern darf daher im Attribut **keyUsage** nicht das Bit "**certSign"** gesetzt sein. Sie müssen im Attribut **basicConstraints.cA** den Wert "**false**"[38] enthalten.

R33) Das BSI geht davon aus, Zertifizierungsstellen nach SigI für Endanwender nur Teilnehmerzertifikate ausstellen, die nicht das Bit "**certSign"** und im Attribut **basicConstraints.cA** den Wert "**false**" enthalten. Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingung durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt wird. SigI-konforme Prüffunktionen KÖNNEN DESHALB DAVON AUSGEHEN, daß diese Prüfbedingung erfüllt ist.

Da für Zertifikatketten sichergestellt werden muß, daß diese in der Zertifizierungshierarchie von SigI liegen, müssen die entsprechenden Konsistenzbedingungen nicht geprüft werden.

37 Die Prüfung des Attribut-Zertifikats wird in dieser Spezifikation bereits im Zusammenhang mit der Prüfung des Primärdokuments angestoßen. Das Prüfergebnis für das Attribut-Zertifikat muß nicht erneut bestimmt werden. Es ist ausreichend, wenn ein technisch gültiges Attribut-Zertifikat enthalten ist.

38 Zur geforderten Codierung von "false" vgl. [BSI-ZERT]. Dort wird gefordert, daß der Wert der Extension in Teilnehmerzertifikaten stets als SEQUENCE mit Null Komponenten darzustellen ist.

Die Zertifikate für Endanwender und die Dienste von Zertifizierungsstellen außer zum Ausstellen von Zertifikaten werden als "zum Prüfen rechtsverbindlicher Willenserklärungen bestimmt" gekennzeichnet, indem im Attribut **KeyUsage** das Bit für **nonRepudiation** gesetzt wird.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	Im Attribut **KeyUsage** des [$Zert_{Tln}$] ist das Bit für **nonRepudiation** gesetzt	nicht erfüllt	tng

5.3.3 Spezifische Zweck- und Autorisierungsprüfungen für Zertifikate für Dienste von Zertifizierungsstellen

Die Prüfbedingungen dieses Abschnitts gelten für Zertifikate, deren Schlüssel zum Prüfen von "Zeitstempeln", "Verzeichnisdienstauskünften" und "Sperrlisten" eingesetzt werden sollen. Die Prüfobjekte sollen nur anerkannt werden, wenn im Zertifikat eine entsprechende Zweckangabe enthalten ist.

Zertifizierungsstellen setzen besondere Teilnehmerzertifikate für die Dienste "Zeitstempeldienst", "Verzeichnisdienst" und "Sperrlisten" ein. Daraus ergeben sich für die Zertifikate dieser Dienste die folgenden spezifischen Prüfbedingungen der Zweck- und Autorisierungsprüfung.

Zertifikate für Dienste von Zertifizierungsstellen sind Signatur-Zertifikate, deren bestätigtes Schlüsselpaar *nicht* zum Zertifizieren verwendet werden darf. Sie sind deshalb von Zertifizierungsstellen-Zertifikaten zu unterscheiden. In diesen Zertifikaten darf daher im **keyUsage** nicht das Bit "**certSign**" gesetzt sein. Sie müssen im Attribut **basicConstraints.cA** den Wert "**false**" enthalten.

R34) Das BSI geht davon aus, daß Zertifizierungsstellen nach SigI für Dienste von Zertifizierungsstellen nur Zertifikate ausstellen, die nicht das Bit "**certSign**" und im Attribut **basicConstraints.cA** den Wert "**false**" enthalten. Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingung durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt wird. SigI-konforme Prüffunktionen KÖNNEN DESHALB DAVON AUSGEHEN, daß diese Prüfbedingung erfüllt ist.

Da für Zertifikatketten sichergestellt werden muß, daß diese in der Zertifizierungshierarchie von SigI liegen, müssen die entsprechenden Konsistenzbedingungen nicht geprüft werden.

Die Zertifikate für die Dienste von Zertifizierungsstellen werden wie andere Teilnehmerzertifikate als "zum Prüfen rechtsverbindlicher Willenserklärungen bestimmt" gekennzeichnet, indem im Attribut **KeyUsage** das Bit für **nonRepudiation** gesetzt wird. Außerdem wird die jeweilige Zweckangabe für den Dienst gefordert.

5.3.3.1 Zertifikate zum Prüfen von Zeitstempeln

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	Im Attribut **KeyUsage**([$Zert_{TSS}$]) ist das Bit für **nonRepudiation** gesetzt	nicht erfüllt	tng
	Im Attribut **extKeyUsage**([$Zert_{TSS}$]) ist der Object Identifier für **id-kp-timeStamping** eingetragen.	nicht erfüllt	tng

5.3.3.2 Zertifikate zum Prüfen von Verzeichnisdienstauskünften

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	Im Attribut **KeyUsage**([$Zert_{Dir}$]) ist das Bit für **nonRepudiation** gesetzt	nicht erfüllt	tng
	Im Attribut **extKeyUsage**([$Zert_{Dir}$]) ist der Object Identifier für **id-sigi-kp-directoryService** eingetragen.	nicht erfüllt	tng

5.3.3.3 Zertifikate zum Prüfen von Sperrlisten

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	Im Attribut **KeyUsage**([$Zert_{RL}$]) ist das Bit für **nonRepudiation** gesetzt (vgl. oben "Signatur-Zertifikat")	nicht erfüllt	tng
	Im Attribut **KeyUsage**([$Zert_{RL}$]) ist das Bit für **cRLSign** gesetzt.	nicht erfüllt	tng

5.3.4 Zweck- und Autorisierungsprüfung für Zertifizierungsstellen-Zertifikate

Die Prüfbedingungen dieses Abschnitts gelten für Zertifikate, die zum Prüfen von Zertifikaten eingesetzt werden sollen.

Zertifizierungsstellen-Zertifikate enthalten zwei Kennzeichen, durch die die Verwendung zum Prüfen von Zertifikaten bestimmt wird. Dies sind die Attribute **basicConstraints.cA** und das **keyUsage**-Bit "**certSign**"

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen müssen die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	gefordert ist, daß **basicConstraints.cA**([$Zert_{ZS}$]) ist "**true**" und **keyUsage.certSign**"([$Zert_{ZS}$]) ist gesetzt	nicht erfüllt	tng

5.3.5 Spezifische Prüfbedingungen für Attribut-Zertifikate

Die Prüfbedingungen dieses Abschnitts gelten für Attribut-Zertifikate.

Attribut-Zertifikate bestätigen zusätzliche Informationen zu einem Teilnehmerzertifikat. Im Kontext von SigI entsprechen die möglichen Einträge den Beschränkungen und Berechtigungen in Zertifikaten (vgl. [BSI-ZERT]). Während Beschränkungen und Berechtigungen in Teilnehmerzertifikaten bereits direkt mit der Auswertung des Zertifikats zum Prüfschlüssel eines Primärdokuments zur Verfügung stehen, ist dies für Attribut-Zertifikate nicht der Fall.

Angaben aus Attribut-Zertifikaten müssen daher in der technischen Signaturprüfung gesondert berücksichtigt werden.

Nach der Begriffsbestimmung von § 2 Abs. 3 SigG bezieht sich jedes Attribut-Zertifikat eindeutig auf ein Teilnehmerzertifikat (*Bezugszertifikat*). Da die Angaben in einem Attribut-Zertifikat unabhängig vom Bezugszertifikat zur Verfügung stehen, könnten sie einem digital signierten Dokument auch unabhängig vom Bezugszertifikat beigefügt werden. Für solche "konstruierten" Primärdokumente kann jedoch eine technische Prüfung nur sehr eingeschränkt und nur unter bestimmten Annahmen erfolgen.[39] Im Rahmen dieser Spezifikation werden sie nicht unterstützt. SigI fordert deshalb, daß sich alle im Primärdokument enthaltenen oder referenzierten Attribut-Zertifikate auf das Teilnehmerzertifikat beziehen, das den Schlüssel zum Prüfen des Primärdokuments enthält. Damit ergibt sich folgende Regel:

R35) Sind in einem Primärdokument Attribut-Zertifikate enthalten oder werden Attribut-Zertifikate referenziert, die sich nicht auf das Teilnehmerzertifikat mit dem Prüfschlüssel für das Primärdokument beziehen, ist das digital signierte Dokument "technisch nicht gültig".

Unter Berücksichtigung der nach Annahme des BSI implizit erfüllten Prüfbedingungen muß lediglich sichergestellt werden, daß die im Attribut-Zertifikat enthaltene Referenz für das Bezugszertifikat auf das Zertifikat verweist, das den Prüfschlüssel für das Primärdokument enthält.

Die Zweck- und Autorisierungsprüfung für Attribut-Zertifikate ist bereits in der "allgemeinen Zweck- und Autorisierungsprüfung für Zertifikate" enthalten.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	baseCertificateID([$Zert_{Attr}$]) referenziert [$Zert_{Tln}$]	nicht erfüllt	tng

5.3.6 Spezifische Prüfbedingungen für Wurzelzertifikate

Die Prüfbedingungen dieses Abschnitts gelten nur für die Prüfung des Sicherungsankers einer Zertifikatkette. Einige Hinweise zur "Erstprüfung von Wurzelzertifikaten" finden sich im Anhang.

5.3.6.1 Eigenschaft "Wurzelzertifikat"

Zertifikatketten müssen in einem Wurzelzertifikat enden. Die technisch gültigen Wurzelzertifikate werden in einer Liste verwaltet (vgl. Kapitel 4). Im Rahmen der Vorhandenseins- und Sperrprüfung oder bei der Auswertung von CRLs kann jedoch festgestellt werden, daß ein neues Wurzelzertifikat benötigt wird. Solche neuen Zertifikate müssen einem besonderen

39 So könnte ein Signierender ein Attribut-Zertifikat hinzufügen, daß einem anderen Teilnehmerzertifikat auf seinen Namen zugeordnet ist. SigI-konforme Signaturfunktionen sollten solche Konstruktionen erschweren oder sogar verhindern. Eine formale Prüfung solcher "Optionen" ist erheblichen Problemen und Unsicherheiten behaftet. Juristisch können solche "konstruierten" Primärdokument allerdings dennoch als gültig bewertet werden. Die juristischen Tatbestände von Attribut-Zertifikaten mit "inkonsistenter Referenz" in rechtsverbindlichen Willenserklärungen werden durch die technische Signaturprüfung daher nur eingeschränkt abgebildet.

Prüfprozeß unterworfen werden. Erst nachdem die Erstprüfung für ein neues Wurzelzertifikate erfolgreich abgeschlossen wurde, darf es in die Liste der Wurzelzertifikate aufgenommen werden. Dann erst darf es im Rahmen des Prüfprozesses auch als Wurzelzertifikat verwendet werden.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN für die Überprüfung der Eigenschaft "Wurzelzertifikat" die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	Zertifikat ist Element der Liste der Wurzelzertifikate	nicht erfüllt	tng
		erfüllt	tg

SigI-konforme Prüffunktionen KÖNNEN im Falle des Teilergebnisses "tng" die folgende Funktionalität anbieten: Die Funktion prüft, ob das fragliche Zertifikat als neues Wurzelzertifikat der RegTP in Frage kommt. Indizien sind beispielsweise:

- Der distinguished name der RegTP ist im Subject und im Issuer des Zertifikats enthalten und
- das Zertifikat ist ein Selbstzertifikat.

