Gültigkeitsmodell der elektronischen Arztausweise und Laufzeit der Zertifikate

Gültigkeitsmodelle beschreiben den Algorithmus nach dem ein Client oder Dienst entscheidet, ob eine Signatur, ein Authentisierungsvorgang oder ein Zertifikat als gültig oder ungültig betrachtet wird.

Im Geltungsbereich des Signaturgesetzes gilt das so genannte „Kettenmodell“. Nach dem Kettenmodell ist eine Signatur (über ein Dokument) gültig, wenn zum Zeitpunkt der Signaturerstellung das zugrunde liegende Signaturzertifikat gültig war. Dabei ist es unerheblich, ob übergeordnete Zertifikate (CA- und Root-Zertifikate) zum Zeitpunkt der Signaturerstellung ungültig waren. Entscheidend für die Gültigkeit eines Zertifikats ist lediglich, dass zum Zeitpunkt seiner **Produktion** die jeweils übergeordneten Zertifikate (Aussteller) gültig waren.

Im Schalenmodell (oder PKIX-Modell) wird ein Zertifikat als gültig betrachtet, wenn zum Zeitpunkt auf den sich die Prüfung bezieht (z.B. Signaturzeitpunkt oder Zeitpunkt eines Authentisierungsvorgangs), alle Zertifikate im Zertifikatspfad (d.h. bis inkl. Root-Zertifikat) gültig waren.

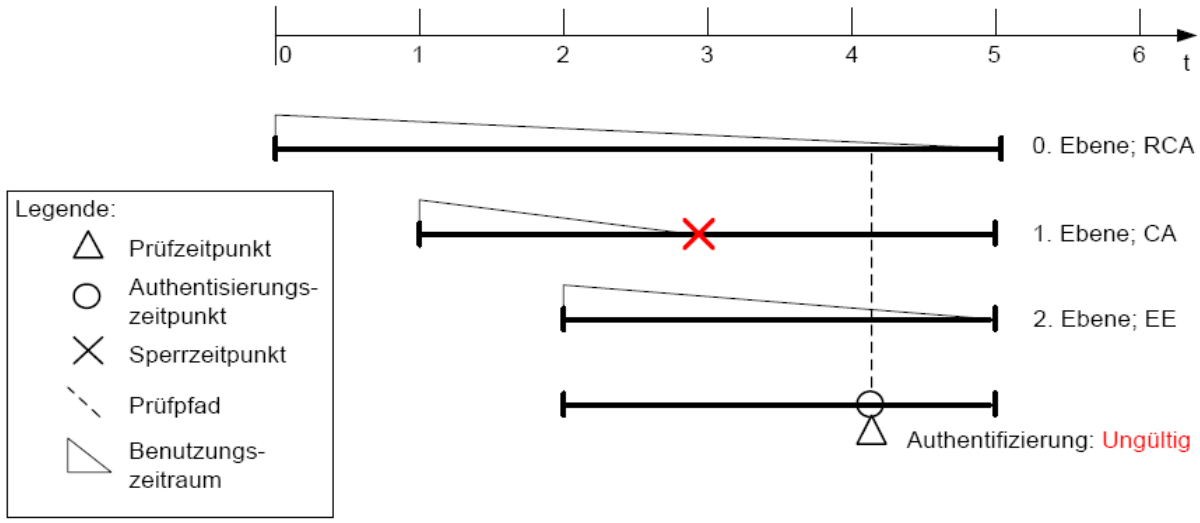

Abbildung 1: Prüfung nach Schalenmodell, CA-Zertifikat gesperrt, Massensperrung

Für den SigG-Bereich, insbesondere für „akkreditierte“ qualifizierte Signaturen, ist das Kettenmodell zwingend, wenngleich es für den nicht-SigG-Bereich der Verschlüsselung und Authentisierung keine Rolle spielt. Beide Modelle haben Vor- und Nachteile.

