DuD
Datenschutz und Datensicherheit

Signaturprüfungen nach SigI

Volker Hammer

Bei der Nutzung digital signierter Dokumente in der Praxis ist die Prüfung von Signaturen das wesentliche Element aus dem Vertrauenswürdigkeit abgeleitet wird . Der Beitrag stellt die grundlegenden Prüftatbestände für Prüffunktionen nach SigI vor und erläutert die Beziehungen zwischen verschiedenen Prüfobjekten.[40]

Dr.-Ing. Volker Hammer

Secorvo Security Consulting GmbH. Arbeitsschwerpunkt: Public Key Infrastrukturen, Anforderungsanalyse, Technikgestaltung
E-Mail: hammer@secorvo.de

[40] Der vorliegende Text ist eine überarbeitete Fassung eines Beitrags zur Konferenz „Systemsicherheit 2000".

Einleitung

Digital signierte Dokumente werden sich in der Praxis nur bewähren, wenn der Signierende absehen kann, dass seine elektronische Willenserklärung korrekt geprüft wird und unterschiedliche Prüfende – bis hin zum Richter – zu gleichen Ergebnissen kommen werden.

Das Signaturgesetz (SigG) setzt einige Rahmenbedingungen, durch die digitale Signaturen in den Genuss einer Sicherheitsvermutung [Roßn98] kommen sollen. Diese Vorgaben sind weitgehend technikoffen. Um mit konkreten Implementierungen die oben genannten Ziele zu erreichen, müssen daher präzise Spezifikationen entwickelt werden, die die Vorgaben des SigG aufgreifen und für Interoperabilität sorgen. Die *technische Gültigkeitsprüfung* (oder das *Gültigkeitsmodell*) kann dabei quasi als die Nagelprobe für die Interoperabilität angesehen werden: Nur wenn die Standards für die signierte Willenserklärung, für Zertifikate und für andere Prüfobjekte aufeinander abgestimmt sind und von der Prüffunktion korrekt ausgewertet werden, kann die Sicherheitsvermutung tragen. Und nur wenn die Prüffunktionen unterschiedlicher Hersteller zum gleichen Prüfergebnis kommen, ist Interoperabilität in der SigG-PKI (Public Key Infrastruktur) erreicht.

Dieser Beitrag fasst die Spezifikation der technischen Gültigkeitsprüfung nach SigI [BSI-GÜM] zusammen. Er gibt einen Überblick über die Prüfobjekte, Prüftatbestände und einige spezifische Prüfbedingungen.

1 Kontext von Signaturprüfungen

Digital signierte Dokumente versprechen hohe Sicherheit für den Nachweis der Integrität und der Urheberschaft – aber nur, wenn sie geprüft werden. Da eine Sichtprüfung des elektronischen Dokuments kein aussagekräftiges Ergebnis liefern kann und manuelle Verfahren wegen des Aufwandes in der Praxis nicht möglich sind, müssen technische Funktionen zur technischen Gültigkeitsprüfung eingesetzt werden.[41]

Besondere Anforderungen bestehen, wenn digitale Signaturen zur Sicherung rechtsverbindlicher Willenserklärungen nach SigG eingesetzt werden, aus deren technischer Gültigkeit eine Sicherheitsvermutung[42] abgeleitet wird. Dabei sollen nicht nur die spezifischen gesetzlichen Anforderungen untersucht und das gewünschte hohe Sicherheitsniveau auf der Seite des Prüfenden unterstützt werden, sondern auch zwei Prüfende mit Prüffunktionen unterschiedlicher Hersteller zum gleichen Prüfergebnis kommen. Das Gültigkeitsmodell[43] in der „Spezifikation zur Entwicklung interoperabler Verfahren nach SigG / SigV"[44] (Signatur-Interoperabilitätsspezifikation, SigI) definiert dazu den Prüfumfang und die Prüfergebnisse SigI-konformer Prüffunktionen.

Umfang von Prüfungen

Über die grundsätzlich erforderliche Prüfung der mathematischen Relation zwischen der digitalen Signatur und dem Prüfschlüssel hinaus können eine Vielzahl von Prüftatbeständen untersucht werden. Der Umfang der technischen Prüfungen wird dabei

[41] Siehe zu Prüfregeln auch [ITU-T X.509] oder [RFC 2459]. Letztere werden gegenwärtig aber bereits wieder überarbeitet, (draft-ietf-pkix-new-part1-00.txt). Sowohl X.509 als auch PKIX konzentrieren sich aber auf die Prüfung von Zertifikatketten und berücksichtigen die spezifischen Anforderungen nach SigG bisher nicht. Zu einem Architekturvorschlag für kontextabhängige Prüffunktionen vgl. auch [BePo 499, 225 ff.]. Probleme der Präsentation von digital signierten Dokumenten auch im Kontext der Prüfung diskutiert [Pord99]. Hinweise zu den Gültigkeitsregeln nach SigI finden sich auch bei [Baum99].

[42] [Roßn98, 3312 ff.] oder [Roßn99, Einl SigG Rn 5].

[43] [BSI-GÜM].

[44] Vgl. zu den anderen Teilen des Standards [BSI-DIR], [BSI-ZERT], [BSI-SIG], [BSI-AIS] und [BSI-TSS]. Erweiterungen von SigI sind in Vorbereitung (siehe unter www.bsi.bund.de/aufgaben/projekte/pbdigsig/index.htm).

wesentlich durch den Anwendungskontext bestimmt. Faktoren sind beispielsweise:

- besondere Anforderungen im Anwendungskontext, z. B. eine bestimmte Zeichnungsberechtigung,
- das Sicherheitsbedürfnis des Prüfenden und dessen Vertrauen in Zertifizierungsstellen,
- Prüftatbestände, die sich aus der „Policy" der jeweiligen Sicherungsinfrastruktur ergeben,
- Informationen, die aus der Zugehörigkeit zu einer bestimmten Zertifizierungshierarchie abgeleitet werden können (implizite Prüfergebnisse) und Angaben, die explizit und obligatorisch im Zertifikat enthalten sein müssen,
- Bedingungen, unter denen Interoperabilität gefordert wird oder erreicht werden kann.

Solche Faktoren bestimmen primär die Menge der Prüftatbestände. Die Anzahl der zu prüfenden Prüfobjekte wird dagegen wesentlich dadurch bestimmt, ob Prüfergebnisse wiederverwendet werden sollen oder ob jedes Prüfobjekt immer wieder neu zu prüfen ist. Darauf wird auch die Sicherheit von gespeicherten Prüfergebnissen in der Anwendungsumgebung Einfluss haben.