In diesem Fall kann die Prüffunktion dem Benutzer anbieten, für das fragliche Zertifikat eine "Erstprüfung für Wurzelzertifikate" durchzuführen (siehe Anhang). Wenn Prüffunktionen diese Unterstützung für die Fortschreibung der Liste der Wurzelzertifikate bieten, steht nach einer erfolgreichen Erstprüfung ein zusätzliches Wurzelzertifikat zur Verfügung. Sie können dem Benutzer daher anbieten, den "unterbrochenen" Prüfprozeß mit dem neuen Wurzelzertifikat fortzusetzen.

5.3.6.2 Vorhandenseins- und Sperrprüfung

Die Vorhandenseinsprüfung für Wurzelzertifikate erfolgt implizit im Rahmen der Erstprüfung für Wurzelzertifikate durch den Vergleich gesicherter Daten über einen alternativen Kanal (out of Band). Eine zusätzliche Vorhandenseinsprüfung ist daher nicht erforderlich.

Eine regelmäßige Sperrprüfung kann dagegen aus zwei Gründen sinnvoll sein:

- Im Konzept für den Schlüsselwechsel der RegTP ist vorgesehen, daß beim Wechsel auf eine neue Schlüsselgeneration die alten Zertifikate gesperrt werden. Eine regelmäßige Sperrprüfung für das aktuellste Wurzelzertifikat kann daher dazu beitragen, daß der Benutzer diese Situation erkennt und sich um das neue Wurzelzertifikat bemühen kann.
- Sperrungen des Wurzelzertifikats wegen Unregelmäßigkeiten werden erkannt.

Da für ein Wurzelzertifikat keine weitere Zertifikatprüfung angestoßen wird, muß die Sperrprüfung unmittelbar durchgeführt werden. Sofern eine technisch gültige und geeignete Sperrliste vom Issuer RegTP vorliegt, kann diese für die Prüfung verwendet werden.

SigI-Konformitätsanforderungen

Sofern die Sperrprüfung des Wurzelzertifikats gemäß der Konfiguration durch den Benutzer gefordert ist, MÜSSEN SigI-konforme Prüffunktionen die folgende Funktionalität aufweisen:

- Als Referenzzeitpunkt wird **dateOfCertGen** des Zertifikats verwendet, das mit dem Wurzelzertifikat bestätigt werden soll.
- Dieser Referenzzeitpunkt wird verwendet, um die Prüfungen gemäß Kapitel 5.3.1.6 durchzuführen.

Hinweis: Die Sperrung eines Wurzelzertifikats ist nach den Regeln der technischen Gültigkeitsprüfung mit einem Zertifikat des Verzeichnisdienstes oder Sperrdienstes der RegTP möglich. Dieses [$Zert_{RL}$, RegTP] bzw. [$Zert_{Dir}$, RegTP] muß lediglich vor der Sperrung des Wurzelzertifikats ausgestellt werden und ist dann von der (späteren) Sperrung des Wurzelzertifikats nicht betroffen.

> Um einen gleitenden Wechsel der verschiedenen Schlüsselgenerationen zu erlauben, wird der RegTP empfohlen, bei regulären Schlüsselwechseln die Schlüssel zum Signieren von Verzeichnisdienstauskünften und Sperrlisten für einen Übergangszeitraum weiterzuverwenden und erst mit einer zeitlichen Verzögerung zu sperren.

Aktualisierung der Liste der Wurzelzertifikate

Um einen kontinuierlichen Einsatz der Prüffunktion zu gewährleisten, benötigen die Benutzer eine möglichst aktuelle Liste von Wurzelzertifikaten. Daher SOLLEN SigI-konforme Prüffunktionen den Benutzer auf einen Zertifikatwechsel der RegTP hinweisen. Um die Information des Benutzers und die Aktualisierung der Liste der Wurzelzertifikate zu unterstützen, KÖNNEN SigI-konforme Prüffunktionen die folgende Funktionalität anbieten:

Unabhängig von einem Referenzzeitpunkt für die Prüfung eines Zertifizierungsstellen-Zertifikats kann die Prüffunktion beim Aktualisieren einer Sperrliste feststellen, ob das aktuellste Wurzelzertifikat dort aufgeführt ist. Wenn von der Prüffunktion erstmals für das aktuellste Wurzelzertifikat ein $t_{Sperr}([Zert_{RegTP}])$ festgestellt wird, wird der Benutzer über einen möglichen Schlüsselwechsel der RegTP informiert. Es wird angeboten, das neue Zertifikat abzufragen und die Erstprüfung von Wurzelzertifikaten zur Aufnahme in die Liste der Wurzelzertifikate durchzuführen. Um dem Benutzer die Prüfung gegen die Informationen im Bundesanzeiger zu erleichtern, SOLLEN SigI-konforme Prüffunktionen eine download-Möglichkeit oder einen WWW-Zugang zum Bundesanzeigers anbieten. SigI-konforme Prüffunktionen MÜSSEN beim Abruf jedoch darauf hinweisen, daß die elektronisch abgerufene Information nicht gegen Manipulation oder Maskerade gesichert ist und unter Sicherheitsaspekten deshalb das Printmedium nicht ersetzen kann.

5.4 Eignung und Abfrage von Statusinformationen

Notationen

Statusinformationen werden für das Zertifikat benötigt, das Gegenstand der Prüfung nach Kapitel 5.3 ist.

- Das Zertifikat wird mit [$Zert_i$] bezeichnet.
- Als *Referenzzeitpunkt* t_{Ref} wird der Zeitpunkt bezeichnet, für den die Statusprüfungen für [$Zert_i$] durchgeführt werden, für den also die Statusinformationen für [$Zert_i$] geeignet sein müssen.
- Als $t_{Statusinfo}([Zert_i])$ wird der Zeitpunkt bezeichnet, für den die Statusinformation von der Sicherungsinfrastruktur bereitgestellt wurde.

Struktur der Darstellung

Für die Statusprüfungen müssen Statusinformationen verwendet werden. Dies sind die Informationen zum Vorhandensein und zum Sperrstatus eines Zertifikats. Diese Informationen können aus einem Verzeichnisdienst oder einem X.500-Directory abgefragt werden oder (aus früheren Abfragen) lokal vorliegen. Die eigentlichen Statusinformationen sind von den signierten Verzeichnisdienstauskünften oder Sperrlisten zu unterscheiden. Diese Quellen müssen ausgewertet werden, um die Statusinformationen für den Prüfprozeß zu erhalten.

Statusinformationen sind bezüglich eines Referenzzeitpunktes (t_{Ref}), für den der Status eines Zertifikats [$Zert_i$] festzustellen ist, nur unter bestimmten Bedingungen geeignet. Dazu ist die Eignung der Statusinformationen für den Referenzzeitpunkt, der in den zeitbezogenen Prüfbedingungen für [$Zert_i$] verwendet wird, zu entscheiden. Zunächst werden daher die Bedingungen für die Eignung verfügbarer Statusinformationen angegeben. Diese Prüfung der Eignung muß unabhängig davon durchgeführt werden, ob die Statusinformationen lokal in CRLs vorliegen oder ob sie auf andere Art verwaltet werden. Die Eignungsprüfung stellt sicher, daß die Statusinformationen auch für Referenzzeitpunkte in der Vergangenheit, die z. B. durch das Gültigkeitsmodell "Zertifikat-Gültigkeit" oder bei der Prüfung archivierter Dokumente erforderlich sind, zu interoperablen Ergebnisse führen. Eine für die Bewertung relevante Information ist der Zeitpunkt, für den die Statusinformation bereitgestellt wurde. Er wird als $t_{StatusInfo}$ bezeichnet. Für die Statusinformationen sind unterschiedliche Prüfbedingungen zu berücksichtigen.

Sind verfügbare Statusinformationen nicht geeignet oder liegen keine Statusinformationen vor, kann versucht werden, solche durch eine Abfrage aus der Sicherungsinfrastruktur des SigG zu erhalten. In diesem Fall ist es notwendig, zu entscheiden, welche Quelle für die Abfrage verwendet wird. Die Entscheidungskriterien werden ebenfalls in diesem Kapitel angegeben. Das auf eine Abfrage hin erhaltene digital signierte Dokumente muß zunächst auf technisch Gültigkeit geprüft werden. Nur bei erfolgreicher Prüfung dürfen die Statusinformationen verwendet werden. Auch für die neu erhaltenen Statusinformationen ist jedoch die Eignung zu überprüfen.

Wenn keine geeigneten Statusinformationen zur Verfügung stehen, keine geeigneten abgefragt werden können oder die abgefragten digital signierten Dokumente nicht gültig sind, wird die jeweilige Prüfbedingung mit "technisch nicht prüfbar" bewertet.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen SOLLEN dem Benutzer die Option anbieten, einmal erhaltene Statusinformationen zu einem Zertifikat wiederzuverwenden, wenn diese nach den im weiteren definierten Regeln geeignet sind. Dazu müssen Sperrlisten oder Verzeichnisdienstauskünfte lokal gespeichert oder die daraus abgeleiteten Statusinformationen zu Zertifikaten und der Zeitpunkt ihrer Bereitstellung ($t_{Statusinfo}$) lokal verwaltet werden. Im Rahmen der Konfiguration dieser Option ist der Benutzer auf die Folgen für Prüfergebnisse hinzuweisen, wenn die lokal verwalteten Statusinformationen durch Dritte verändert werden können.

Der Benutzer muß lokal gespeicherte Statusinformationen zu Zertifikaten einsehen und löschen können.

5.4.1 Eignung verfügbarer Vorhandenseinsinformationen

Für Vorhandenseinsinformationen gelten die folgenden Regeln:

R36) Eine einmal positiv gegebene Vorhandenseinsinformation kann zu einem Zertifikat nicht zurückgenommen werden. Sie ist für die Vorhandenseinsprüfung geeignet, wenn t_{Ref} nach $t_{Statusinfo}$ liegt. Zu einem Zeitpunkt vor $t_{Statusinfo}$ könnte das Zertifikat jedoch noch nicht freigegeben sein.