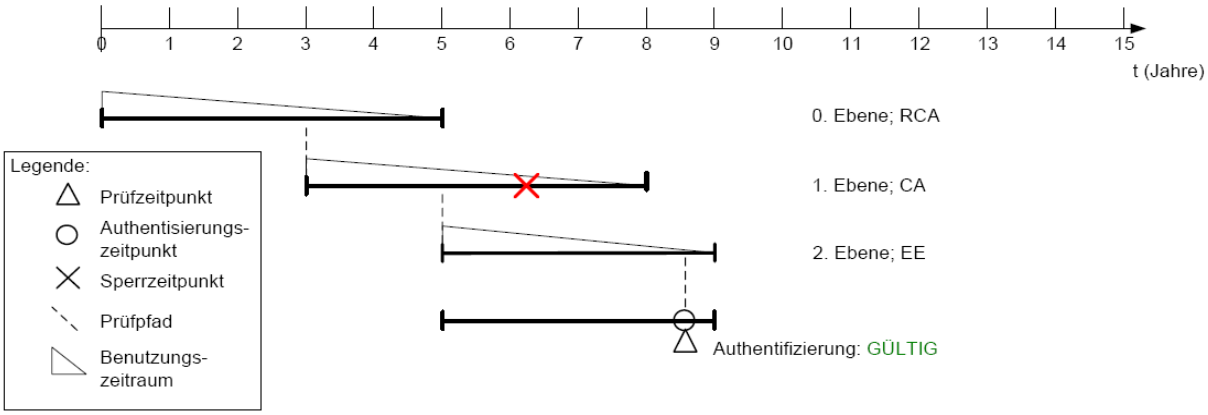

Abbildung 2: Prüfung nach reinem Kettenmodell, Zertifikat ist länger gültig als sein Aussteller

Die Verfügbarkeit der PKI ist im Rahmen der Telematik-Infrastruktur eine kritische Forderung. Das Eintreten von Massensperrungs-Ereignissen (Sperrung eines nicht-SigG Root- oder CA-Zertifikats im Schalenmodell) hätte zur Folge, dass alle von diesem Zertifizierungspfad betroffenen Ärzte über einen längeren Zeitraum keinen Zugang zur Telematik-Infrastruktur hätten, da Ihre Arztausweise implizit mit gesperrt sind. Die Mechanismen des Kettenmodells würden solche Massensperrungen verhindern, würden jedoch höhere Kosten für die Prüfkomponenten und Inkompatibilität verursachen. Um Standardkonformität weitestgehend zu erreichen und die Kosten niedrig zu halten, wird folgender Kompromiss als Hybridmodell vorgeschlagen, damit in der Telematik-Infrastruktur weitestgehend Standardkomponenten eingesetzt werden können. Das Hybridmodell kombiniert Vorteile von Schalen- und Kettenmodell und ist einfach umzusetzen:

Die Authentisierungs- und Verschlüsselungszertifikate unterliegen formal dem Kettenmodell als Gültigkeitsmodell. Sie werden jedoch so ausgestellt, dass sie nicht länger gültig als ihre Aussteller-Zertifikate sind. Dies entspricht praktisch den Vorgaben des Schalenmodells, so dass Standard-Komponenten für die Prüfung der Signaturen/Authentisierungen eingesetzt werden können. Nach Sperrung eines übergeordneten Root- oder CA-Zertifikates bleiben jedoch die End-User-Zertifikate für Verschlüsselung und Authentisierung weiterhin als gültig akzeptiert, da eine Gültigkeitsprüfung nur in der untersten Ebene des Zertifizierungspfades durchgeführt wird. Somit ist der Betrieb der Telematik-Infrastruktur weiterhin gewährleistet ist. Dies entspricht den Vorgaben des Kettenmodells. Ein Austausch der betroffenen Arztausweise ist somit nicht erforderlich (Schutz vor Massensperrungen).