Kontext für Signaturprüfungen nach SigI

Im folgenden werden die Grundzüge der technischen Gültigkeitsprüfung nach SigI vorgestellt.[45] Für diese Signaturprüfungen sind zu berücksichtigen:

- die Vorgaben des Signaturgesetzes (SigG) und der Signaturverordnung (SigV),
- die weiteren Festlegungen der SigI-Spezifikation [BSI-DIR, BSI-ZERT, BSI-SIG],
- soweit möglich die internationalen Standards X.509 [ITU-T X.509] und PKIX [RFC 2459] und
- Entwurfsentscheidungen der Regulierungsbehörde für Telekommunikation und Post (RegTP) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Im Vergleich zu anderen Spezifikationen für Prüffunktionen ergeben sich durch die rechtlichen Vorgaben für die Public Key Infrastruktur und die Anwendung digitaler Signaturen nach SigG einige Besonderheiten, die in der Prüffunktion berücksichtigt werden müssen:

- Das SigG geht davon aus, dass die Kompromittierung des Schlüssels einer Zertifizierungsstelle durch eine Verzeichnisdienstauskunft beherrscht werden kann.[46] SigI-konforme Prüffunktionen müssen deshalb Vorhandenseinsprüfungen[47] durchführen können.
- Da digital signierte Dokumente zu einem Zeitpunkt als Beweismittel benötigt werden können, der lange nach dem Signierzeitpunkt liegt, muss das Prüfverfahren „Langzeitprüfungen" unterstützen. Daher sind unter anderem die Eignung von Algorithmen und die Eignung von Sperr- und Vorhandenseinsinformationen zum Prüfzeitpunkt zu berücksichtigen.
- Während in internationalen Standards gefordert wird, dass alle Zertifikate einer Zertifikatkette zum Prüfzeitpunkt gültig sein müssen, genügt es für SigG-Signaturen, dass das Zertifikat zum Signierzeitpunkt gültig war.[48]
- Um reproduzierbare Prüfergebnisse zu erreichen, fordert das SigG, dass Zertifikate der Zertifikatkette nicht ausgetauscht werden dürfen. Die Prüfung muss daher sicherstellen, dass immer das Zertifikat verwendet wird, auf das im jeweils geprüften Objekt verwiesen wird.
- Zu berücksichtigen ist auch die vom SigG auf maximal zwei Ebenen von Zertifizierungsstellen festgelegte Zertifizierungsinstanz-Hierarchie. Der Schlüsselwechsel nach dem Modell der RegTP muss damit auf unverkettete Wurzelzertifikate abgebildet werden.
- Schließlich fordert das SigG, dass von Zertifizierungsstellen Attribut-Zertifikate und Zeitstempel ausgestellt werden können. SigI-konforme Prüffunktionen müssen diese Prüfobjekte daher unterstützen und insbesondere den Zusammenhang mit der zugehörigen digital signierten Willenserklärung überprüfen können.

Für elektronische Dokumente, die rechtsverbindlich sein sollen, soll das Ergebnis einer Gültigkeitsprüfung dem Prüfenden anzeigen, ob er eine Willenserklärung als gültig akzeptieren oder ablehnen sollte. Dabei ist zu beachten, dass nicht jede „technisch gültige" Willenserklärung auch juristisch gültig sein muss und nicht jede „technisch nicht gültige" Willenserklärung auch juristisch ungültig ist. Beispielsweise kann ein technisch gültiger elektronischer Kaufvertrag mit einem Minderjährigen rechtlich unwirksam sein. Es ist auch denkbar, dass eine Willenserklärung, die durch die technische Prüfung abgelehnt wird, weil z. B. kein Zeitstempel beigefügt wurde und bis zum Prüfzeitpunkt das Teilnehmer-Zertifikat ausgelaufen war, dennoch vor Gericht Anerkennung findet.

Die technische Gültigkeitsprüfung kann eine rechtliche Prüfung daher nicht ersetzten. Mit Hilfe der technischen Gültigkeitsprüfung wird nach den Regeln des SigG festgestellt, ob die Willenserklärung mit dem im Gesetz vorgegebenen Sicherheitsniveau einem Urheber zugerechnet werden kann und unverfälscht ist. Insofern trägt das Ergebnis der technischen Prüfung allerdings wesentlich zur rechtlichen Bewertung bei.

Die Spezifikation einer technischen Gültigkeitsprüfung nach SigI verfolgt drei Ziele:

- Zum ersten soll das Prüfergebnis den juristischen Normen entsprechen, die vom Gesetzgeber bestimmt wurden.
- Zum zweiten soll die Konformität der Prüffunktion mit den technischen Vorgaben für digital signierte Dokumente und den Leistungen der Zertifizierungsstellen erreicht werden, z. B. dem Inhalt von Zertifikaten oder den Verzeichnisdienstauskünften.[49]
- Zum dritten schließlich soll erreicht werden, dass zwei unterschiedliche SigI-

[45] Vgl. dazu ausführlich [BSI-GÜM].

46 Die Verzeichnisdienstauskunft enthält Informationen darüber, ob der Zertifizierungsstelle ein vorgeblich von ihr ausgestelltes Zertifikat bekannt ist bzw. ob es bereits von ihr freigegeben wurde. Außerdem wird auch der Sperrstatus mitgeteilt.

[47] In der Vorhandenseinsprüfung wird geprüft, ob ein Zertifikat einem Verzeichnisdienst bekannt ist. Ist dies nicht der Fall, kann eine Unregelmäßigkeit in der Zertifizierungsstelle oder eine vorzeitige Verwendung des Signaturschlüssels vorliegen und das digital signierte Dokument wird als „technisch ungültig" abgelehnt.

[48] Die beiden Modelle haben unterschiedliche Vor- und Nachteile, die an dieser Stelle jedoch nicht diskutiert werden. Relevant sind hier nur die Vorgaben von SigG und SigV. Diese werden auch nicht durch die Policy der RegTP „überwunden", die mit überlappenden Gültigkeitsdauern in der Zertifizierungshierarchie beiden Modellen Rechnung tragen will.

[49] 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.

konforme Prüffunktionen für das gleiche digital signierte Dokument bei gleichem angenommenen Signierzeitpunkt zum gleichen Prüfergebnis kommen.

Diese Ziele müssen nicht nur für die eigentliche signierte Willenserklärung, sondern für eine Reihe von Prüfobjekten erreicht werden.