R37) Die Vorhandenseinsinformation "nicht vorhanden" zu einem Zertifikat ist nur geeignet, wenn der Ausstellungszeitpunkt der Vorhandenseinsinformation nach dem Referenzzeitpunkt liegt, zu dem das Vorhandensein von [$Zert_i$] geprüft werden soll. Zu einem späteren Zeitpunkt kann das Zertifikat jedoch vorhanden sein.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis und Verhalten
	liegt eine Vorhandenseinsinformation vor, die das Vorhandensein des Zertifikats [$Zert_i$] zum Referenzzeitpunkt t_{Ref} bestätigt?	zum Referenzzeitpunkt oder zu einem früheren Zeitpunkt ist [$Zert_i$] "good" oder "revoked"	tg
		es liegt eine Vorhandenseinsinformation vor, die für das Zertifikat zum Referenzzeitpunkt oder zu einem späteren Zeitpunkt "nicht vorhanden" angibt	tg
		in jedem der Fälle • es liegt keine Vorhandenseinsinformation vor oder • Vorhandenseinsinformation([$Zert_i$]) = "nicht vorhanden" und $t_{Ref} > t_{Statusinfo}$[40] oder • Vorhandenseinsinformation([$Zert_i$]) = "vorhanden" und $t_{Ref} < t_{Statusinfo}$[41]	es muß eine neue Vorhandenseinsinformation für den Zeitpunkt t_{Ref} abgefragt werden. Das Teilergebnis wird durch die Eignung der neuen Vorhandenseinsinformation bestimmt.

Sofern die Prüfbedingung nicht mit "tg" bewertet wird, MÜSSEN SigI-konforme Prüffunktionen mindestens einen Versuch machen, geeignete Vorhandenseinsinformationen aus der Sicherungsinfrastruktur nach SigI abzufragen. Dazu sind die funktionalen Anforderungen nach Kapitel 5.4.3 umzusetzen.

40 Unter diesen Bedingungen kann eine jüngere Statusinformation gegebenenfalls das Vorhandensein bestätigen.

41 Unter diesen Bedingungen kann eine jüngere Statusinformation gegebenenfalls anzeigen, daß das Zertifikat zu diesem Zeitpunkt noch nicht freigeschaltet war.

5.4.2 Eignung verfügbarer Sperrinformationen

Für Sperrinformationen gelten die folgenden Regeln:

R38) Eine Sperrinformation "gesperrt ab [Zeitpunkt]" für ein Zertifikat ist in jedem Fall geeignet.

R39) Die Sperrinformation "nicht gesperrt" zu einem Zertifikats ist nur geeignet, wenn sie zu einem Zeitpunkt ausgestellt wurde, der nach dem Referenzzeitpunkt liegt.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis und Verhalten
	Liegt eine Sperrinformation vor, die als Sperrstatus des Zertifikats [$Zert_i$] zum Referenzzeitpunkt t_{Ref} "gesperrt" angibt?	Es liegt eine entsprechende Sperrinformation vor.	tg
		Es liegt eine Sperrinformation vor, die für das Zertifikat zum Referenzzeitpunkt oder zu einem späteren Zeitpunkt "nicht gesperrt" angibt	tg
		in jedem der Fälle • es liegt keine Sperrinformation vor oder • Sperrinformation([$Zert_i$] = "nicht gesperrt" und $t_{Statusinfo} < t_{Ref}$	es muß eine neue Sperrinformation für den Zeitpunkt t_{Ref} abgefragt werden. Das Teilergebnis wird durch die Eignung der neuen Sperrinformation bestimmt.

Sofern die Prüfbedingung nicht mit "tg" bewertet wird, MÜSSEN SigI-konforme Prüffunktionen mindestens einen Versuch machen, geeignete Sperrinformationen aus der Sicherungsinfrastruktur nach SigI abzufragen. Dazu sind die funktionalen Anforderungen nach Kapitel 5.4.3 umzusetzen.

5.4.3 Abfrage neuer Statusinformationen

Sollen neue Statusinformationen aus der Sicherungsinfrastruktur abgerufen werden, muß zunächst entschieden werden, welche Quelle dafür herangezogen werden kann. Dafür spielen folgende Faktoren eine Rolle:

- die Art der Information und die zu verwendende Quelle, die vom Benutzer für den Prüfprozeß konfiguriert wurde (vgl. Kapitel 4),
- der Zeitraum für den die gewünschte Information in der Quelle bereitgestellt wird.

Abgefragte Verzeichnisdienstauskünfte und Sperrlisten müssen auf technische Gültigkeit geprüft werden. Die in technisch gültigen Verzeichnisdienstauskünften und Sperrlisten enthaltenen Informationen müssen wie lokal vorhandene Statusinformationen auf ihre Eignung geprüft werden.

5.4.3.1 Wahl der Quelle für neue Statusinformationen

In Kapitel 4 wurde festgelegt, daß SigI-konforme Verzeichnisdienste mindestens für 10 Jahre ab dem Ausstellungszeitpunkt des Zertifikats automatisiert Statusinformationen bereitstellen.

In Kapitel 4 wurde festgelegt, daß die Seriennummern gesperrter Zertifizierungsstellen-Zertifikate in den Sperrlisten bis zum Ende der Gültigkeitsdauer des letzten nachgeordneten Teilnehmerzertifikats geführt werden müssen.

Diese Regeln werden für die Auswahl der Quellen von Statusinformationen berücksichtigt.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN prüfen, ob sie aus der konfigurierten Quelle eine geeignete Statusinformation für den Zeitpunkt t_{Ref} ableiten können. Falls dies wegen des Umfangs der Sperrliste oder Verzeichnisdienstauskunft nicht möglich ist,[42] müssen sie den Benutzer darauf hinweisen. Soweit möglich, MÜSSEN sie alternative Möglichkeiten zum Abruf von Statusinformationen anbieten. Durch den vorgegebenen Zeitraum für die Bereitstellung von Statusinformationen durch den zuständigen Verzeichnisdienst kann dieser nach Ablauf des Gültigkeitsendes des [$Zert_{TIn}$] noch für einen gewissen Zeitraum statt Sperrlisten zur abfrage von Sperrinformationen herangezogen werden. Die Anforderungen der folgenden Abschnitte präzisieren das funktionale Verhalten und die Verwertung abgerufener Verzeichnisdienstauskünfte und Sperrlisten.

Information über die Statusinformation
SigI-konforme Prüffunktionen MÜSSEN dem Benutzer für jede Prüfung die Information zur Verfügung stellen, welche Quellen für Vorhandenseins- und Sperrinformationen verwendet wurde und wie aktuell diese Statusinformationen waren. Die Anforderung ist ausreichend erfüllt, wenn sie in den Detailinformationen bereitgestellt wird.

Erweiterte Auswahl der zu verwendenden Sperrinformation
Der Benutzer MUSS für jede Prüfung im Einzelfall entscheiden können, welche Quellen er für die Sperrinformationen der im einzelnen geprüften Zertifikate wählt. Die Anforderung ist ausreichend erfüllt, wenn er bei der Anzeige eines Prüfergebnisses eine zusätzliche Prüfung mit differenzierter Auswahl von Sperrinformationen veranlassen kann.

5.4.3.2 Abruf und Verwendung von Verzeichnisdienstauskünften

5.4.3.2.1 Abruf einer Verzeichnisdienstauskunft

SigI-Konformitätsanforderungen

Falls eine Verzeichnisdienstauskunft abgefragt werden soll, MÜSSEN SigI-konforme Prüffunktionen die folgende Funktionalität aufweisen:

42 Der Umfang möglicher Informationen bestimmt sich aus dem Zeitraum, für den Statusinformationen in der Quelle bereitgestellt werden, vgl. die Regeln R0 und R0.

Nr.	Prüfbedingung	Fall	Teilergebnis
	Statusinformationen können durch aktuelle Anfrage beschafft werden	$t_{Prüf}$ > **dateOfCertGen**([$Zert_i$])+10Jahre	tnp
		Anfrage gelingt nicht erfolgreich	tnp
		Anfrage gelingt nicht erfolgreich und Benutzer entscheidet, daß die Vorhandenseinsprüfung oder Sperrprüfung entfallen soll	kp

Eine erfolgreich abgerufene Verzeichnisdienstauskunft MUSS gemäß der folgenden Abschnitte auf technische Gültigkeit und Eignung geprüft werden.

5.4.3.2.2 Prüfung der Verzeichnisdienstauskunft

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN abgerufene Verzeichnisdienstauskünfte auf technische Gültigkeit prüfen.

Nr.	Prüfbedingung	Fall	Teilergebnis
	abgerufene Verzeichnisdienstauskunft ist technisch gültig		Zwischenergebnis der Gültigkeitsprüfung für die Verzeichnisdienstauskunft

Neu abgerufene Verzeichnisdienstauskünfte dürfen nur dann weiterverwendet werden, wenn das Zwischenergebnis der Gültigkeitsprüfung auf "tg" lautet. Ein "kp"-Vermerk im Teilergebnis der technischen Gültigkeitsprüfung der Verzeichnisdienstauskunft hat keinen Einfluß auf die Verwendung der Vorhandenseins- bzw. Sperrinformation.

Im Falle der erneuten Prüfung archivierter Verzeichnisdienstauskünfte muß der Benutzer ihrer Verwendung zustimmen, wenn das Zwischenergebnis der Gültigkeitsprüfung auf "mso" oder "mu" lautet.

5.4.3.2.3 Verwendung von Statusinformationen aus Verzeichnisdienstauskünften

Die in den abgerufenen und zur Verwendung zugelassenen Verzeichnisdienstauskünfte enthaltenen Statusinformationen müssen vor ihrer Verwendung darauf hin geprüft werden, welchem Zertifikat sie zuzuordnen sind. Für das jeweilige Zertifikat sind für die weitere Eignungsprüfung die relevanten Zeitangaben für Statusinformationen zu bestimmen.

R40) Eine Verzeichnisdienstauskunft ist für die Bereitstellung von Vorhandenseinsinformationen und Sperrinformationen geeignet. Der Zeitpunkt, zu dem eine Statusinformation für ein Zertifikat gilt, wird in der Verzeichnisdienstauskunft durch das Attribut **singleResponse.thisUpdate** angegeben.

Im Unterschied zu Sperrlisten, aus denen implizite Sperrinformationen für nicht enthaltene Seriennummern abgeleitet werden, können aus Verzeichnisdienstauskünften nur die expliziten Angaben verwendet werden.

SigI-Konformitätsanforderungen "Identifikation von Zertifikaten zu Statusinformationen aus Verzeichnisdienstauskünften"

SigI-konforme Prüffunktionen dürfen aus Verzeichnisdienstauskünften nur Statusinformationen zu den Zertifikaten ableiten, die in einer Verzeichnisdienstauskunft explizit referenziert werden.

SigI-konforme Prüffunktionen dürfen sich nicht darauf verlassen, daß in Verzeichnisdienstauskünften genau zu den Zertifikaten Statusinformationen gegeben werden, zu denen sie sie angefragt haben. Sie MÜSSEN beim Auswerten von Verzeichnisdienstauskünften prüfen, für welche Zertifikate die darin enthaltenen Statusinformationen gegeben werden. Zur Absicherung der Referenzierung von Zertifikaten kann vom Verzeichnisdienst **singleResponse.certHash** zurückgeliefert werden. In diesem Fall MÜSSEN SigI-konforme Prüffunktionen diesen Mechanismus zur lokalen Absicherung der Referenzierung von Zertifikaten verwenden, für die die Statusinformationen übermittelt wurden.