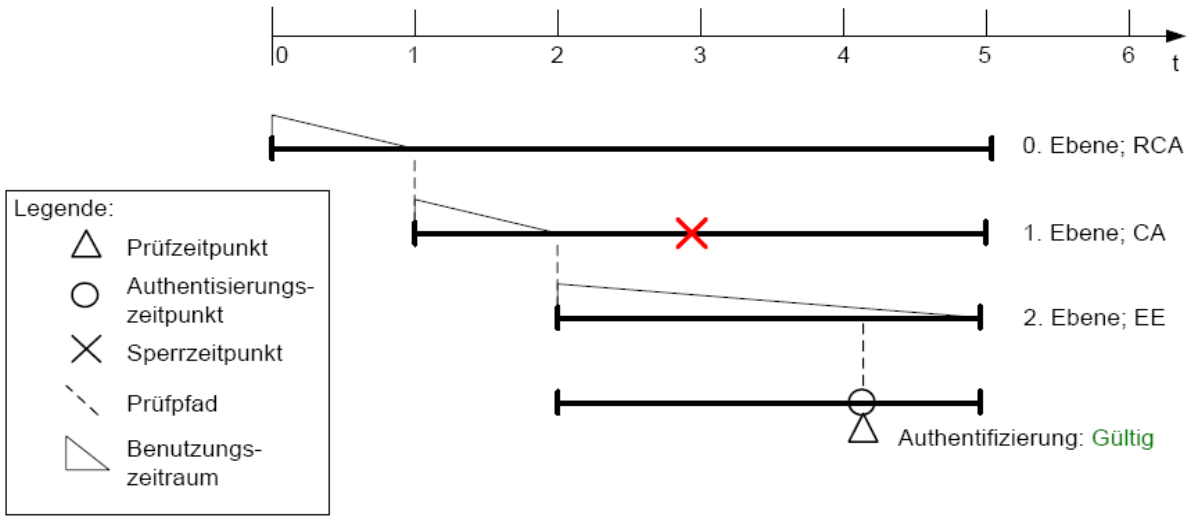

Abbildung 3: Prüfung nach Kompromissmodell, Zertifikate nicht länger gültig als ihr Aussteller, CA-Zertifikat gesperrt

Technisch kann das Kompromissmodell umgesetzt werden, indem die etablierten Prüfkomponenten, die nach Schalenmodell prüfen, (z.B. VPN-Konzentratoren, Access-Gateways) nur den Status (über CRL/OCSP) der Enduser-Zertifikate prüfen und ein Zertifikat zurückweisen, wenn es explizit gesperrt bzw. „nicht vorhanden“ (OCSP) ist. Der aktuelle Status der übergeordneten CA- und Root-Zertifikate darf nicht geprüft werden, d.h. auch wenn sie gesperrt werden, sollen abgeleitete Zertifikate weiterhin als gültig betrachtet werden. Eine gewollte bzw. zwingend notwendige Massensperrung (z.B. bei

kryptographischer Kompromittierung und Bekanntwerden eines privaten CA- oder Root-Schlüssels) wird durch die Sperrung jedes einzelnen abgeleiteten Zertifikates explizit durchgeführt.

Da CRLs/OCSP-Auskünfte für Root- und CA-Zertifikate nicht in die Gültigkeitsprüfung einbezogen werden sollen, wäre es ein offensichtlicher Angriff, wenn eine CA auch nach Sperrung des CA-Zertifikates weiterhin Enduser-Zertifikate produziert. In diesem Falle wäre (abgesehen von organisatorischen und vertraglichen Reaktionen) der Betreiber der CA als böswillig zu betrachten. Insbesondere sind dann auch die Verzeichnisdienstauskünfte (CRL/OCSP) für die Enduser-Zertifikate nicht mehr vertrauenswürdig.

Dieser Angriff kann durch die Einordnung der PKI der eArztausweise in die Infrastruktur einer Bridge-CA nach ETSI TS 102 231 (z.B. der Bridge-CA der gematik) abgewehrt werden. Die Trusted Service Lists der Bridge-CA beinhalten insbesondere auch Informationen zu den vertrauenswürdigen Verzeichnisdienstkomponenten. Da der Verzeichnisdienst der o.g. böswilligen CA als nicht-vertrauenswürdig eingestuft werden muss, wird der Betrieb des Verzeichnisdienstes an einen anderen, vertrauenswürdigen Betreiber vergeben. Damit dies möglich wird, werden organisatorisch-technische Maßnahmen im Vorfeld getroffen (Archivierung von Zertifikaten und Sperrlisten). Mit der Ausstellung einer neuen TSL wird der neue Verzeichnisdienst als autoritativ für die Zertifikate des böswilligen Betreibers definiert. Die unbefugt ausgestellten Zertifikate werden vom vertrauenswürdigen OCSP-Responder als „unbekannt“ deklariert.