2 Prüfobjekte und Prüfprozess

Gegenstand der technischen Gültigkeitsprüfung sind digital signierte Dokumente nach SigI (*Prüfobjekte*). Dazu zählen auch Zertifikate, Zeitstempel, Verzeichnisdienstauskünfte oder Sperrlisten. Verschiedene Prüfobjekte haben eine unterschiedliche Rolle im Prüfprozess und können danach in die folgenden drei Klassen eingeteilt werden:

- Die Willenserklärung des Signierenden mit der digitalen Signatur nach [BSI-SIG] ist der eigentliche Gegenstand der technischen Gültigkeitsprüfung. Das digital signierte Dokument wird deshalb auch als Primärdokument bezeichnet und als *primäres Prüfobjekt* eingeordnet.
- Im Prüfprozess muss allerdings untersucht werden, ob die Urheberschaft des Primärdokuments sicher festgestellt werden kann. Dazu ist die Kette der *Zertifikate* [BSI-ZERT] vom Teilnehmerzertifikat bis zur Wurzel-Zertifizierungsinstanz zu prüfen und der Signierzeitpunkt festzustellen, möglichst mit Hilfe eines *Zeitstempels* nach [BSI-TSS]. Hinweise zur Autorisierung der digitalen Signatur des Primärdokuments können sich aus Zertifikaten und auch über *Attribut-Zertifikate* [BSI-ZERT] ergeben. Diese Prüfobjekte und die zugehörigen Zertifikatketten werden als *Prüfobjekte zweiter Ordnung* bezeichnet.
- Schließlich werden Verzeichnisdienstauskünfte oder Sperrlisten nach [BSI-DIR] benötigt, um den Vorhandenseins- und Sperrstatus von Zertifikaten und Attribut-Zertifikaten zu bewerten. Sie werden als *Prüfobjekte dritter Ordnung* bezeichnet.

Diese Unterscheidung zwischen Prüfobjekten dritter und zweiter Ordnung ist darin begründet, dass Prüfobjekte dritter Ordnung als zusätzliche Information zur Prüfung benötigt werden, um die Prüfobjekte zweiter Ordnung zu bewerten. Sind erstere „technisch nicht gültig“, dann wird eine Verzeichnisdienstauskunft oder Sperrliste nicht akzeptiert. In diesem Fall kann nicht entschieden werden, ob das Primärdokument als „technisch gültig“ zu bewerten ist, weil die notwendigen Informationen für den Prüfprozess fehlen. Im Unterschied zu Prüfobjekten erster oder zweiter Ordnung tragen „technisch nicht gültige“ Prüfobjekte dritter Ordnung zum Gesamtergebnis daher nur mit dem Resultat „technisch nicht prüfbar“ bei. Zertifikate, die nur zur Prüfung von Verzeichnisdienstauskünften und Sperrlisten benötigt werden,[50] werden ebenfalls in die Klasse der Prüfobjekte dritter Ordnung eingeordnet.

Für jedes Prüfobjekt sind im Rahmen einer technischen Gültigkeitsprüfung eine Reihe von Prüftatbeständen zu untersuchen, z. B.

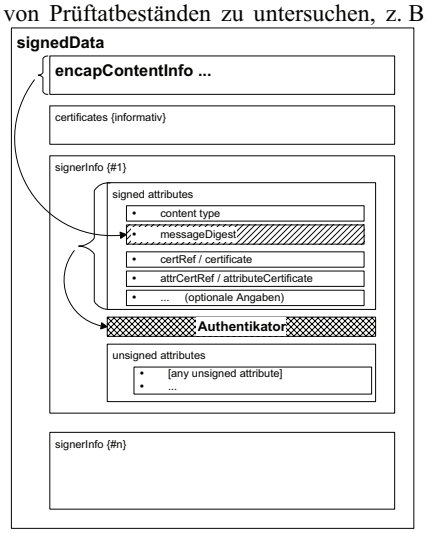

Abb. 1: Grundstruktur eines digital signierten Dokuments nach [BSI-SIG].

sein Aufbau oder der Status des Prüfschlüssels zum Signierzeitpunkt (zeitbezogene Statusprüfungen). Ob ein Prüftatbestand erfüllt ist, wird anhand einer oder mehrerer Prüfbedingungen entschieden. Die Beziehungen zwischen den Prüfobjekten werden im Prüfprozess ebenfalls durch Prüfbedingungen abgebildet, nach denen Prüfobjekte zweiter oder dritter Ordnung mit bestimmten Eigenschaften verfügbar sein müssen. Jede Prüfbedingung führt zu einem Einzelergebnis. Die Menge der Einzelergebnisse wird schließlich im Rahmen des Prüfprozesses zu einem Gesamtergebnis zusammengefasst (dazu und zu den Ergebnisklassen siehe unten).

Die weitere Darstellung gibt einen Überblick über die Prüftatbestände und stellt wichtige Besonderheiten der Gültigkeitsprüfung nach SigG / SigI dar. Für die Konkretisierung der Prüftatbestände zu Prüfbedingungen für die einzelnen Prüfobjekte muss an dieser Stelle aber auf [BSI-GÜM] verwiesen werden.

3 Prüftatbestände

Prüftatbestände sind die generischen Fragestellungen im Prüfprozess. Sie strukturieren die technische Signaturprüfung inhaltlich und sind im Rahmen der Spezifikation auf jedes Prüfobjekt anzuwenden und abzustimmen.

Aufbau von Prüfobjekten

Damit digital signierte Dokumente interoperabel nach SigI geprüft werden können, müssen sie einen bestimmten Aufbau aufweisen. Dazu ist zu prüfen, ob geforderte Attribute in der für das Prüfobjekt spezifizierten Struktur vorhanden und keine unbekannten Attribute enthalten sind (Vgl. z. B. die Struktur für Primärdokumente in Abb. 1).

Mathematische Prüfung

Für alle Typen von digital signierten Dokumenten muss die mathematische Relation zwischen der digitalen Signatur und dem jeweiligen Prüfschlüssel erfüllt sein. Als Besonderheit muss im Bereich des SigG sichergestellt werden, dass das Zertifikat, das den Prüfschlüssel enthält, eindeutig bestimmt werden kann. Andernfalls könnten im Laufe der Zeit durch unterschiedliche Zertifikatketten auch unterschiedliche Prüfergebnisse entstehen.