Konfigurationsmöglichkeiten der Prüffunktion:
Zur Absicherung der Referenzierung von Zertifikaten kann bereits in Anfragen an Verzeichnisdienste das Attribut **request.certHash** verwendet werden. SigI-konforme Prüffunktionen MÜSSEN die Möglichkeit bieten, die Verwendung dieses Mechanismus zu konfigurieren. Wenn das Attribut in Anfragen verwendet wurde, müssen SigI-konforme Prüffunktionen sicherstellen, daß es auch in der Antwort enthalten ist. Für die Berechnung des Hash-Wertes dürfen nur zum Anfragezeitpunkt geeignete Algorithmen nach SigI verwendet werden.

Daraus ergibt sich gleichzeitig folgende besondere Anforderung an die *Prüffunktion von Verzeichnisdiensten*:

R41) In Verzeichnisdienstanfragen kann die Referenzierung von Zertifikaten durch **request.certHash** abgesichert werden. SigI-konforme Verzeichnisdienste MÜSSEN sicherstellen, daß sie vor der Bestimmung einer Statusinformation für eine Verzeichnisdienstauskunft prüfen, ob **request.certHash** zum Hash-Wert des angefragten Zertifikats mathematisch korreliert. Andernfalls MÜSSEN sie die Antwort "**unknown**" geben.

SigI-Konformitätsanforderungen "Zeitangaben für Statusinformationen aus Verzeichnisdienstauskünften"

Für jede in einer Verzeichnisdienstauskunft enthaltene Statusinformation muß jeweils als $t_{Statusinfo}$ der Wert des Attributs **singleResponse.thisUpdate** verwendet werden. Falls **singleResponse.certStatus** dem Wert "**good**" entspricht, hat das Zertifikat zum Zeitpunkt $t_{Statusinfo}$ den Sperrstatus "nicht gesperrt". Falls **singleResponse.certStatus** dem Wert "**revoked**" entspricht, ist t_{Sperr} des betreffenden Zertifikats auf den Wert von **singleResponse.certStatus.revocationTime** zu setzen.

SigI-Konformitätsanforderungen "Änderungen von Statusinformationen"

Da Angreifer versuchen können, eine frühere Antwort eines Verzeichnisdienstes erneut einzuspielen, MÜSSEN SigI-konforme Prüffunktionen auch für neu abgerufene Statusinformationen sicherstellen, daß sie gemäß der *Prüfbedingungen für verfügbare Statusinformationen* auf Eignung geprüft werden.

Durch die Auswertung von Verzeichnisdienstauskünften dürfen Änderungen für die lokal geführten Vorhandenseinsinformation und Sperrinformationen eines Zertifikats nur vorgenommen werden, wenn die Verzeichnisdienstauskunft neuer ist als die bisherigen Statusinformationen. Eine Ausnahme besteht dann, wenn die Statusinformation "nicht gesperrt" implizit aus einer Sperrliste abgeleitet wurde, eine Verzeichnisdienstauskunft aber die explizite Information "nicht vorhanden" enthält.

5.4.3.3 Abruf und Verwendung von Sperrlisten

5.4.3.3.1 Abruf von Sperrlisten

SigI-Konformitätsanforderungen

Falls gemäß Konfiguration eine Sperrliste abgerufen werden soll, MÜSSEN SigI-konforme Prüffunktionen die folgende Funktionalität aufweisen:

- wenn $t_{Prüf} <= t_E([Zert_{Tln}])$, dann wird die Sperrliste abgefragt.
- wenn $t_{Prüf} > t_E([Zert_{Tln}])$ und $t_{Prüf} <$ **dateOfCertGen**$([Zert_i])$+10Jahre, dann muß dem Benutzer angeboten werden, die Statusinformation über eine Verzeichnisdienstauskunft zu beschaffen.
- wenn die Abfrage der Sperrliste aus anderen Gründen nicht erfolgreich ist, dann muß dem Benutzer angeboten werden, die Statusinformation über eine Verzeichnisdienstauskunft zu beschaffen.

Nr.	Prüfbedingung	Fall	Teilergebnis
	Sperrliste kann durch aktuelle Anfrage beschafft werden	$t_{Prüf} > t_E([Zert_{Anf}])$ und Benutzer entscheidet, daß die Sperrprüfung entfallen soll	kp
		Abfrage nicht erfolgreich oder $t_{Prüf} > t_E([Zert_{Anf}])$ und Benutzer bricht den Prüfprozeß ab	pake
		Benutzer wählt "Verzeichnisdienstauskunft" als Alternative	Teilergebnis aus "Abruf von Verzeichnisdienstauskunft"

SigI-konforme Prüffunktionen MÜSSEN CRLs unter dem distinguished name des Issuer eines Zertifikats abfragen können.[43] Eine erfolgreich abgerufene Sperrliste MUSS gemäß den folgenden Abschnitten auf technische Gültigkeit und Eignung geprüft werden.

SigI-konforme Prüffunktionen KÖNNEN auch andere Bereitstellungsmöglichkeiten, wie beispielsweise über *cRLDistribututionPoints* gemäß [BSI-DIR], für die Abfrage von Sperrlisten unterstützen. Die Prüfbedingungen für Sperrlisten aus solchen Quellen sind entsprechend zu definieren. Sie sind nicht Gegenstand ist nicht Gegenstand dieses Teildokuments von SigI.

5.4.3.3.2 Prüfung von Sperrlisten

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN abgerufene Sperrlisten auf technische Gültigkeit prüfen.

43 Andere Bereitstellungsmechanismen können von SigI-konformen Prüffunktionen unterstützt werden, sind aber nicht Gegenstand dieser Spezifikation.

Nr.	Prüfbedingung	Fall	Teilergebnis
	abgerufene Sperrliste ist technisch gültig		Zwischenergebnis der Gültig-keitsprüfung für die Sperrliste

Neu abgerufene Sperrlisten dürfen nur dann weiterverwendet werden, wenn das Zwischenergebnis der Gültigkeitsprüfung auf "tg" lautet. Ein "kp"-Vermerk im Teilergebnis der technischen Gültigkeitsprüfung der Sperrliste hat keinen Einfluß auf die Verwendung der Vorhandenseins- bzw. Sperrinformation.

Im Falle der erneuten Prüfung archivierter Sperrlisten muß der Benutzer ihrer Verwendung zustimmen, wenn das Zwischenergebnis der Gültigkeitsprüfung auf "mso" oder "mu" lautet.

5.4.3.3.3 Gewährleistung der Sperrlistenfolge

Wenn eine Prüffunktion eine Sperrliste vor Ablauf ihres Gültigkeitszeitraums aktualisieren will, ist dies nur dann möglich, wenn von der Zertifizierungsstelle zwischenzeitlich eine neue Sperrliste bereitgestellt wurde. Andernfalls steht nur die bereits bekannte Sperrliste bereit. Daher müssen SigI-konformen Prüffunktion sicherstellen, daß eine neu abgerufene Sperrliste keine niedrigere Sperrlisten-Folgenummer hat, als die letzte abgerufene. Dadurch wird auch bei überlappenden Gültigkeitszeiträumen von Sperrlisten erreicht, daß ein Angreifer höchstens die letzte abgerufene Liste wieder einspielen kann, solange der Abrufzeitpunkt <= **nextUpdate**(Sperrliste) ist.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN für die Aktualisierung von Sperrlisten die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	crlNumber(neuer Sperrliste des **Issuers**) >= max(**crlNumber**(bereits bekannter technisch gültiger Sperrlisten des **Issuers**))	nicht erfüllt	tng

5.4.3.3.4 Konfiguration von $t_{Statusinfo}$

Sperrlisten weisen zwei Eigenschaften auf, die ihre Verwendung in Abhängigkeit vom Anwendungskontext im Verhältnis zu Verzeichnisdienstauskünften interessant machen kann: Zum einen enthalten Sie Sperrinformationen zu vielen Zertifikaten und zum zweiten werden sie für einen definierten Zeitraum ausgestellt. Sperrinformationen, die nur bis zu einem Referenzzeitpunkt < **thisUpdate** zur Prüfung verwendet werden, können als gesichert angenommen werden. Die zweite Eigenschaft vermeidet weitere online Verzeichnisdienstabfragen, wenn der Anwender annimmt, daß sich der Sperrstatus für ein Zertifikat im Zeitraum [**thisUpdate .. nextUpdate**] nicht ändert.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN die folgende Konfigurationsmöglichkeit für die Wahl von $t_{Statusinfo}$ bei der Auswertung der Statusinformationen aus Sperrlisten bieten:

- $t_{Statusinfo}$ für Statusinformationen aus neu abgerufenen Sperrlisten wird auf **thisUpdate** gesetzt[44] oder
- $t_{Statusinfo}$ für Statusinformationen aus neu abgerufenen Sperrlisten wird auf **nextUpdate** gesetzt.

Wenn $t_{Statusinfo}$ auf **nextUpdate** konfiguriert wird, MÜSSEN SigI-konforme Prüffunktionen sicherstellen, daß die Statusinformation "nicht gesperrt" *nicht wiederverwendet* wird, wenn zu einem Zertifikat eine neuere Sperrliste zur Verfügung steht. SigI-konforme Prüffunktionen MÜSSEN außerdem sicherstellen, daß eine neue Sperrliste abgefragt wird, wenn **nextUpdate** inzwischen überschritten wurde und t_{sig}(Prüfobjekt) > **thisUpdate**. Für diese Situation gilt die folgende Prüfbedingung:

Nr.	Prüfbedingung	Fall	Teilergebnis
	Nach dem Abruf liegt eine ausreichend aktuelle technisch gültige Sperrliste vor	t_{sig}(Prüfobjekt) > **thisUpdate** und $t_{Prüf}$ > **nextUpdate**	tnp

Hinweis: Durch diese Konfigurationsmöglichkeit können verschieden konfigurierte SigI-konforme Prüffunktionen zu unterschiedlichen Zeitpunkten zu unterschiedlichen Prüfergebnissen kommen, wenn sich der Sperrstatus eines relevanten Zertifikats im Gültigkeitszeitraum der Sperrliste ändert.

5.4.3.3.5 Verwendung von Statusinformationen aus Sperrlisten

Die in den abgerufenen und technisch gültigen Sperrlisten enthaltenen Statusinformationen müssen vor ihrer Verwendung darauf hin geprüft werden, welchem Zertifikat sie zuzuordnen sind. Für das jeweilige Zertifikat sind für die weitere Eignungsprüfung die relevanten Zeitangaben für Statusinformationen zu bestimmen.

R42) Der Zeitpunkt, zu dem die Sperrliste erzeugt wurde, wird in der Sperrliste durch das Attribut **thisUpdate** angegeben. Dabei muß berücksichtigt werden, daß die Zertifikate von Zertifizierungsstellen und Teilnehmerzertifikate nur bis t_E([$Zert_{Anf}$]) in den zugehörigen Sperrlisten geführt werden müssen.