Das Gültigkeitsmodell wird in den Authentifizierungs- und Verschlüsselungszertifikaten als Teil der certificate policy und ggf. als Text in der Extension „additionalInformation“ aufgenommen und erlangt somit rechtliche Gültigkeit. Eine Aufnahme in der Extension „validityModel“ der ENC/AUTH-Zertifikate ist nicht vorgesehen.

Ein Problem stellt die sich ergebende Laufzeit der Zertifikate und folglich der eArztausweise dar:

Der amtliche Algorithmenkatalog hat eine Gültigkeit von 6 Jahren. Das Signaturgesetz sieht eine maximale Gültigkeit von 5 Jahren für alle (auch Root- und CA-) Zertifikate vor. Im reinen Kettenmodell kann die maximale fünfjährige Gültigkeit für die User-Zertifikate ausgeschöpft werden, da sie auch länger gültig als ihr Aussteller sein dürfen. Eine Gestaltung der Gültigkeitszeiträume nach dem o.g. vorgeschlagenen Kompromissmodell bei maximaler Gültigkeit von 5 Jahren auch für Root- und CA-Zertifikaten hätte zur Folge, dass die User-Zertifikate maximal 3 Jahre gültig sein können, nach folgendem Muster:

Gültigkeit ROOT: 5 Jahre, wird höchstens 1 Jahr lang zur Ausstellung von CA-Zertifikaten verwendet

Gültigkeit CA: 4 Jahre, wird höchstens 1 Jahr lang zur Ausstellung von User-Zertifikaten verwendet

Gültigkeit USER-Zertifikate: 3 Jahre

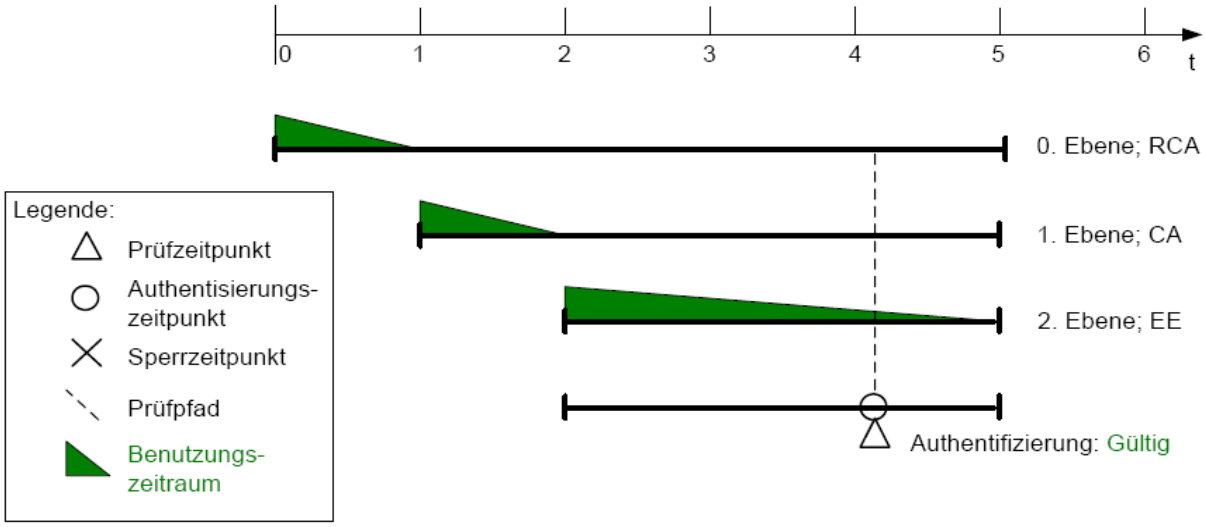

Abbildung 4: Laufzeit nach Schale/Kompromiss bei strikter Einhaltung der 5-jährigen Gültigkeitsdauer

Die Akzeptanz unter den Nutzern steigt, je länger ein eArztausweis gültig ist. Demnach soll eine maximale Gültigkeit von 5 Jahren für die Enduser-Zertifikate angestrebt werden. Nach dem Kompromissmodell würde dies zu einer längeren Gültigkeitsdauer für nicht-qualifizierte Root- und CA-Zertifikate führen.