Um möglichen Fortschritten der Kryptanalyse Rechnung zu tragen, muss auch die Eignung von Verfahren und die Schlüssellänge bewertet werden. Diese Bewertung der Eignung muss zum Prüfzeitpunkt gegeben sein. Die Eignung wird zwar nach § 17 Abs. 2 SigV festgestellt und veröffentlicht, bisher wurden aber keine Protokolle und Formate definiert, um diese Informationen auch zur automatischen Verarbeitung bereitzustellen. Daher setzt das Gültigkeitsmodell nach der Vorgabe des BSI an dieser Stelle teilweise auf impliziten Informationen auf. Zertifizierungsstellen dürfen Zerti-

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

fikate nur bis zu einem Gültigkeitsende ausstellen, zu dem die Eignung der Algorithmen bestätigt ist. Der Prüfende darf daher davon ausgehen, dass die Eignung dieser Algorithmen für die Gültigkeitsdauer des jeweiligen Zertifikats gegeben ist. Nach dem Gültigkeitsende des Zertifikats kann auf dieser Grundlage jedoch keine zuverlässige Annahme zur Eignung von Algorithmen mehr getroffen werden. Informationen zur (vorzeitigen) Nichteignung und zu Hash-Verfahren müssen in der Prüffunktion bei Bedarf manuell verwaltet werden. Eine Besonderheit gilt für Zertifikate, die aus einer (technisch gültigen) Verzeichnisdienstauskunft bezogen werden. Der Prüfende darf auf die Integrität solchermaßen übermittelter Zertifikate vertrauen.

Name des Signierenden

Für den Erklärungsempfänger kann der Name des Signierenden für die Bewertung eines Primärdokuments wesentlich sein. Er wird deshalb in einer Meldungsergänzung zum Gesamtergebnis angezeigt. Für andere Prüfobjekte werden für Namen gegebenenfalls formal prüfbare Konsistenzbedingungen gefordert (siehe unten). Um Manipulationen zu verhindern, muss als Name des Signierenden die Angabe zum Subject aus dem Zertifikat verwendet werden, das den Prüfschlüssel enthält. Um sicherzustellen, dass der Name von einer SigI-konformen Zertifizierungsstelle bestätigt wurde, muss außerdem die Zertifikatkette geprüft werden.

Zulässigkeit von Zertifikatketten

Im Zertifizierungsmodell nach SigG ist eine zweistufige Zertifizierungsinstanz-Hierarchie vorgegeben. Dadurch wird die zulässige Länge von Zertifikatketten implizit auf drei Zertifikate begrenzt (Wurzelzertifikat, Zertifikat der Zertifizierungsstelle und Teilnehmerzertifikat).[51] Die Zertifikatkette muss in einem Wurzelzertifikat enden, das von der RegTP ausgestellt wurde. Da die RegTP in jedem Jahr ein neues Wurzelzertifikat etabliert, müssen Prüffunktionen nach SigI mehrere Wurzelzertifikate verwalten können, die gleichzeitig gültig sind. Jedes dieser Wurzelzertifikate ist als unabhängiger SigI-konformer Sicherungsanker zu betrachten.[52] Die Zertifikatketten verschiedener Prüfobjekte, z. B. Primärdokument, Zeitstempel und Verzeichnisdienstauskunft, können jeweils in unterschiedlichen Wurzelzertifikaten enden.

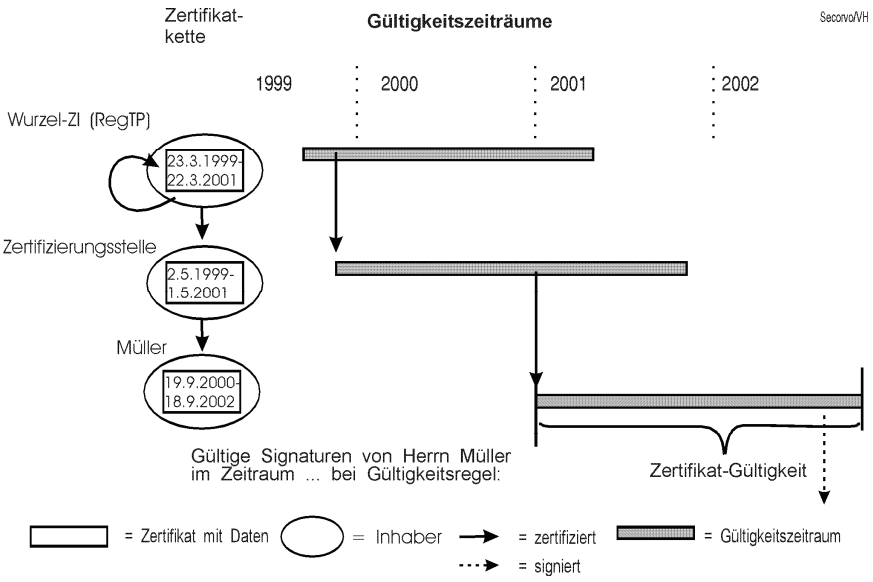

Abb. 2: Hinreichende Signierzeitpunkte bei Zertifikat-Gültigkeit

Zeitbezogene Statusprüfungen für Prüfschlüssel

Mit den zeitbezogenen Statusprüfungen für Prüfschlüssel wird festgestellt, ob das zugehörige Zertifikat zum Signierzeitpunkt vorhanden bzw. freigegeben[53], abgelaufen oder gesperrt war.

Die Internet-Standards PEM und PKIX verlangen, dass alle Zertifikate einer Zertifikatkette zum Prüfzeitpunkt gültig sein müssen (*Zertifizierungspfad-Gültigkeit* oder *Schalenmodell*) und nicht gesperrt sein dürfen. Nach der vom SigG vorgegebene Prüfpolicy muss dagegen ein Signierzeitpunkt nur im Gültigkeitszeitraum des Zertifikats liegen, das den Prüfschlüssel enthält (*Zertifikat-Gültigkeit* oder *Kettenmodell*).[54] Dieses Gültigkeitsmodell vermeidet, dass mit dem Auslaufen eines Zertifizierungsstellen-Zertifikats alle nachgeordneten Teilnehmerzertifikate ungültig werden. Während der Prüfung einer digitalen Signatur ist also zu untersuchen, ob der angenommene Erzeugungszeitpunkt im Gültigkeitszeitraum des übergeordneten Zertifikats liegt.

Für den Signierzeitpunkt des Primärdokuments soll im Kontext von SigI auf einen Zeitstempel zurückgegriffen werden. Falls dieser nicht verfügbar ist, kann der Prüfende alternativ den Eingangszeitpunkt oder auch den aktuellen Prüfzeitpunkt verwenden.[55] Je größer die Abweichung zwischen dem „echten“ und dem angenommenen Signierzeitpunkt ist, desto höher wird allerdings auch die Rate von false reject Fällen bei der Prüfung des Gültigkeitszeitraums

[51] Über das Attribut pathlenConstraints ist in SigI allerdings bereits eine Öffnung für „größere“ Zertifizierungshierarchien vorgesehen.