Soweit Statusinformationen lokal verwaltet werden, MÜSSEN SigI-konforme Prüffunktionen sicherstellen, daß Konflikte zwischen den bereits vorhandenen und den neuen, aus Sperrlisten abgeleiteten Statusinformationen richtig aufgelöst werden. Dies bedeutet insbesondere:

- Zertifikate, die einen Sperrvermerk tragen, dürfen nicht mehr freigegeben werden.
- Zertifikate, die einen Vermerk "nicht vorhanden" mit einer zugeordneten $t_{Statusinfo}$ tragen, dürfen den Status "vorhanden" nur in Verbindung mit einer späteren $t_{Statusinfo}$ erhalten, wenn das Zertifikat in der Sperrliste gesperrt wurde.[45]

---

44 In diesem Fall wird die Annahmen für ein Zertifikat "nicht gesperrt" nur bis zum Zeitpunkt "**thisUpdate**" getroffen. Liegt t_{sig}(Prüfobjekt) nach **thisUpdate**, muß eine neuere Statusinformation beschafft werden. Die offline-Prüfung von digital signierten Dokumenten ist jedoch für alle Signaturen mit älterem t_{sig} möglich.

45 Die implizite Information, daß ein Zertifikat nicht in einer Sperrliste geführt wird und daher nicht gesperrt ist, ist nicht gleichbedeutend mit der Information, daß es vorhanden ist.

SigI-Konformitätsanforderungen

Auswertung der Sperreinträge:
Jedes in der Liste referenzierte Zertifikat hat den Sperrstatus "gesperrt". Als t_{Sperr} des betreffenden Zertifikats muß der Wert von **revocationDate** des entsprechenden Listeneintrags verwendet werden.

Sperrstatus nicht enthaltener Zertifikate für CRLs:
Die Statusinformation, daß ein Zertifikat "nicht gesperrt" sei, darf bei CRLs für alle vom Issuer der Sperrliste ausgestellten Zertifikate implizit getroffen werden. Dabei ist der Umfang der CRL in Abhängigkeit von der Gültigkeitsdauer der Teilnehmerzertifikate zu berücksichtigen.

Nr.	Prüfbedingung	Fall	Sperrstatus
	Es liegt eine technisch gültige CRL vor, die von **issuer** "[ZS]" ausgestellt wurde	Es gilt: • issuer([$Zert_i$)] = "[ZS]" und • $t_{nextUpdate}$(CRL) > t_B([$Zert_i$])[46] und • $t_{nextUpdate}$(CRL) < t_E([$Zert_{Anf}$])[47], wobei [$Zert_i$] das Anfangszertifikat der jeweiligen Kette ist oder in der Zertifikatkette zum Prüfen von [$Zert_{Anf}$] liegt	zum Zeitpunkt $t_{Statusinfo}$ ist [$Zert_i$] "nicht gesperrt"
		andere Fälle	mit dieser CRL ist keine Aussage zum Sperrstatus von [$Zert_i$] möglich

Da Angreifer versuchen können, eine früher ausgestellte Sperrliste unterzuschieben, MÜSSEN SigI-konforme Prüffunktionen auch für neu abgerufene Statusinformationen sicherstellen, daß sie gemäß den *Prüfbedingungen für vorhandene Statusinformationen* auf Eignung geprüft werden.

5.4.3.4 Statusinformationen aus anderen Quellen

Um auch Statusinformationen zur Prüfung verwenden zu können, die auf anderem Wege beschafft werden, beispielsweise über eine schriftliche Anfrage bei einer Zertifizierungsstelle, muß eine Eingabemöglichkeit vorgesehen werden.

---

46 Zertifikate können erst in der nächsten nach ihrem Gültigkeitsbeginn ausgestellten Sperrliste geführt werden. Der Verzicht auf diese Bedingung würde bei einer Auswertung alter Sperrlisten dazu führen, daß Zertifikate als "nicht gesperrt" bewertet würden, auch wenn die Sperrliste dazu keine Information gibt.

47 Diese Bedingung ist möglich, weil Zertifizierungsstellen-Zertifikate bis zum Ende des letzten nachgeordneten Zertifikats in der zugehörigen Sperrliste geführt werden müssen (vgl. die entsprechende Regel). Daher ist das Gültigkeitsende von [$Zert_{Anf}$], also dem Teilnehmerzertifikat der aktuell geprüften Kette, der Zeitpunkt, bis zu dem auch übergeordnete Zertifizierungsstellen-Zertifikate anhand der zugehörigen Sperrliste geprüft werden können. Auch die Zertifikate für die Dienste der Zertifizierungsstelle, z. B. [$Zert_{DIR}$] oder [$Zert_{TSS}$], sind in diesem Sinne als Teilnehmerzertifikat zu verstehen.

SigI-Konformitätsanforderungen "manuelle Eingabe"

SigI-konforme Prüffunktionen MÜSSEN die Möglichkeit bieten, Statusinformationen für ein Zertifikat manuell in den Prüfprozeß einzugeben. Die Eingabe der Daten muß den Vorhandenseinsstatus, den Sperrstatus und gegebenenfalls das Sperrdatum sowie $t_{Statusinfo}$ abfragen.

SigI-konforme Prüffunktionen MÜSSEN darauf hinweisen, wenn manuell eingegebene Statusinformationen im Widerspruch zu lokal verfügbaren stehen. Der Benutzer muß der weiteren Verwendung im Prüfprozeß explizit zustimmen.

SigI-konforme Prüffunktionen SOLLEN die Möglichkeit bieten, manuell eingegebene Statusinformationen lokal zur Wiederverwendung zu speichern.

5.5 Prüfbedingungen für Verzeichnisdienstauskünfte

Verzeichnisdienstauskünfte müssen auf technische Gültigkeit geprüft werden, um Manipulationen und Maskeradeangriffe abzuwehren.

5.5.1 Aufbau der Verzeichnisdienstauskunft

SigI-Konformitätsanforderungen

Für den Aufbau der Verzeichnisdienstauskunft sind die Prüfbedingungen nach Kapitel 4.1 zu überprüfen.

5.5.2 Mathematische Prüfung der Verzeichnisdienstauskunft

SigI-Konformitätsanforderungen

Für die mathematische Prüfung der Verzeichnisdienstauskunft sind die Prüfbedingungen nach Kapitel 4.2 zu überprüfen.

Wie dort beschrieben, ist als Teilnehmerzertifikat das über die Referenz **responderID** adressierte Zertifikat zu verwenden. `<?? Dieses Attribut bietet bisher nicht das Format Issuer und Seriennummer und ist deshalb nicht SigG-konform. Hier besteht Anpassungsbedarf.??>`

Das Zertifikat, das den Prüfschlüssel der Verzeichnisdienstauskunft enthalten soll,[48] wird im weiteren mit [$Zert_{Dir}$] bezeichnet. Das Zertifikat, auf das sich eine Verzeichnisdienstauskunft bezieht, wird im folgenden mit [$Zert_i$] bezeichnet.[49]

5.5.3 Prüfung des Namens des Signierenden

Angreifer können versuchen, Antworten des Verzeichnisdienstes unterzuschieben. Um dies zu verhindern, muß geprüft werden, ob der Issuer der Verzeichnisdienstauskunft berechtigt ist, diese Auskunft zu geben.

---

48 Diese Annahme wird erst durch die mathematische Prüfung des Primärdokuments bestätigt.

49 In einer Verzeichnisdienstauskunft können Statusinformationen zu mehreren Zertifikaten gegeben werden, wenn alle Zertifikate von gleichen Issuer ausgestellt wurden. In diesem Fall sind die Bedingungen für die Statusinformationen für [$Zert_i$] entsprechend des jeweiligen Zertifikats anzuwenden, auf die sich die Statusinformation bezieht.

R43) Verzeichnisdienstauskünfte müssen in der Sicherungsinfrastruktur nach SigI vom Issuer des Zertifikats signiert werden, dessen Vorhandenseins- und Sperrstatus geprüft werden soll.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	subject([$Zert_{Dir}$]) = issuer([$Zert_i$])	nicht erfüllt	tng

5.5.4 Bestimmen des Signaturzeitpunktes

Für den Signaturzeitpunkt, zu dem die Verzeichnisdienstauskunft erzeugt wurde, ist gefordert, daß er im Gültigkeitszeitraum des Teilnehmerzertifikats des Verzeichnisdienstes liegt. Außerdem muß das Zertifikat [$Zert_{Dir}$] zum Signaturzeitpunkt vorhanden, gültig und ungesperrt sein.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN als Signaturzeitpunkt der Verzeichnisdienstauskunft den Wert aus dem Attribut "**producedAt**" verwenden. Dieser Zeitpunkt wird im weiteren als t_{sig}(Verzeichnisdienstauskunft) bezeichnet.

Für weitere Zeitangaben in einer Verzeichnisdienstauskunft müssen Konsistenzbedingungen erfüllt werden.

R44) Die Zeitangaben zu "**thisUpdate**" und "**revocationTime**" in einer Verzeichnisdienstauskunft dürfen nicht nach dem Erzeugungszeitpunkt ("**producedAt**") liegen. Der Erzeugungszeitpunkt ("**producedAt**") darf nicht in der Zukunft liegen. Das BSI geht davon aus, daß diese Konsistenzbedingungen durch die Technikkomponenten von Zertifizierungsstellen, mit denen Verzeichnisdienstauskünfte erzeugt werden, sichergestellt werden. Die Anforderungen an die Zertifizierungsstelle sind durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchzusetzen.

Weitere Konsistenzbedingungen für den t_{sig}(Verzeichnisdienstauskunft) müssen daher nicht geprüft werden. Die Eignung der enthaltenen Statusinformationen muß jedoch sichergestellt werden (vgl. oben).

5.5.5 Prüfung des Teilnehmerzertifikats des Verzeichnisdienstes

Mit der Prüfung des Teilnehmerzertifikats, mit dem die Verzeichnisdienstauskunft geprüft wird, wird implizit die Prüfung der Zertifikatkette angestoßen. Daher ist eine zusätzliche explizite Prüfung der Zertifikatkette nicht erforderlich.

SigI-Konformitätsanforderungen

Das Zertifikat, in dem der Prüfschlüssel enthalten ist, muß ein Teilnehmerzertifikat sein. Die Sperrprüfung und die Prüfung des Gültigkeitszeitraums müssen auf den angenommenen Signaturzeitpunkt der Verzeichnisdienstauskunft bezogen werden.

Nr.	Prüfbedingung	Fall	Teilergebnis

	[$Zert_{Dir}$] ist ein technisch gültiges Teilnehmerzertifikat aus der Zertifizierungshierarchie von SigI. Es ist für einen Verzeichnisdienst ausgestellt. Als Referenzzeitpunkt für die zeitbezogenen Statusprüfungen ist t_{sig}(Verzeichnisdienstauskunft) zu verwenden.		Zwischenergebnis für das Prüfobjekt [$Zert_{Dir}$]

Die Prüfbedingungen für das Zertifikat sind in Kapitel 5.3 angegeben.

