Erschienen in R. Koschke, O. Herzog, K.-H. Rödiger, M. Ronthaler (Hrsg.):
INFORMATIK 2007 – Informatik trifft Logistik, Band 2,
GI e. V. LNI P-110, S. 179–183, ISBN 978-3-88579-204-8, 2007.

Anmerkungen zur Gültigkeit von Zertifikaten

Bodo Möller

Horst-Görtz-Institut für IT-Sicherheit
Ruhr-Universität Bochum
bmoeller@acm.org

Abstract: Gültigkeitsmodelle für Zertifikate und andere Signaturen wie das sogenannte „Kettenmodell“ verwischen den Begriff der Gültigkeit von Schlüsseln: Schlüssel können auch außerhalb ihres Gültigkeitsintervalls gültige Signaturen erzeugen und sind so faktisch selbst noch gültig. Der irreführenden Terminologie setzen wir eine Faustregel entgegen.

1 Einleitung

Digitale Signaturen erscheinen, wenn man von den kryptographischen und technischen Details abstrahiert, im Grunde recht einfach: Der Inhaber eines privaten *Signaturschlüssels* kann mit diesem Schlüssel zu jeder beliebigen Nachricht eine Signatur berechnen (*Signieren*). Zum privaten Signaturschlüssel gehört ein öffentlicher *Signaturprüfschlüssel,* und zu einer gegebenen Nachricht und Signatur kann mit diesem Schlüssel jeder überprüfen, ob die Signatur „gültig“ ist (*Signaturprüfung*), also mutmaßlich mit besagtem privaten Signaturschlüssel angefertigt wurde. Unter geeigneten Sicherheitsvoraussetzungen (nämlich für geeignete Verfahren und bei Geheimhaltung des privaten Signaturschlüssels) kann man sicher sein, daß eine Nachricht mit „gültiger“ Signatur tatsächlich vom Inhaber des Signaturschlüssels signiert wurde. Ein Sonderfall einer signierten Nachricht ist ein *Zertifikat:* Hier unterschreibt der Signierende eine bestimmte Zuordnung eines öffentlichen Schlüssels (z. B. eines weiteren Signaturprüfschlüssels) zu dessen Inhaber. Offensichtlich sollte man eine solche Zertifizierung nicht jedem beliebigen Signierenden ohne weiteres glauben. Mit Zertifikaten aber, die von vertrauenswürdigen Stellen oder Personen ausgestellt wurden, ergibt sich die Grundform einer *Public-Key-Infrastruktur.* Damit kann man Signaturen auch prüfen, ohne den Signaturprüfschlüssel des Signierenden von vornherein zu kennen: Von mindestens einem *Vertrauensanker* aus hangelt man sich von Zertifikat zu Zertifikat bis hin zum passenden Schlüssel.

Die Praxis ist, wie so oft, viel komplexer. Beträchtliche Komplikationen ergeben sich bereits, wenn man die Dimension der *Zeit* in die Betrachtungen einbezieht: Wenn ein Signaturschlüssel heute jemandem gehört, stimmt diese Zuordnung dann auch noch morgen, kann man auf Signaturen zu diesem Schlüssel weiterhin vertrauen? Für die Ewigkeit gelten lassen jedenfalls will man Signaturen und gerade Zertifikate meist nicht – das kryptographische Verfahren könnte früher oder später gebrochen werden, der private Signaturschlüssel könnte in falsche Hände geraten (vielleicht durch bloße Nachlässigkeit; viel-

leicht, indem technische Hindernisse überwunden werden, etwa Sicherheitsmaßnahmen einer Chipkarte), und möglicherweise sind bei einem Zertifikat lediglich Detailangaben zum Inhaber überholt (z. B. die Firmenzugehörigkeit). Also stattet man Zertifikate und damit öffentliche Schlüssel gerne mit einer zeitlich begrenzten Gültigkeit aus. Im Zertifikat kann ein Gültigkeitszeitraum vermerkt werden; und für alle Fälle kann man sich die Möglichkeit eines nachträglichen *Widerrufs* (durch geeignete Mechanismen) vorbehalten.

Aber was bedeutet es eigentlich, wenn ein Signaturschlüssel nicht mehr gültig ist, wenn er also abgelaufen oder widerrufen ist? Was ist ein „ungültiges“ Zertifikat, ein „ungültiger“ Schlüssel, eine „ungültige“ Signatur? Diese Fragestellung ist das Thema dieses Artikels.