[52] Diese Sichtweise ist unabhängig von einer Verkettung der Schlüsselpaare der RegTP durch Crosszertifikate, die die Verteilung neuer Sicherungsanker erleichtert.

[53] Über das Attribut CertInDirSince nach [BSI-DIR, 25], kann der Prüffunktion mitgeteilt werden, seit wann ein Zertifikat im Verzeichnis geführt wird. Diese Option wurde allerdings erst nach dem Redaktionsschluss für [BSI-GÜM] ergänzt und ist dort deshalb noch nicht berücksichtigt.

[54] Vgl. zu den beiden Gültigkeitsmodellen auch [Hamm99, 561 ff.]und [Baum,99].

[55] Wenn der Prüfende einen zu frühen Signaturzeitpunkt annimmt, wird in der Prüfung möglicherweise eine Sperrung nicht berücksichtigt. Der „originäre“ Signaturzeitpunkt kann von Prüfenden aber kaum festgestellt werden. Die nächste gesicherte Annäherung erlaubt ein Zeitstempel. Da der Eingang des Dokuments beim Prüfenden nach der Signaturerzeugung liegen muss, sichert auch der Eingangszeitpunkt, dass eine zwischenzeitliche Sperrung berücksichtigt wird. Wenn auch der Eingangszeitpunkt nicht bekannt ist, kann mit noch größerer zeitlicher Abweichung auch der Zeitpunkt der Prüfung (Prüfzeitpunkt) als Signaturzeitpunkt angenommen werden.

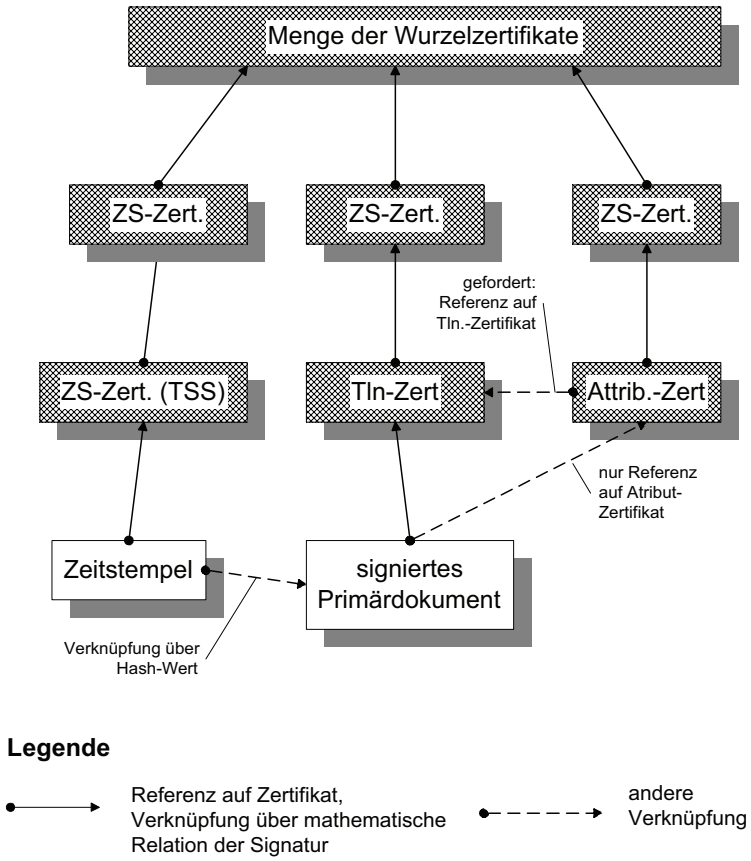

Abb. 3: Relationen zwischen Prüfobjekten ohne Sperrlisten und Verzeichnisdienstauskünfte

und Sperrprüfung sein.[56] Für Prüfobjekte, die von Zertifizierungsstellen erzeugt wurden, wird der Signierzeitpunkt aus Angaben im jeweiligen Prüfobjekt bestimmt. In diesen Fällen darf gemäß BSI davon ausgegangen werden, dass die enthaltenen Zeitangaben authentisch sind.

Die Vorhandenseinsprüfung ist eine weitere Besonderheit, die sich aus den gesetzlichen Vorgabe eines abfragbaren Verzeichnisses aller ausgestellten Zertifikate für jede Zertifizierungsstelle nach § 5 Abs. 1 SigG und der Prüfvorschrift aus § 16 Abs. 3 SigV ergibt. Anhand von Verzeichnisdienstauskünften untersucht die Prüffunktion, ob ein zu prüfendes Zertifikat zum Signierzeitpunkt bereits im Verzeichnis geführt wurde. Zusätzlich zur Vorhandenseinsprüfung ist auch eine Sperrprüfung durchzuführen. SigI bietet als Option zusätzlich Sperrlisten nach X.509 an. Als Quelle für Sperrinformationen können von SigI-konformen Prüffunktion daher sowohl Verzeichnisdienstauskünfte als auch Sperrlisten ausgewertet werden.

Sperrungen werden generell in der Weise berücksichtigt, dass Signaturen, die vor dem Sperrzeitpunkt erzeugt wurden, als „technisch gültig“ und Signaturen, die nach dem Sperrzeitpunkt erzeugt wurden, als „technisch nicht gültig“ interpretiert werden. Sind keine geeigneten Vorhandenseins- oder Sperrinformation verfügbar,[57] führt dies zum Teilergebnis „technisch nicht prüfbar“.

Zweck- und Autorisierungsprüfung

In der Zweck- und Autorisierungsprüfung wird untersucht, ob ein Prüfobjekt für den geforderten Zweck signiert wurde und der Signierer ausreichend autorisiert ist.

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

- ein Objectidentifier (OID) und der Aufbau[58], der den Typ des digital signierten Dokuments kennzeichnet,
- Zweckangaben im digital signierten Dokument, z. B. zur Unterscheidung von CRL und ARL, und
- Zweckangaben des Zertifikates, das den Prüfschlüssel bestätigt, z. B. die Angabe im Attribut `keyUsage` oder `basicConstraints`.