Die Sicherheit von Zertifikaten in einer PKI ist etwas reales und messbares. Sie wird von getroffenen organisatorischen und technischen Sicherheitsmaßnahmen definiert, z.B. ob die CA in geschützten Räumlichkeiten läuft, ob die privaten CA-Schlüssel ausreichend geschützt werden und ob die Regelungen eines vernünftigen Sicherheitskonzeptes eingehalten werden. AUTH- und ENC-Userzertifikate für eArztausweise sollen nach den gleichen organisatorischen und technischen Sicherheitsanforderungen wie qSIG-Userzertifikate produziert und verwaltet werden. Die Behauptung, dass nur im Kettenmodell ausgestellte Zertifikate sicher sein können, ist sicherlich nicht haltbar. Qualifizierte Signaturzertifikate mit einer fünfjährigen Gültigkeit werden vom SigG/SigV als sicher angesehen. Es muss also möglich sein, gleich sichere, fünf Jahre lang gültige Userzertifikate für Authentifizierung und Verschlüsselung auszustellen, auch wenn Root- und CA-Zertifikate dafür länger gültig sein müssen. Im Folgenden wird beschrieben, wie im Kompromiss- oder Schalenmodell eine Gültigkeit von 5 Jahren für ENC-/AUTH-Userzertifikate, die gleichwertige Sicherheit wie qualifizierte Signaturzertifikate haben, erreicht werden kann.

SigG-konforme Enduser-Signaturzertifikate dürfen 5 Jahre lang gültig sein. Ein 5 Jahre lang gültiges qualifiziertes CA-Zertifikat im Kettenmodell darf am letzten Tag seiner Gültigkeit ein 5 Jahre lang gültiges Enduser-Zertifikat ausstellen. Ebenso darf im Kettenmodell am letzten Tag der Gültigkeitsdauer eines qualifizierten Root-Zertifikates ein qualifiziertes CA-Zertifikat ausgestellt werden.

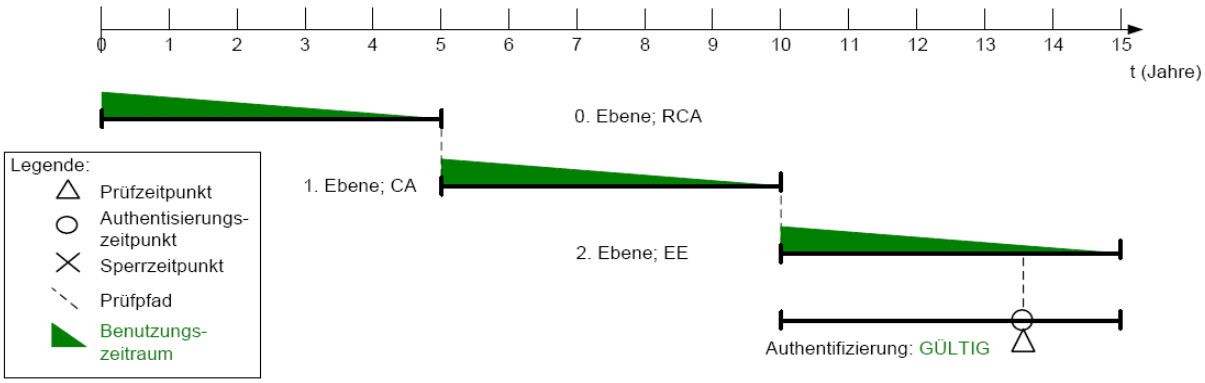

Abbildung 5: Laufzeiten der Zertifikate und Verwendung des privaten Schlüssels nach Kettenmodell