2 Schalenmodell und Kettenmodell

Gehen wir aus von einer Zertifizierungsstruktur mit zum Beispiel drei Ebenen: Als Vertrauensanker ist ein *„Wurzelzertifikat“* C_0 gegeben, das Angaben zu einer speziellen *Zertifizierungsstelle* enthält (inbesondere deren Signaturprüfschlüssel). Beim Wurzelzertifikat handelt es sich jedoch nicht um ein Zertifikat im engeren Sinne, denn eine Zertifizierung durch einen Dritten liegt in diesem Sonderfall nicht vor. Für eine weitere Zertifizierungsstelle ist ein Zertifikat C_1 ausgestellt, signiert von der ersten Stelle als *Aussteller* dieses Zertifikates. Die zweite Zertifizierungsstelle wiederum ist Aussteller eines Zertifikats C_2 für einen Endnutzer. Das Zertifikat C_2 enthält also dessen öffentlichen Schlüssel und ist so signiert, daß die Signaturprüfung mit dem öffentlichen Schlüssel aus C_1 geschehen kann. Der in C_2 genannte Endnutzer sei Unterzeichner eines Dokuments m. Um die Signatur auf m zu prüfen, benötigt man also unmittelbar das Zertifikat C_2 und mittelbar auch die Zertifikate C_1 und C_0, um so beim Vertrauensanker anzukommen.

Stark vereinfacht enthält ein Zertifikat nach [X.509] folgende Angaben:

$$C_i = (\mathsf{subject}_i, \mathsf{issuer}_i, K_i, t_i^{\mathsf{notBefore}}, t_i^{\mathsf{notAfter}}, \Sigma_i)$$

Hier bezeichnen $\mathsf{subject}_i$ und issuer_i Namen des Zertifikatsinhabers bzw. des Zertifikatsausstellers. K_i ist der durch dieses Zertifikat zertifizierte öffentliche Schlüssel. Die Angaben $t_i^{\mathsf{notBefore}}$ und t_i^{notAfter} bestimmen als zwei Zeitpunkte das zeitliche Gültigkeitsintervall, wobei $t_i^{\mathsf{notBefore}}$ in der Regel der Zeitpunkt der Zertifizierung ist. Σ_i schließlich ist die Signatur des Zertifikatsausstellers auf alle Angaben in C_i außer Σ_i selbst. Mit dieser Signatur bestätigt er, daß diese Angaben als Teile eines Zertifikats zusammengehören.

In einer Zertifikatskette wie oben gilt stets $\mathsf{issuer}_{i+1} = \mathsf{subject}_i$, und entsprechend kann die Signatur Σ_{i+1} mit dem Schlüssel K_i geprüft werden. Speziell für das Wurzelzertifikat ist $\mathsf{issuer}_0 = \mathsf{subject}_0$ (das Zertifikat ist also von seinem Inhaber selbst signiert, Σ_0 ist eine mit dem Schlüssel K_0 zu prüfende Signatur – vor allem aus Gründen der Einheitlichkeit verwendet man die Form eines Zertifikats auch hier für C_0). Zur signierten Nachricht m gehört optional eine Zeitangabe t_3 und dann eine Signatur Σ_3 auf (m, t_3), die mit dem Schlüssel K_2 geprüft werden kann. Hier liefert t_3 eine Datierung des Signiervorgangs.

Wie sieht nun eine vom Vertrauensanker ausgehende Prüfung der Signatur des Endnutzers auf m aus unter Berücksichtigung all dieser Zeitpunkte? Klar ist: Wenn mit den Signaturen

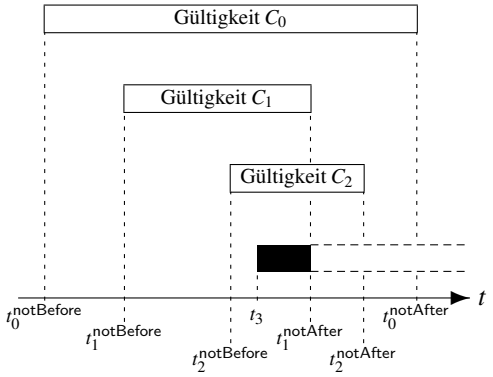

Abbildung 1: Überprüfbarkeit einer Signatur auf Basis des Schalenmodells (schwarzes Rechteck) und des Kettenmodells (gestrichelte Erweiterung)