Angaben zur Autorisierung drücken Nutzungsbeschränkungen und -berechtigungen aus. Zu untersuchen ist, ob der jeweilige Prüfschlüssel im Kontext von SigI zertifiziert (Angabe in `certificatePolicies`) und ob in das Zertifikat von der Zertifizierungsstelle eine besondere Berechtigung oder Nutzungsbeschränkung aufgenommen wurde. Die Informationen können aus den Attributen `certificatePolicies`, `keyUsage`, `extKeyUsage`, `liabilityLimitationFlag` (Kennzeichnung einer Beschränkung über ein Attribut eines Attribut-Zertifikats), `procuration` (Vertretungsmacht), `admission` (Zulassung), `monetaryLimit` (Monetäre Beschränkung), `declarationOfMajority` (Volljährigkeit) oder `restriction` (sonstige Einschränkungen) entnommen werden.

Für die Autorisierung des Primärdokuments sind nicht nur die Angaben im Zertifikat, sondern auch in Attribut-Zertifikaten, die dem digital signierten Dokument hinzugefügt wurden, zu berücksichtigen. Einige dieser Angaben müssen anwendungsspezifisch bewertet werden, z. B. eine Berufszulassung oder Vertretungsmacht. Sie werden daher nach SigI nicht technisch geprüft, sondern dem Prüfenden im Gesamtergebnis als zusätzliche als Informationen dargestellt.

4 Spezifische Prüfbedingungen

An dieser Stelle wird exemplarisch auf einige spezifische Prüfbedingungen eingegangen, durch die die Bezüge der Prüfobjekte untereinander sichergestellt (vgl. Abb. 3) oder durch die der Zweck bzw. die Autorisierung eines Prüfobjekts nachgewiesen werden.

[56] Unter diesem Gesichtspunkt empfiehlt sich die frühzeitige Beantragung eines Zeitstempels bereits durch den Signierenden, der ihn mit dem digital signierten Dokument verschicken kann. Andererseits kann der Prüfende unter Inkaufnahme von false reject Fällen bewusst einen späteren Zeitpunkt zur Prüfung verwenden, um zwischenzeitliche Sperrungen zu berücksichtigen.

[57] Siehe zur Eignung solcher Informationen unten.

[58] Insofern ergeben sich Überschneidungen mit dem Prüftatbestand zum Aufbau des Prüfobjekts.

Zeitstempel

Zeitstempel sollen die Signierzeitpunkte digital signierter Dokumente nachweisen. Damit ein Zeitstempel für eine Prüfung aussagekräftig ist, muss er sich auf das Primärdokument beziehen. Prüfbedingung ist, dass der im Zeitstempel enthaltene Hash-Wert des Primärdokuments mit einem aktuell gebildeten Wert übereinstimmt. Das Hash-Verfahren muß gemäß SigI geeignet sein.

Der Zeitstempel selbst muss nach der SigI-Policy für Zeitstempel erzeugt worden sein (`TSTInfo.policy` enthält den OID für „Id-sigi-sigts-sigconform“). Außerdem muss sichergestellt werden, dass der Zeitstempel nicht von einer beliebigen Instanz, sondern von einem SigI-konformen Zeitstempeldienst ausgestellt wurde. Dazu müssen die Autorisierungen im Zertifikat des Zeitstempeldienstes überprüft und die SigI-Konformität der Zertifikatkette sichergestellt werden.

Attribut-Zertifikate

Attribut-Zertifikate werden verwendet, um zusätzliche Informationen über einen Schlüsselinhaber bereitzustellen. Das Primärdokument kann ein oder mehrere Attribut-Zertifikate enthalten oder auf solche verweisen (vgl. `attrCertRef` in Abb. 1). Die jeweils enthaltenen Zweck- und Autorisierungsinformationen müssen im Gesamtergebnis angezeigt werden. Jedes der im Primärdokument verwendeten Attribut-Zertifikate muss sich außerdem auf das Teilnehmerzertifikat beziehen, das den Prüfschlüssel zum Primärdokument enthält. Dazu muss der Verweis auf das Bezugszertifikat (Issuer und Serialnumber in `baseCertificateID` des Attribut-Zertifikats) mit Issuer und Serialnumber des zum Prüfen des Primärdokument verwendeten Zertifikats übereinstimmen. Auch für die Attribut-Zertifikate müssen zum Signierzeitpunkt des Primärdokuments die zeitbezogenen Statusprüfungen erfüllt und die Zertifikatketten technisch gültig sein. Anwendungsspezifische Prüfbedingungen für Attribut-Zertifikate sind nicht Gegenstand der SigI-Gültigkeitsprüfung.

Statusinformationen

Für alle Zertifikate müssen Vorhandenseins- und Sperrprüfung durchgeführt werden. Die dazu notwendigen Statusinformationen werden über besondere digital signierte Dokumente der Zertifizierungsstellen bereitgestellt (*Verzeichnisdienstauskünfte*). Verzeichnisdienstauskünfte enthalten Informationen über die Freigabe und den Sperrstatus eines Zertifikats. Sie können für einzelne Zertifikate zeitnah bezogen werden. Zusätzlich können von Zertifizierungsstellen nach SigI auch *Sperrlisten* angeboten werden, die jedoch nur über gesperrte Zertifikate informieren. Sie decken zwar eine Menge von Zertifikaten ab, werden typischerweise aber nur in gewissen Zeitabständen aktualisiert. Welcher Prüfumfang abzuarbeiten ist und woher die Informationen bezogen werden müssen, muss in SigI-konformen Prüffunktion konfiguriert werden können.

Um bereits eingeholte Informationen lokal wiederverwenden zu können, schlägt [BSI-GÜM] eine interne Verwaltung durch die Prüffunktion vor. Für die Wiederverwendung muss allerdings neben der Integrität auch die Eignung der lokalen Statusinformationen gegeben sein.

Aussteller und Autorisierung

Sperrlisten und Verzeichnisdienstauskünfte zu einem Zertifikat dürfen nur von bestimmten Instanzen ausgestellt werden. Soweit keine Sonderformen zur Bereitstellung eingesetzt werden, muss deshalb der Name des Ausstellers einer Statusinformation gleich dem Namen des Issuers des Zertifikats sein, für das der Status geprüft wird. Die Prüffunktion darf Statusinformationen nur aus den dafür vorgesehenen digital signierten Dokumenten verwenden. Sie muss dazu prüfen, ob eine Verzeichnisdienstauskunft oder eine Sperrliste vorliegt (Aufbau) und ob insbesondere auch das Zertifikat des Ausstellers zum Signieren dieser Informationen berechtigt (Attribute `keyUsage` und `extKeyUsage` geeignet belegt).