5.5.6 Bildung des Zwischenergebnisses

Die Teilergebnisse der technischen Gültigkeitsprüfung einer Verzeichnisdienstauskunft werden zu einem Zwischenergebnis zusammengefaßt. Dadurch wird entschieden, ob ein Prüfobjekt dritter Ordnung zur Verfügung steht oder im Prüfprozeß nicht verwertet werden kann. Durch die Regeln für die Bildung des Zwischenergebnisses werden alle Fälle, in denen keine verwertbare Verzeichnisdienstauskunft beschafft wurde, als "technisch nicht prüfbar" eingestuft. Dies sind die Fälle:

- mindestens eine Prüfbedingung "tng" oder
- mindestens eine Prüfbedingung "tnp", weil dann keine Aussage über die technisch Gültigkeit der Verzeichnisdienstauskunft getroffen werden kann, oder
- mindesten eine Prüfbedingung "mu" bzw. "mso", weil aktuelle Verzeichnisdienstauskünfte nur mit geeigneten Algorithmen erzeugt werden dürfen.

Das Zwischenergebnis entspricht damit der Situation, daß die Verzeichnisdienstauskunft nicht verfügbar ist, beispielsweise bei einer Netzwerkstörung.

Für archivierte Verzeichnisdienstauskünfte kann ein Ergebnis "mso" oder "mu" gegebenenfalls nach Entscheidung des Benutzers akzeptiert werden.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN für neu abgefragte Verzeichnisdienstauskünfte die folgende Funktionalität aufweisen:

Nr.	Teilergebnisse für die Prüfbedingungen der "Verzeichnisdienstauskunft"	Zwischenergebnis für die technische Gültigkeitsprüfung "Verzeichnisdienstauskunft"
	mindestens eine Prüfbedingung tng oder tnp oder mu oder mso	tnp
	"kp" Kennzeichnungen	"kp" Kennzeichnungen werden beibehalten
	pake	pake

5.6 Prüfbedingungen für Sperrlisten

Sperrlisten müssen auf technische Gültigkeit geprüft werden, um Manipulationen und Maskeradeangriffe abzuwehren.

5.6.1 Aufbau der Sperrliste

SigI-Konformitätsanforderungen

Für den Aufbau der Sperrliste sind die Prüfbedingungen nach Kapitel 4.1 zu überprüfen.

5.6.2 Mathematische Prüfung der Sperrliste

SigI-Konformitätsanforderungen

Für die mathematische Prüfung der Verzeichnisdienstauskunft sind die Prüfbedingungen nach Kapitel 4.2 zu überprüfen.

Wie dort beschrieben, ist als Teilnehmerzertifikat das über die Referenz **authorityKeyIdentifier** adressierte Zertifikat zu verwenden.

Das Zertifikat, das den Prüfschlüssel des Ausstellers der Sperrliste enthalten soll,[50] wird im weiteren mit [$Zert_{RI}$] bezeichnet. Das Zertifikat, auf das sich ein Sperreintrag bezieht, wird im folgenden mit [$Zert_i$] bezeichnet.[51]

5.6.3 Prüfung des Namens des Signierenden

Angreifer können versuchen, Antworten unterzuschieben. Um dies zu verhindern, muß geprüft werden, ob der Aussteller der Sperrliste berechtigt ist, diese Auskunft zu geben.

R45) Sperrlisten müssen in der Sicherungsinfrastruktur nach SigI vom Issuer des Zertifikats signiert werden, dessen Sperrstatus geprüft werden soll.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN die folgende Funktionalität aufweisen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	subject([$Zert_{RL}$]) = issuer([$Zert_i$])	nicht erfüllt	tng

5.6.4 Bestimmen des Signaturzeitpunkt

Für den Signaturzeitpunkt, zu dem die Sperrliste erzeugt wurde, ist gefordert, daß er im Gültigkeitszeitraum des Teilnehmerzertifikats des Ausstellers der Sperrliste liegt. Außerdem muß das Zertifikat [$Zert_{RL}$] zum Signaturzeitpunkt vorhanden, gültig und ungesperrt sein.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN als Signaturzeitpunkt der Verzeichnisdienstauskunft den Wert aus dem Attribut "**thisUpdate**" der Sperrliste verwenden. Dieser Zeitpunkt wird im weiteren als t_{sig}(Sperrliste) bezeichnet.

Für weitere Zeitangaben in einer Sperrliste müssen Konsistenzbedingungen erfüllt werden.

---

50 Diese Annahme wird erst durch die mathematische Prüfung des Primärdokuments bestätigt.

51 In einer Sperrliste können Statusinformationen zu mehreren Zertifikaten gegeben werden, wenn alle Zertifikate vom gleichen Issuer ausgestellt wurden. In diesem Fall sind die Bedingungen für die Statusinformationen für [$Zert_i$] entsprechend des jeweiligen Zertifikats anzuwenden, auf die sich die Statusinformation bezieht.

R46) Die Zeitangaben zu "**revocationDate**" in einer Sperrliste dürfen nicht nach dem Erzeugungszeitpunkt ("**thisUpdate**") liegen. Der Erzeugungszeitpunkt ("**thisUpdate**") darf nicht in der Zukunft liegen. Das BSI geht davon aus, daß diese Konsistenzbedingungen durch die Technikkomponenten von Zertifizierungsstellen, mit denen Sperrlisten erzeugt werden, sichergestellt werden. Die Anforderungen an die Zertifizierungsstelle sind durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchzusetzen.

Weitere Konsistenzbedingungen für den t_{sig}(Sperrliste) müssen daher nicht geprüft werden. Die Eignung der enthaltenen Statusinformationen muß jedoch sichergestellt werden, wie dies oben beschrieben wurde.

5.6.5 Prüfung des Teilnehmerzertifikats des Ausstellers der Sperrliste

Mit der Prüfung des Teilnehmerzertifikats, das den Prüfschlüssel für die Signatur der Sperrliste enthält, wird implizit die Prüfung der Zertifikatkette angestoßen. Daher ist eine zusätzliche explizite Prüfung der Zertifikatkette nicht erforderlich.

SigI-Konformitätsanforderungen

Das Zertifikat, in dem der Prüfschlüssel enthalten ist, muß ein Teilnehmerzertifikat sein. Die Sperrprüfung und die Prüfung des Gültigkeitszeitraums müssen auf den angenommenen Signaturzeitpunkt der Verzeichnisdienstauskunft bezogen werden.

Nr.	Prüfbedingung	Fall	Teilergebnis
	[$Zert_{RL}$] ist ein technisch gültiges Teilnehmerzertifikat aus der Zertifizierungshierarchie von SigI. Es ist zum Signieren von Sperrlisten ausgestellt. Als Referenzzeitpunkt für die zeitbezogenen Statusprüfungen ist t_{sig}(Sperrliste) zu verwenden.		Zwischenergebnis für das Prüfobjekt [$Zert_{RL}$]

Die Prüfbedingungen für das Zertifikat sind in Kapitel 5.3 angegeben.

5.6.6 Bildung des Zwischenergebnisses

Die Teilergebnisse der technischen Gültigkeitsprüfung einer Sperrliste werden zu einem Zwischenergebnis zusammengefaßt. Dadurch wird entschieden, ob ein Prüfobjekt dritter Ordnung zur Verfügung steht oder die Sperrliste im Prüfprozeß nicht verwertet werden kann. Durch die Regeln für die Bildung des Zwischenergebnisses werden alle Fälle, in denen keine verwertbare Sperrliste beschafft wurde, als "technisch nicht prüfbar" eingestuft. Dies sind die Fälle:

- mindestens eine Prüfbedingung "tng" oder
- mindestens eine Prüfbedingung "tnp", weil dann keine Aussage über die technisch Gültigkeit der Sperrliste getroffen werden kann, oder
- mindesten eine Prüfbedingung "mu" bzw. "mso", weil aktuelle Sperrlisten nur mit geeigneten Algorithmen erzeugt werden dürfen.

Das Zwischenergebnis entspricht damit der Situation, daß die Sperrliste nicht verfügbar ist, beispielsweise bei einer Netzwerkstörung.

Für archivierte Sperrlisten kann ein Ergebnis "mso" oder "mu" gegebenenfalls nach Entscheidung des Benutzers akzeptiert werden.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN für neu abgefragte Sperrlisten die folgende Funktionalität aufweisen:

Nr.	Teilergebnisse für die Prüfbedingungen der Sperrliste	Zwischenergebnis für die technische Gültigkeitsprüfung "Sperrliste"
	mindestens eine Prüfbedingung tng oder tnp oder mu oder mso	tnp
	kp	kp
	pake	pake

Anhang 1: Hinweise zur Erstprüfung von Wurzelzertifikaten

Für die Erstprüfung von Wurzelzertifikaten werden an dieser Stelle nur einige technische Konsistenzbedingungen angegeben. Die Prüfung gegen eine Veröffentlichung im Bundesanzeiger oder über andere Verteilmechanismen von Referenzinformationen ist nicht Gegenstand ist nicht Gegenstand dieses Teildokuments von SigI.

SigI-Konformitätsanforderungen

SigI-konforme Prüffunktionen MÜSSEN für die Aufnahme von Zertifikaten in die Liste der Wurzelzertifikate die Bedingungen aus Kapitel 4 einhalten.

Außerdem SOLLEN SigI-konforme Prüffunktionen die folgenden Konsistenzbedingungen vor der Aufnahmen von Zertifikaten in die Liste der Wurzelzertifikate prüfen:

Nr.	Prüfbedingung	Fall	Teilergebnis
	Der distinguished name der RegTP ist im Subject und im Issuer des Zertifikats enthalten	nicht erfüllt	MELDUNGSERGÄNZUNG
	Das Zertifikat ist ein Selbstzertifikat.	nicht erfüllt	MELDUNGSERGÄNZUNG
	Bewertung der Eignung der eingesetzten Verfahren gemäß zum Prüfzeitpunkt Kapitel 4	nicht erfüllt	mso / mu
	basicConstraints.cA([$Zert_{ZS}$]) ist "**true**" und **keyUsage.certSign**"([$Zert_{ZS}$]) ist gesetzt	nicht erfüllt	tng

Folgende ergänzende Hinweise für den Benutzer MÜSSEN gegeben werden:

- Die MELDUNGSERGÄNZUNGen müssen darauf hinweisen, daß die Abweichungen nur dann berechtigt sind, wenn die RegTP dafür besondere Gründe im Rahmen der Veröffentlichung des Zertifikats oder in ihrem CPS angegeben hat. Dies können beispielsweise eine Namensänderung oder eine Verkettung zwischen den Zertifikaten für die Wurzelschlüssel sein. Die Informationen müssen dem Benutzer vertrauenswürdig vorliegen.
- Die Teilergebnisse "mu" oder "mso" sind nur dann akzeptabel, wenn ein altes Wurzelzertifikat zur Prüfung alter digitaler Signaturen hinzugefügt werden soll. Andernfalls muß von einem Angriff ausgegangen werden.
- Ein Wurzelzertifikat mit dem Teilergebnis "tng" ist in keinem Fall akzeptabel.