und den Zertifikaten insgesamt ansonsten in jeder Hinsicht alles in Ordnung ist, kann man die Signaturprüfung jedenfalls dann akzeptieren, wenn jedes der Zertifikate derzeit gültig ist, wenn also für die aktuelle Zeit t gilt

$$t \in [t_0^{\text{notBefore}}, t_0^{\text{notAfter}}], \qquad t \in [t_1^{\text{notBefore}}, t_1^{\text{notAfter}}], \qquad t \in [t_2^{\text{notBefore}}, t_2^{\text{notAfter}}],$$

und wenn auch die eventuell angegebene Signierzeit t_3 plausibel ist:

$$t_3 \in [t_2^{\text{notBefore}}, t_2^{\text{notAfter}}], \qquad t_3 \leq t$$

Der Ansatz, eine Zertifikatskette *nur* dann zu akzeptieren, wenn alle Gültigkeitsintervalle $[t_i^{\text{notBefore}}, t_i^{\text{notAfter}}]$ auf diese Weise um den aktuellen Zeitpunkt herum angeordnet sind (vgl. [RFC 3280]), wird bildlich auch als *Schalenmodell* bezeichnet in Abgrenzung vom sogenannten *Kettenmodell* als einem Gültigkeitsmodell, in dem auch abgelaufene Zertifikate toleriert werden können. Das zeigt Abb. 1 für eine Beispielkonstellation: Das schwarze Rechteck gibt an, zu welchen Zeitpunkten t eine Signaturüberprüfung gemäß Schalenmodell möglich ist. Wie die Erweiterung des Rechtecks nach rechts andeutet, ist die Überprüfbarkeit der Signatur im Kettenmodell zeitlich nicht begrenzt.

Das Kettenmodell ist im Zusammenhang mit dem deutschen Signaturgesetz [SigG] aufgekommen, um der langfristigen Überprüfbarkeit von Signaturen weniger Steine in den Weg zu legen [BNetzA]. Nicht die aktuelle Zeit, sondern der Signierzeitpunkt t_3 wird mit dem Gültigkeitsintervall des Zertifikats C_2 abgeglichen: Das Zertifikat darf zum späteren Zeitpunkt der Prüfung also abgelaufen sein. Zwischen C_1 und C_2 wird eine Überschneidung der Gültigkeitsintervalle verlangt, aber C_1 darf zum Zeitpunkt t_3 abgelaufen sein. Entsprechend müssen sich auch die Gültigkeitsintervalle von C_0 und C_1 überschneiden, während C_0 längst abgelaufen sein darf (auch schon beim Gültigkeitsbeginn von C_2). So ergibt sich eine Kette von C_0 über C_1 und C_2 bis hin zum Signierzeitpunkt t_3.

Im Kettenmodell bleiben also nominell ungültige, da abgelaufene, Zertifikate höchst relevant bei der Prüfung von Signaturen! Der Mechanismus des Gültigkeitsintervalls (und ähnlich auch der Mechanismus des Zertifikatswiderrufs [BNetzA]) wird hier anders gebraucht

als eigentlich bei X.509 beabsichtigt (vgl. [X.509, 8.2.1 d und 8.2.2.5]): Nicht die Benutzung des öffentlichen Signaturprüfschlüssels soll mit Ablauf (oder Widerruf) eingestellt werden, sondern primär nur die Benutzung des zugehörigen privaten Signaturschlüssels.

3 Ein Kriterium für Ungültigkeit

Was bewirkt der Ablauf oder Widerruf irgendeines Zertifikats zu einem Signaturprüfschlüssel überhaupt? Eigentlich (so der Grundgedanke auch beim Kettenmodell) können fortan keine gültigen Signaturen mit dem nominell ungültig gewordenen Schlüssel erzeugt werden. Wer jedoch über den privaten Signaturschlüssel verfügt (oder das Signaturverfahren gebrochen hat), ist hieran gar nicht gebunden: Neu gefälschte Signaturen (und ggf. Zertifikate) können *zurückdatiert* werden und sind dann aus Sicht des Kettenmodells weiterhin gültig. So läßt sich in diesem Gültigkeitsmodell eine beliebig große Zeitdauer überbrücken, solange der zugrundeliegende Vertrauensanker von den Zertifikats- und Signaturprüfern noch berücksichtigt wird. Ein Zertifikat mit abgelaufenem Gültigkeitsintervall ist also faktisch nicht völlig ungültig: Der Ablauf ist vor allem *deklarativ,* aber ist nicht zwingend wirksam. Auch ein widerrufenes Zertifikat ist nicht völlig ungültig, denn – das ist der Sinn des Kettenmodells – bei der Sperrung von Zertifikaten ist wegen [SigG, § 8 Abs. 1 S. 4] keine Rückwärtswirkung erwünscht [BNetzA], und so kann ein widerrufenes Zertifikat im Rahmen des Kettenmodells berücksichtigt werden für die Verifikation einer früheren oder scheinbar früheren Signatur. ([X.509] geht ohnehin davon aus, daß ein Zertifikatswiderruf nach Ablauf des Gültigkeitsintervalls nicht mehr nötig sein könnte.)