Eignung

Um zu entscheiden, ob eine bestimmte Statusinformation für ein Zertifikat überhaupt aussagekräftig ist, muss die Prüffunktion die hinter den Konzepten stehenden „Pflegemodelle“ des Zertifikat-Managements berücksichtigen. Ein Zertifikat muss in den Sperrlisten einer Zertifizierungsstelle gemäß X.509 nur solange geführt werden, bis sein Gültigkeitszeitraum abgelaufen ist. Für Verzeichnisdienstauskünfte wird dagegen in [BSI-GÜM] gefordert, dass sie mindestens für einen Zeitraum von 10 Jahren ab dem Ausstellungszeitpunkt bereitgestellt werden. Prinzipiell unterliegen Zertifizierungsstellen zwar längeren Dokumentationspflichten. Es ist aber nicht gefordert, dass die darauf basierenden Auskünfte automatisiert erteilt werden.

Die Prüffunktion kann anhand der Relationen zwischen Prüfzeitpunkt, Signierzeitpunkt und dem Erstellungszeitpunkt der Statusinformation bestimmen, ob eine Statusinformation für den aktuellen Prüfprozess geeignet ist. Beispielsweise ist eine Sperrliste einer Zertifizierungsstelle nicht mehr für ein bestimmtes Zertifikat aussagekräftig, wenn sie nach dem Gültigkeitsende des Zertifikats ausgestellt wurde. Eine Verzeichnisdienstauskunft mit der Statusinformation „good“ muss nach dem Signierzeitpunkt erstellt worden sein, um den Sperrstatus zum Signierzeitpunkt wiederzugeben. Entsprechend kann eine Vorhan-

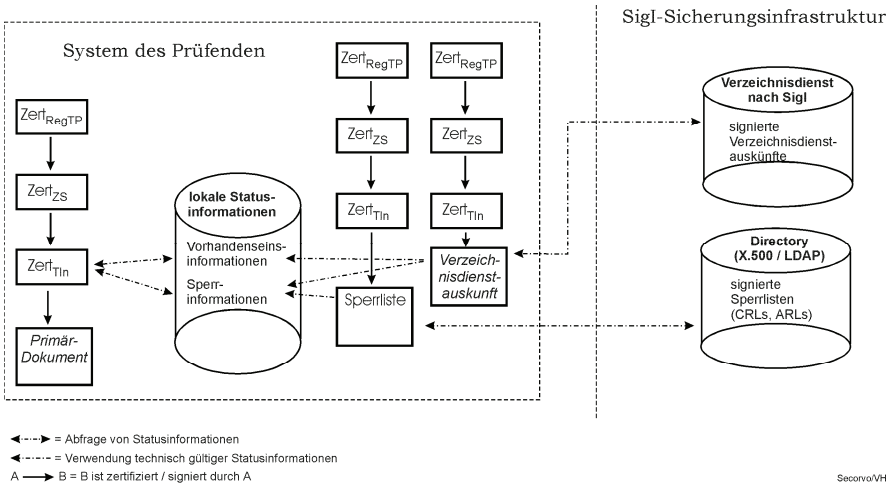

Abb. 4: Bereitstellung von Statusinformationen am Beispiel eines Teilnehmerzertifikats

denseinsinformation nur verwendet werden, wenn sie bereits für den Signierzeitpunkt aussagekräftig ist, also entweder vorher erstellt wurde oder ein Freigabedatum enthält. Für weitere Details und Fälle sei auf [BSI-GÜM] verwiesen.

Die Eignungsinformationen werden lokal gespeichert. Dadurch muss die Prüffunktion nur dann neue Informationen anfordern, wenn die vorhandenen Daten nicht geeignet sind. Unter Umständen kann das lokale Archiv auch Statusinformationen für Prüfungen bereitstellen, in denen ein lange zurückliegender Signierzeitpunkt angenommen wird.

5 Prüfergebnis

Ziel der technischen Gültigkeitsprüfung ist ein möglichst einfaches Prüfergebnis, mit dem der Empfänger eines digital signierten Dokuments entscheiden kann, ob er es akzeptieren will. Aus der Menge der Ergebnisse für die oben skizzierten Prüfbedingungen wird daher ein Gesamtergebnis abgeleitet. Das Gesamtergebnis soll allerdings zwei sich widersprechenden Zielen genügen. Zum einen soll der Prüfende mit einem „kurzen Blick" entscheiden können, ob er die signierte Willenserklärung akzeptieren will oder nicht. Zum anderen soll der Prüfende die Details dieses Prüfergebnisses zur Kenntnis nehmen können, insbesondere um im Falle des Ergebnisses „technisch nicht gültig" differenzierter bewerten oder um berücksichtigte und nicht berücksichtigte Prüfbedingungen[59] nachvollziehen zu können. Wenn er dies will, soll er auch die Details eines „technisch gültigen" Prüfergebnisses nachvollziehen können.

Um beiden Zielen nachzukommen, werden in [BSI-GÜM] sechs abstrakte Ergebnisklassen gebildet, die dem Prüfenden eine schnelle Bewertung ermöglichen:

- Werden eine oder mehrere Prüfbedingungen, die technisch überprüfbar sind, nicht erfüllt, lautet das Gesamtergebnis: *„Signatur technisch nicht gültig."* Die unzureichende Eignung von Algorithmen wird allerdings gesondert behandelt (siehe unten), weil sie im Rahmen von Langzeitprüfungen vom Prüfenden differenziert bewertet werden muss.
- Können bestimmte Prüfbedingungen nicht überprüft werden, weil die dazu notwendigen Informationen aus Prüfobjekten dritter Ordnung nicht oder nicht ausreichend aktuell vorliegen, und sind alle anderen Prüfbedingungen erfüllt, lautet das Gesamtergebnis: *„Signatur technisch nicht prüfbar."*
- Der Prüffunktion können Informationen zur Verfügung stehen, die einen oder mehrere Algorithmen oder eine Schlüssellänge als unsicher kennzeichnen. Können alle technischen Prüfbedingungen, soweit sie nicht die Eignung von Algorithmen betreffen, geprüft werden und sind sie erfüllt, lautet in diesem Fall das Gesamtergebnis: *„Sicherheitsvermutung nicht gegeben: Signatur mathematisch unsicher, alle anderen technischen Prüfbedingungen werden erfüllt."*
- In Zertifikaten werden Algorithmen angegeben. Der Prüfende darf davon ausgehen, dass die Eignung dieser Algorithmen gegeben ist, falls der Prüfzeitpunkt vor dem Gültigkeitsende des Zertifikats liegt und keine Informationen zur Nichteignung bekannt gegeben wurden. Falls das Gültigkeitsende bereits überschritten ist, besteht jedoch Unsicherheit über die Eignung dieser Algorithmen. 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."*

Das Gesamtergebnis wird um Zusatzinformationen ergänzt, z. B. den Namen des Signierenden oder unbekannte Erweiterungen in einem Prüfobjekt mit `criticalFlag` = „false".