Anhang 2: Voraussetzungen und Anforderungen an Zertifizierungsstellen

In den folgenden Absätzen sind die Voraussetzungen, Anforderungen und Hinweise zusammengefaßt, die in der Spezifikation der technischen Gültigkeitsprüfung in Form von Regeln als Grundlagen der Entwurfsentscheidungen verwendet wurden. Der Anhang dient als zusätzliche Übersicht über die im Text bereits aufgeführten Anforderungen. Sie sind textgleich dargestellt. Zusätzliche Anforderungen werden nicht definiert.

R1) Der Prüfende kann die Zertifikatkette zum Zertifikat des Prüfschlüssels und die Attribut-Zertifikate mit den zugehörigen Zertifikatketten, durch die die Urheberschaft und die Autorisierung des digital signierten Dokuments nachgewiesen wird, anhand der Referenzen auf das jeweils übergeordnete Zertifikat eindeutig rekonstruieren. Diese Voraussetzung ist erfüllt, weil nach SigI in jedem Prüfobjekt der eindeutige Verweis auf das zur Prüfung zu verwendende Zertifikat enthalten ist.

R2) Das BSI setzt voraus, daß in Zertifizierungsstellen nach SigI nur Zertifikate ausgestellt werden, deren Algorithmen und Schlüssellängen für den Gültigkeitszeitraum des Zertifikats geeignet sind. Dabei wird sichergestellt, daß die Algorithmen und Schlüssellängen, die für das Zertifikat der Zertifizierungsstelle und deren übergeordnete Zertifikate verwendet wurden, ebenfalls bis zum Ende des Gültigkeitszeitraums des Teilnehmerzertifikats geeignet sind. Diese Bedingungen sind durch das Sicherheitskonzept der Zertifizierungsstelle mit einem hohen Sicherheitsniveau durchzusetzen.

R3) Das BSI setzt voraus, daß von Zertifizierungsstellen nach SigI nur Zertifikate und Attribut-Zertifikate ausgestellt werden, deren Authentikatoren mit Hash-Verfahren erzeugt werden, die für den Gültigkeitszeitraum des Zertifikats geeignet sind. Dabei wird sichergestellt, daß auch die Hash-Verfahren, die für das Zertifikat der Zertifizierungsstelle und deren übergeordnete Zertifikate verwendet wurden, ebenfalls bis zum Ende des Gültigkeitszeitraums des Teilnehmerzertifikats geeignet sind. Diese Bedingungen sind durch das Sicherheitskonzept der Zertifizierungsstelle mit einem hohen Sicherheitsniveau durchzusetzen.

R4) Das BSI setzt voraus, daß von Zertifizierungsstellen nach SigI Verzeichnisdienstauskünfte nur mit aktuell geeigneten Verfahren signiert werden. Da die Zertifikate in der Zertifizierungsstelle mit geprüften Komponenten verwaltet werden und insofern gegen Verfälschung geschützt sind, werden durch die Signatur der Verzeichnisdienstauskunft auch die (alten) Zertifikate selbst gegen Verfälschung gesichert. Die Anforderungen an die Zertifizierungsstelle sind durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchzusetzen.

R5) Die Namensgebung für Zertifikate, die von Zertifizierungsstellen eingesetzt werden, muß die folgenden automatisierten Abläufe und Prüfbedingungen in Prüfprozessen berücksichtigen: Der distinguished name von Zertifizierungsstellen entspricht implizit der "Adresse", unter der im Directory die aktuellen Sperrlisten abgefragt werden können. Außerdem wird dieser Name verwendet, um zu entscheiden, ob der Signierende überhaupt eine bestimmte

Statusinformation bereitstellen darf. Um einfache Implementierungen der Prüffunktionen zu erlauben, wird auf die Grundregeln aus [ITU-T X.509 1997] zurückgegriffen. Danach muß der Name des Signierenden einer Standard-Sperrliste mit dem Namen des Ausstellers des zu prüfenden Zertifikats übereinstimmen. Eine entsprechende Annahme wird in dieser Spezifikation für den Namen des Signierenden von Verzeichnisdienstauskünften getroffen. Um einen geordneten Betrieb aufrecht zu erhalten, dürfen SigI-konforme Zertifizierungsstellen ihren distinguished name mit neuen Zertifikaten daher nicht wechseln, auch wenn sie neue Schlüsselpaare verwenden. Die Zertifikate, die zum Zertifizieren und zum Signieren von Verzeichnisdienstauskünften und Sperrlisten Zertifizierungsstelle ausgestellt werden, müssen den identischen distinguished name als Inhaber (subject) enthalten.

R6) Die Zertifizierungshierarchie nach SigG hat genau 3 Ebenen (Ebene 1 = RegTP, Ebene 2 = Zertifizierungsstellen, Ebene 3 = Teilnehmer-Zertifikate und Attribut-Zertifikate). Das BSI geht davon aus, daß eine SigI-konforme Zertifizierungsstelle auf Ebene 2 keine weiteren Zertifikate zum Ausstellen von Zertifikaten erzeugt. Implizit gilt für Zertifikatketten daher, daß sie maximal 3 Zertifikate enthalten dürfen. Das Attribut **pathLenConstraint** kann jedoch eingesetzt werden, um größerer Längen freizugeben. Es darf von SigI-konformen Zertifizierungsstellen nur mit Zustimmung der Wurzel-Zertifizierungsinstanz verwendet werden. Die Anforderungen an die einzelne Zertifizierungsstelle sind durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchzusetzen.

R7) Alle Selbstzertifikate der RegTP, die als Sicherungsanker für SigI verwendet werden sollen, genügen den Formatanforderungen von [BSI-ZERT]. Diese Anforderungen an die RegTP sind durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchzusetzen.

R8) Das BSI setzt voraus, daß Zertifizierungsstellen für die folgenden Attribute im oben beschrieben Sinn authentische Zeitangaben eintragen. Der Signaturzeitpunkt wird eingetragen in Zertifikaten und Attribut-Zertifikaten in "**dateOfCertGen**" [BSI-ZERT], in Zeitstempeln in "**tstTime**"; in Verzeichnisdienstauskünften in "**producedAt**" und in Sperrlisten und Zertifikatlisten in "**thisUpdate**". Diese Bedingungen sind durch das Sicherheitskonzept und die relevanten Technikkomponenten mit einem hohen Sicherheitsniveau durchzusetzen.

R9) Das Ende der Zertifikatkette bildet das Wurzelzertifikat. Für diesen Schlüssel liegt ein Selbstzertifikat $Zert_{RegTP}$ mit Gültigkeitszeitraum vor. Der Erzeugungszeitpunkt muß gegebenenfalls im Rahmen der Übernahme dieses Zertifikats in die Menge der Wurzelzertifikate geprüft werden. Diese Prüfung muß über andere Mechanismen, z. B. per Augenschein, erfolgen und ist nicht Gegenstand dieses Teildokuments von SigI.

R10) Unter der Gültigkeitsregel *Zertifikat-Gültigkeit* ist ein Signaturzeitpunkt genau dann technisch gültig, wenn er im Gültigkeitszeitraum des bestätigenden Zertifikats liegt. Die Kette der Zertifikate ist gültig, wenn jedes Zertifikat $[Zert_i]$ im Gültigkeitszeitraum des übergeordneten Zertifikats $[Zert_{i-1}]$ ausgestellt wurde.

R11) Zertifikate mit rückdatiertem Gültigkeitsbeginn sind nicht zulässig. Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingung durch das Sicherheitskonzept und die Technikausstattung mit einem hohen

Sicherheitsniveau durchgesetzt wird. Dadurch soll es Angreifern erschwert werden, rückdatierte Zertifikate auszustellen.

R12) Zertifikate mit vordatiertem Gültigkeitsbeginn sind zulässig. Das BSI setzt voraus, daß die Zertifizierungsstellen auch für vordatierte Zertifikate sicherstellen, daß der Gültigkeitszeitraum den Zeitraum der Eignung von Algorithmus und Schlüssellänge nicht überschreitet. Diese Bedingung ist durch das Sicherheitskonzept von Zertifizierungsstellen mit einem hohen Sicherheitsniveau durchzusetzen.

R13) Zertifizierungsstellen dürfen Zertifikate erst ab Gültigkeitsbeginn ihres Zertifikats zum Zertifizierungsstellen-Schlüssel ausstellen. Daraus folgt auch, daß der früheste Gültigkeitsbeginn eines nachgeordneten Zertifikats nach dem Gültigkeitsbeginn des übergeordneten Zertifikats liegen muß. Das BSI setzt voraus, daß die Zertifizierungsstellen diese Forderungen auch dann mit einem hohen Sicherheitsniveau sicherstellen, wenn sie Inhaber vordatierter Zertifikate sind.

R14) Zertifikate mit vordatiertem Gültigkeitsbeginn dürfen bereits vor dem Gültigkeitsbeginn gesperrt werden.

R15) Die maximale Gültigkeitsdauer (GD_{max}) von Zertifikaten und Attribut-Zertifikaten beträgt 5 Jahre (§ 7 SigV). Eine kürzere Gültigkeitsdauer ist zulässig (§ 7 SigV). Das BSI setzt voraus, daß Zertifizierungsstellen keine Zertifikate ausstellen, deren Gültigkeitsdauer > GD_{max} ist. Diese Bedingungen ist durch das Sicherheitskonzept der Zertifizierungsstellen mit einem hohen Sicherheitsniveau durchzusetzen.

R16) Attribut-Zertifikate sind nicht länger gültig als das Bezugszertifikat (§ 7 SigV). Das BSI setzt voraus, daß Zertifizierungsstellen keine Attribut-Zertifikate ausstellen, deren Gültigkeitsbeginn vor dem des Bezugszertifikats oder deren Gültigkeitsende nach dem des Bezugszertifikats liegt. Diese Bedingungen sind durch das Sicherheitskonzept der Zertifizierungsstellen mit einem hohen Sicherheitsniveau durchzusetzen.

R21) Das BSI fordert von SigI-konformen Zertifizierungsstellen, daß sie Verzeichnisdienstauskünfte nach [BSI-DIR] mindestens für einen Zeitraum von 10 Jahren ab dem Ausstellungszeitpunkt bereitstellen, auch wenn die verwendeten Algorithmen zu diesem Zeitraum bereits ungeeignet sind. Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingung durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt wird.

R22) Rückwirkende Sperrungen sind nicht zulässig (§ 8 (1) SigG).

R23) Sperrungen werden in keinem Fall aufgehoben (§ 9 SigV).

R24) Aus der Information, daß ein Zertifikat zu einem Zeitpunkt nicht gesperrt war, kann der Prüfende ableiten, daß es zu keinem Zeitpunkt vorher gesperrt war.