Unter der Voraussetzung, dass die zugrunde liegende Schlüssellänge und Algorithmus für das Root-, CA- und Userzertifikat nach 15 Jahren weiterhin gültig ist, kann ein nach dem Kettenmodell ausgestelltes gültiges Zertifikat zum Ende seiner Gültigkeit auf ein 15 Jahre altes Root-Zertifikat abgeleitet und validiert werden. Wenn das Root-Zertifikat nach den Vorgaben des Schalenmodells ausgestellt worden wäre, müsste es eine Gültigkeitsdauer von 15 Jahren haben, wobei der private Schlüssel (zur Ausstellung von CA-Zertifikaten) 5 Jahre lang verwendet werden darf. Das CA-Zertifikat müsste 10 Jahre lang gültig sein (Benutzung des privaten Schlüssels zur Ausstellung von User-Zertifikaten: 5 Jahre). Also (bei weiterhin gültigen Algorithmen und Schlüssellängen) entspricht ein nach Schale ausgestelltes Root-Zertifikat mit einer Gültigkeit von 15 Jahren (privateKey: 5 Jahre) einem den SigG-Anforderungen nach Kette ausgestellten 5 Jahre gültigen Root-Zertifikat. Analog entspricht ein 10 Jahre gültiges Schalen-CA-Zertifikat (Benutzung privateKey: 5 Jahre) einem SigG-konformen 5 Jahre gültigen CA-Zertifikat. Folglich werden die im SigG definierten Sicherheitsanforderungen von den o.g. Root- (15 Jahre) und CA- (10 Jahre) faktisch eingehalten: die Zertifikate können als genau so sicher betrachtet werden. (Voraussetzungen: Benutzung privater Schlüssel immer 5 Jahre, Algorithmen & Schlüssellängen gleich bleibend gültig. Gleiche organisatorische und technische Sicherheit für den gesamten Lifecycle). Die Gültigkeitsdauer im Kettenmodell entspricht der „private key usage period“ im Schalenmodell.

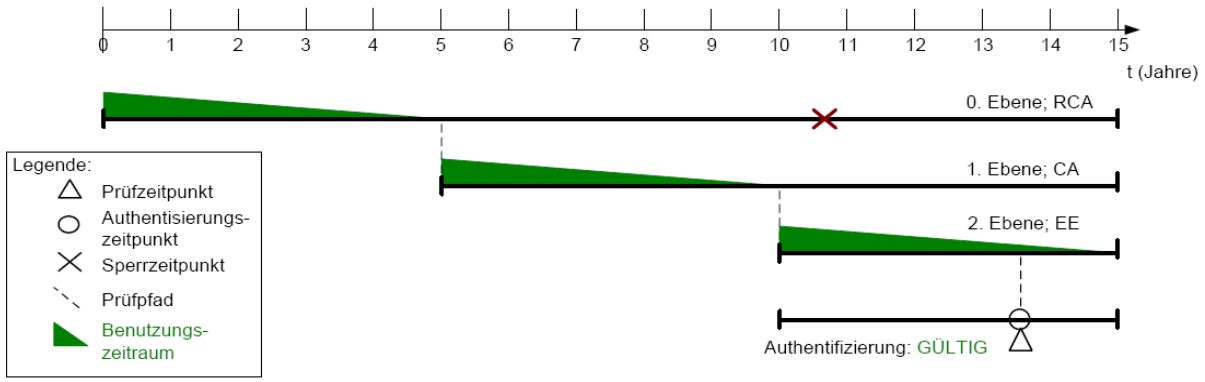

Abbildung 6: Zertifikate im Kompromissmodell, entsprechen Sicherheitsanforderungen SigG-konformer Zertifikate bei unverändert gültigen Algorithmen und Schlüssellängen

Es ist jedoch unwahrscheinlich, dass Algorithmen und Schlüssellängen über einen Zeitraum von 15 Jahren unverändert gültig bleiben. Um diese Problematik aus den SigG-Anforderungen im Kompromissmodell abzubilden, kann folgendes Verfahren angewandt werden:

Der amtliche Algorithmenkatalog definiert gültige Algorithmen und Schlüssellängen für die jeweils nächsten 6 Jahren. Beträgt die zulässige Gültigkeit eines Algorithmus oder einer Schlüssellänge weniger als 5 Jahre, dürfen von einem Root- oder CA-Zertifikat, das diesen Algorithmus oder Schlüssellänge verwendet, keine 5 Jahre lang gültige untergeordnete Zertifikate (CA- oder Enduser)

mehr ausgestellt werden (kürzere Laufzeiten sind wie im SigG-Kontext natürlich erlaubt). D.h. die maximale Gültigkeitsdauer eines neu ausgestellten Zertifikats darf nicht länger sein als die Gültigkeit des Algorithmus / der Schlüssellänge im amtlichen Algorithmenkatalog. Zertifikate (Root-, CA- oder auch Enduser-Zertifikate), dessen Algorithmen und Schlüssellängen abläuft, werden beim Erreichen dieses Zeitpunktes (Ablauf Algorithmus/Schlüssellänge) gesperrt.