Zusätzlich zu diesem Gesamtergebnis muss der Prüfende mit einer SigI-konformen Prüffunktion die Möglichkeit haben, alle Teilergebnisse eines Prüfprozesses festzustellen. Wenn ihm ein Gesamtergebnis zu wenig Informationen bietet, kann er dadurch für jede Prüfbedingung jedes Prüfobjekts im Detail feststellen, welchen Beitrag sie zum Gesamtergebnis geleistet hat.

Fazit

Die Serie der SigI-Spezifikationen setzen die Vorgaben des SigG um, die beispielsweise durch einige Prüfbedingungen von PKIX[60] nicht erfüllt werden. Die technische Gültigkeitsprüfung definiert die Prüfbedingungen für die einzelnen Objekte eines Prüfprozesses so detailliert, dass herstellerunabhängig das gleiche Prüfergebnis erwartet werden kann. Die Spezifikation der technischen Gültigkeitsprüfung schafft daher eine wesentliche Grundlage für einen interoperablen elektronischen Rechtsverkehr. SigI ist allerdings nur eine Empfehlung und für die Betreiber von Zertifizierungsinstanzen und die Teilnehmer am elektronischen Rechtsverkehr nach SigG nicht verbindlich.

Der Umfang der Spezifikation für die technische Gültigkeitsprüfung nach SigI im Vergleich bspw. zum Vorschlag von PKIX hat mehrere Ursachen. SigI berücksichtigt die Bedingungen einer „Langzeitprüfbarkeit". Im Unterschied zu PKIX werden in SigI auch alle Prüfobjekte und ihre Beziehungen untereinander in Prüfbedingungen spezifiziert. PKIX berücksichtigt bisher nur Zertifikatketten. Dagegen dürften die Unterschiede zu PKIX in der Prüfung der Gültigkeitszeitraums und der Sperrprüfung im wesentlichen nur zu anderen und nicht zu komplizierteren Prüfbedingungen führen. Zusätzliche Komplexität ist dagegen der Vorhandenseinsprüfung und den Attribut-Zertifikaten geschuldet. Während Vorhandenseinsprüfungen Unregelmäßigkeiten in Zertifizierungsstellen und Schlüsselkompromittierung aufdecken sollen, bilden Attribut-Zertifikate das Modell von Bescheinigungen zu einem „zentralen Ausweis" ab. Ob sich diese beiden Ansätze des Gesetzgebers in der Praxis bewähren, muss die Anwendung SigI-konformer Signaturen in den nächsten Jahren zeigen.

Nächste Schritte in der Weiterentwicklung des Standards zur technischen Gültigkeitsprüfung nach SigI sollten die Integration von Mehrfachsignaturen, z. B. Gegenzeichnung oder „erneute digitale Signaturen", und eine weitere Abstimmung zu den Vorgaben für die Anwenderinfrastruktur sein. Im Kontext einer Weiterentwicklung

[59] Es sind Konfigurationsmöglichkeiten vorgesehen, durch die die Prüftiefe begrenzt werden kann, z. B. durch den Verzicht auf Vorhandenseinsprüfungen von Zertifizierungsstellen-Zertifikaten. Der Prüfende erhöht damit allerdings sein Risiko eines „false accept" einer digitalen Signatur.

60 Zu einigen anderen Unterschieden zwischen PKIX und SigI siehe [Hets99].

der SigI-Standards sollte auch nochmals systematisch überprüft werden, welche denkbaren Störfälle mit den bisher definierten Gültigkeits- und Sperregeln beherrscht werden. SigG und PKIX verfolgen hier unterschiedliche Strategien, die jeweils ihre spezifischen Vor- und Nachteile aufweisen.[61] Es könnte für beide Standards sinnvoll sein, sie jeweils um die anderen Konzepte zu ergänzen. Schließlich bleibt auch abzuwarten, ob das Gültigkeitsmodell vor dem Hintergrund von EU-Regelungen angepasst oder differenziert werden muss.

Literatur

[Baum99] *Baum, Michael*: Das Gültigkeitsmodell des Signaturgesetzes. DuD 4/1999, S. 199-205.

[BePo99] *Berger, A. / Pordesch, U. (1999):* Kontextabhängige Gültigkeitsprüfung digitaler Signaturen, in: Baumgart, R. / Rannenberg, K. / Wähner, D. / Weck, G. (1999, Hrsg.): Verläßliche Informationssysteme – IT-Sicherheit an der Schwelle des neuen Jahrtausends, Braunschweig/ Wiesbaden, 1999, 225 ff.

[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.

[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 3.0.

[BSI-GÜM] *BSI – Bundesamt für Sicherheit in der Informationstechnik (1999):* Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV – SigI Abschnitt A6 Gültigkeitsmodell, BSI, Bonn 1999, Version 1.1.

[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 6.1.

[BSI-TSS] *BSI – Bundesamt für Sicherheit in der Informationstechnik (1999):* Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV – SigI Abschnitt A4 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.

[Hamm99] *Hammer, V. (1999):* Die 2. Dimension der IT-Sicherheit – Verletzlichkeitsreduzierende Technikgestaltung am Beispiel von Public Key Infrastrukturen, Braunschweig/ Wiesbaden, 1999.

[Hets99] *Hetschold, Thomas*: PKI-Interoperabilität: PKIX und SigI im Vergleich. DuD 4/1999, S. 213-217.

[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.

[Pord99] *Pordesch, U. (1999):* Nachweis der Präsentation signierter Daten, GMD Report 68, Darmstadt, 1999.

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

[Roßn98] *Roßnagel, A. (1998):* Die Sicherheitsvermutung des Signaturgesetzes, NJW 45/1998, 3312 ff.

[Roßn99] *Roßnagel, A. (1999, Hrsg.):* Recht der Multimediadienste, München, Loseblatt, Stand Januar 1999.

Hinweis: Die Dokument der SigI-Spezifikation [BSI-DIR], [BSI-ZERT], [BSI-SIG], [BSI-AIS] [BSI-TSS] und [BSI-GÜM] stehen unter www.bsi.bund.de/aufgaben/projekte/pbdigsig/index.htm zum Abruf zur Verfügung.

[61] Vgl. zu verschiedenen Aspekten [Hamm99, 536 ff. und 561 ff.].