R25) Aus der Information, daß ein Zertifikat zu einem Zeitpunkt gesperrt war, kann der Prüfende ableiten, daß es jedem Zeitpunkt nachher ebenfalls gesperrt ist.

R26) Die Sperrung eines Zertifizierungsstellen-Zertifikats wird genauso interpretiert, wie die eines Teilnehmerzertifikats. Sie führt insbesondere nicht zur Sperrung des gesamten nachgeordneten Teilbaums. Lediglich Zertifikate, die

nach dem Sperrzeitpunkt ausgestellt wurden, werden als "technisch nicht gültig" bewertet.

R27) Sperrgründe werden bei der Auswertung von Sperrinformationen nicht berücksichtigt. Relevant für den Status eines Zertifikats "gesperrt" ist ausschließlich der Eintrag in der Sperrliste.

R28) Jede Zertifizierungsstelle darf jede Seriennummer nur einmal vergeben, unabhängig davon, ob sie einem Zertifizierungsstellen-Zertifikate, einem Teilnehmerzertifikate oder Attribut-Zertifikat zugeordnet wird. Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingungen durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt wird. Damit können alle Zertifikate unabhängig von ihrem Typ eindeutig über Issuer und Seriennummer referenziert werden.

R29) Die "normale" CRL einer Zertifizierungsstelle enthält grundsätzlich die Seriennummern aller Typen von Zertifikaten (Zertifizierungsstellen-Zertifikate, Teilnehmerzertifikate und Attribut-Zertifikate), die gesperrt wurden. Die Seriennummer eines gesperrten Zertifikats darf nach dem Gültigkeitsende des Zertifikats aus der CRL nur in Übereinstimmung mit den Regeln dieser Spezifikation entfernt werden. Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingungen durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt wird.

R30) Zertifizierungsstellen stellen sicher, daß sie nur CRLs bereitstellen. Die jeweils aktuelle CRL ist im X.500-Directory identisch in den beiden Attributen "**authorityRevocationList**" und "**certificateRevocationList**" im Directory-Eintrag der Zertifizierungsstelle abzulegen. Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingungen durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt wird.

R32) Das BSI nimmt an, daß in der Zertifizierungshierarchie nach SigG nur Zertifikate ausgestellt werden, die die genannte Verkettung von **subject** und **issuer** aufweisen. Diese Bedingung ist durch das Sicherheitskonzept der Zertifizierungsstelle mit einem hohen Sicherheitsniveau durchzusetzen.

R33) Das BSI geht davon aus, Zertifizierungsstellen nach SigI für Endanwender nur Teilnehmerzertifikate ausstellen, die nicht das Bit "**certSign"** und im Attribut **basicConstraints.cA** den Wert "**false**" enthalten. Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingung durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt wird. SigI-konforme Prüffunktionen KÖNNEN DESHALB DAVON AUSGEHEN, daß diese Prüfbedingung erfüllt ist.

R34) Das BSI geht davon aus, daß Zertifizierungsstellen nach SigI für Dienste von Zertifizierungsstellen nur Zertifikate ausstellen, die nicht das Bit "**certSign**" und im Attribut **basicConstraints.cA** den Wert "**false**" enthalten. Das BSI setzt voraus, daß in Zertifizierungsstellen diese Bedingung durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchgesetzt wird. SigI-konforme Prüffunktionen KÖNNEN DESHALB DAVON AUSGEHEN, daß diese Prüfbedingung erfüllt ist.

R35) Sind in einem Primärdokument Attribut-Zertifikate enthalten oder werden Attribut-Zertifikate referenziert, die sich nicht auf das Teilnehmerzertifikat mit dem Prüfschlüssel für das Primärdokument beziehen, ist das digital signierte Dokument "technisch nicht gültig".

Um einen gleitenden Wechsel der verschiedenen Schlüsselgenerationen zu erlauben, wird der RegTP empfohlen, bei regulären Schlüsselwechseln die Schlüssel zum Signieren von Verzeichnisdienstauskünften und Sperrlisten für einen Übergangszeitraum weiterzuverwenden und erst mit einer zeitlichen Verzögerung zu sperren.

R36) Eine einmal positiv gegebene Vorhandenseinsinformation kann zu einem Zertifikat nicht zurückgenommen werden. Sie ist für die Vorhandenseinsprüfung geeignet, wenn t_{Ref} nach $t_{Statusinfo}$ liegt. Zu einem Zeitpunkt vor $t_{Statusinfo}$ könnte das Zertifikat jedoch noch nicht freigegeben sein.

R37) Die Vorhandenseinsinformation "nicht vorhanden" zu einem Zertifikat ist nur geeignet, wenn der Ausstellungszeitpunkt der Vorhandenseinsinformation nach dem Referenzzeitpunkt liegt, zu dem das Vorhandensein von [$Zert_i$] geprüft werden soll. Zu einem späteren Zeitpunkt kann das Zertifikat jedoch vorhanden sein.

R38) Eine Sperrinformation "gesperrt ab [Zeitpunkt]" für ein Zertifikat ist in jedem Fall geeignet.

R39) Die Sperrinformation "nicht gesperrt" zu einem Zertifikats ist nur geeignet, wenn sie zu einem Zeitpunkt ausgestellt wurde, der nach dem Referenzzeitpunkt liegt.

R40) Eine Verzeichnisdienstauskunft ist für die Bereitstellung von Vorhandenseinsinformationen und Sperrinformationen geeignet. Der Zeitpunkt, zu dem eine Statusinformation für ein Zertifikat gilt, wird in der Verzeichnisdienstauskunft durch das Attribut **singleResponse.thisUpdate** angegeben.

R41) In Verzeichnisdienstanfragen kann die Referenzierung von Zertifikaten durch **request.certHash** abgesichert werden. SigI-konforme Verzeichnisdienste MÜSSEN sicherstellen, daß sie vor der Bestimmung einer Statusinformation für eine Verzeichnisdienstauskunft prüfen, ob **request.certHash** zum Hash-Wert des angefragten Zertifikats mathematisch korreliert. Andernfalls MÜSSEN sie die Antwort "**unknown**" geben.

R42) Der Zeitpunkt, zu dem die Sperrliste erzeugt wurde, wird in der Sperrliste durch das Attribut **thisUpdate** angegeben. Dabei muß berücksichtigt werden, daß die Zertifikate von Zertifizierungsstellen und Teilnehmerzertifikate nur bis $t_E([Zert_{Anf}])$ in den zugehörigen Sperrlisten geführt werden müssen.

R43) Verzeichnisdienstauskünfte müssen in der Sicherungsinfrastruktur nach SigI vom Issuer des Zertifikats signiert werden, dessen Vorhandenseins- und Sperrstatus geprüft werden soll.

R44) Die Zeitangaben zu "**thisUpdate**" und "**revocationTime**" in einer Verzeichnisdienstauskunft dürfen nicht nach dem Erzeugungszeitpunkt ("**producedAt**") liegen. Der Erzeugungszeitpunkt ("**producedAt**") darf nicht in der Zukunft liegen. Das BSI geht davon aus, daß diese Konsistenzbedingungen durch die Technikkomponenten von Zertifizierungsstellen, mit denen Verzeichnisdienstauskünfte erzeugt werden, sichergestellt werden. Die Anforderungen an die Zertifizierungsstelle sind durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchzusetzen.

R45) Sperrlisten müssen in der Sicherungsinfrastruktur nach SigI vom Issuer des Zertifikats signiert werden, dessen Sperrstatus geprüft werden soll.

R46) Die Zeitangaben zu "**revocationDate**" in einer Sperrliste dürfen nicht nach dem Erzeugungszeitpunkt ("**thisUpdate**") liegen. Der Erzeugungszeitpunkt ("**thisUpdate**") darf nicht in der Zukunft liegen. Das BSI geht davon aus, daß diese Konsistenzbedingungen durch die Technikkomponenten von Zertifizierungsstellen, mit denen Sperrlisten erzeugt werden, sichergestellt werden. Die Anforderungen an die Zertifizierungsstelle sind durch das Sicherheitskonzept mit einem hohen Sicherheitsniveau durchzusetzen.

Anhang 3: Geplante Erweiterungen

Offline Vorhandenseinsprüfung

Das BSI plant, auch für die Vorhandenseinsprüfung eine offline-Unterstützung zu spezifizieren. Dazu sollen durch Hashwertlisten die ausgestellten Zertifikate einer Zertifizierungsstelle nachweisen. In der Hashwertliste einer Zertifizierungsstelle werden je Zertifikat abgelegt:

- die Seriennummer
- ein Hash-Wert über das Zertifikat.

Die Hashwertliste soll mit einer Angabe zum Aussteller und einen Gültigkeitszeitraum versehen werden und wird vom Aussteller signiert.

Austauschformat für Eignungsinformationen

Bisher müssen Anwender die Informationen zur Eignung aus dem Bundesanzeiger entnehmen. Das BSI plant, ein Verfahren zur Verteilung von Informationen zur Eignung von Algorithmen zu spezifizieren. Dadurch kann auch die implizite und ungenaue Bindung der Eignung an die Gültigkeitsdauer von Zertifikaten abgelöst werden. Der Aufwand für ein rein manuelle Pflege solcher Information würde erheblich reduziert,

Literaturverzeichnis

BSI-AIS *BSI - Bundesamt für Sicherheit in der Informationstechnik (1999): Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV - SigI Abschnitt A3 Anwenderinfrastruktur, BSI, Bonn, 1999, Version 2.0. <ZS: BSI?99SzE3> <LR: BSI-AIS>*

BSI-DIR *BSI - Bundesamt für Sicherheit in der Informationstechnik (1999):* Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV - SigI Abschnitt A5 Verzeichnisdienst, BSI, Bonn, 1999, Version 2.0.

BSI-SIG *BSI - Bundesamt für Sicherheit in der Informationstechnik (1999):* Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV - SigI Abschnitt A2 Signatur, BSI, Bonn, 1999, Version 4.0.

BSI-TSS *BSI - Bundesamt für Sicherheit in der Informationstechnik (1999):* Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV - SigI Abschnitt A3 Zeitstempel, BSI, Bonn, 1999, Version 3.0.

BSI-ZERT *BSI - Bundesamt für Sicherheit in der Informationstechnik (1999):* Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV - SigI Abschnitt A1 Zertifikate, BSI, Bonn, 1999, Version 3.0.

Hammer, V. (1999): Die 2. Dimension der IT-Sicherheit - Verletzlichkeitsreduzierende Technikgestaltung am Beispiel von Public Key Infrastrukturen, Braunschweig/ Wiesbaden, 1999, im Erscheinen.

ITU-T X.509 - International Telecommunication Union - Telecommunication sector (1997): ITU-T Recommendation X.509 - Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 06/1997 (= ISO/IEC 9594-8), 1997 E.

ITU-T X.521 - International Telecommunication Union - Telecommunication sector (1995): ITU-T X.521 - The Directory - Selected Object Classes, 1995.

RFC 2459 - Housley, R. / Ford, W. / Polk, W. Solo, D. (1999): RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile, 1999.