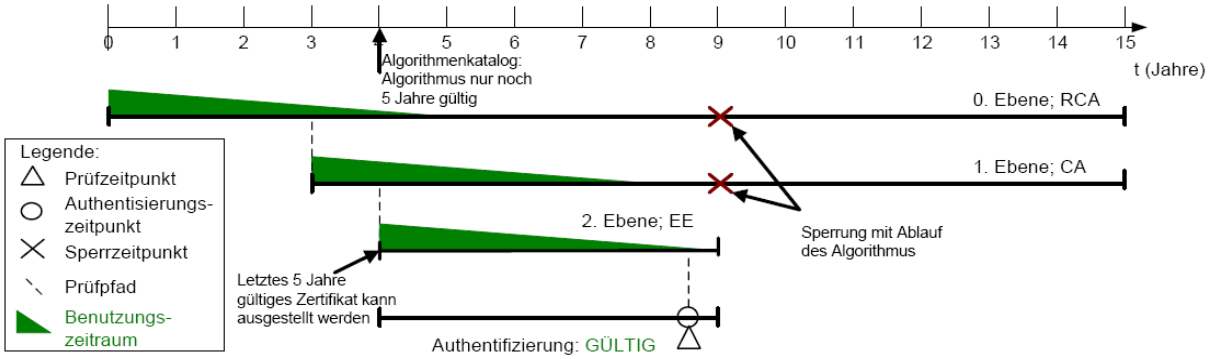

Abbildung 7: Kompromissmodell, Ausstellung nach Schale, Vorgehen bei Ablauf der Algorithmen / Schlüssellängen

Im Sinne einer „Best-Practice"-Lösung soll ein privater nicht-qualifizierter Root-Schlüssel 2 Jahre lang für die Ausstellung von CA- und Cross-Zertifikaten verwendet werden. Ein privater nicht-qualifizierter CA-Schlüssel soll 3 Jahre lang für die Ausstellung von User-Zertifikaten für Verschlüsselung und Authentisierung verwendet werden. Enduser-Zertifikate sollen genauso lang gültig wie die qualifizierten Signaturzertifikate auf dem eArztausweis, d.h. maximal 5 Jahre lang gültig sein. Damit ergibt sich eine maximale Gültigkeit von 10 Jahren für das Root- und von 8 Jahren für das CA-Zertifikat. Diese Zeiträume stellen, bei Vorhandensein geeigneter Trägermedien für die Root- und CA-Schlüssel, eine praktikable und im Sinne des Algorithmenkatalogs belastbare Lösung für die Root-, CA- und Bridge-CA-Instanzen sowie die PKI-Clients, die somit nicht jährlich neue Root- und CA-Zertifikate importieren müssen.

Fazit:

Mit dem Kompromissmodell werden die Vorteile des Ketten- und Schalenmodells kombiniert. Es können etablierte IT-Komponenten für Authentifizierung und Verschlüsselung eingesetzt werden, die Zertifikate nach Schalenmodell prüfen (s. o.), was zu einer Kostenreduktion der Infrastruktur führt. Massensperrungen sind ausgeschlossen (Ausnahme: echte kryptographische Kompromittierung, d.h. Bekanntwerden eines privaten Root- oder CA-Schlüssels). Es können maximal 5 Jahre lang gültige Heilberufsausweise ausgestellt werden unter Einhaltung der faktischen Sicherheitsanforderungen, die das Signaturgesetz definiert. Sie werden trotz längerer Gültigkeitsdauer der nicht-qualifizierten Root- und CA-Zertifikate eingehalten, weil sie das Ergebnis der organisatorischen und technischen Sicherheitsmaßnahmen deren Produktion und Verwaltung sind, die den Sicherheitsanforderungen des SigG entsprechen. Die Vorgaben des amtlichen Algorithmenkatalogs werden berücksichtigt.

Durch die Wahl des Gültigkeitsmodells und durch die Definition einer einheitlichen Gültigkeitsdauer werden gleiche Bedingungen für alle Zertifikate eines eArztausweises geschaffen. Die Gültigkeit des kompletten eArztausweises kann somit einheitlich betrachtet und verwaltet werden.