Das Kettenmodell höhlt also die Wirkung von Gültigkeitsintervallen und Zertifikatswiderrufen stark aus. Diese Beobachtung sorgt immer wieder für Erstaunen, obwohl sie nach einer gewissen Beschäftigung mit der Sache eigentlich auf der Hand liegt: Der Begriff der „Gültigkeit“ wird beim Kettenmodell ad absurdum geführt. Wir schlagen deshalb für die Beurteilung von Gültigkeitsmodellen das folgende Kriterium als Faustregel vor, um der Irreführung durch die Terminologie entgegenzuwirken:

> *Ein Schlüssel für Signaturen kann erst dann als wirklich ungültig angesehen werden, wenn die Veröffentlichung des privaten Signaturschlüssels keinen Schaden mehr anrichten könnte.*

Diese Regel lenkt die Gedanken in die richtige Richtung: Im Schalenmodell kann ein Schlüssel die Gültigkeit verlieren, wenn sein Zertifikat abläuft – ob dann der private Signaturschlüssel bekannt wird, ist unerheblich, denn Signaturen von diesem Schlüssel werden sowieso überhaupt nicht mehr akzeptiert. Ganz anders im Kettenmodell.

Ist eine faktisch lange Schlüsselgültigkeit wie im Kettenmodell tatsächlich beabsichtigt, so kann sie auch erreicht werden, indem das Gültigkeitsintervall in den Zertifikaten explizit entsprechend angegeben wird. Mit langen Gültigkeitsdauern entfällt der Grund, das Kettenmodell zu bemühen. Sinnvoll bei der Verifikation von digitalen Signaturen ist es dann, anzuzeigen, für welche verbleibende Dauer die Verifikation laut den Gültigkeitsintervallen der vorliegenden Zertifikatskette noch möglich sein wird.

X.509 bietet eine *"private key usage period extension",* die verwendet werden kann, um als Zusatzinformation dasjenige Zeitintervall in Zertifikaten zu vermerken, das bei Benutzung des Kettenmodells irreführend als „Gültigkeitsintervall" angegeben würde.

Die Begründung [BT 13/7385] zur ursprünglichen Fassung des Signaturgesetztes [SigG 97] weist bereits auf eine Lösung, mit der sich die Probleme der Gültigkeitsverlängerung vermeiden lassen: Bei konsequenter Benutzung von Zeitstempeldiensten (die aber mit dem neuen Signaturgesetz vom 16. Mai 2001 nun optional sind) kann man im Nachhinein noch demonstrieren, daß Zertifikate und andere Signaturen zusammen mit signierten Dokumenten schon zu einem bestimmten Stichtermin vorlagen. So läßt sich im Nachhinein feststellen, ob zu dem Termin eine gültige Signatur (z. B. laut Schalenmodell) vorlag. Die entsprechenden Schlüssel können inzwischen vollständig ungültig geworden sein in dem Sinne, daß es nicht mehr schadete, würden die entsprechenden privaten Signaturschlüssel kompromittiert: Durch die Zeitstempel – Signaturen vertrauenswürdiger Stellen auf beliebige Daten zusammen mit akkurater Zeitinformation [RFC 3161] – bleibt die langfristige Überprüfbarkeit gewährleistet, und sie bleibt beschränkt auf diejenigen Signaturen, die tatsächlich bereits während der Gültigkeit der relevanten Zertifikate vorlagen.

4 Fazit

Die Änderung der Semantik von Gültigkeitsintervallen und Zertifikatswiderrufen durch das Kettenmodell ist sehr unglücklich. Eine deutlich verlängerte Gültigkeitsdauer von Zertifikaten wäre eine weniger irreführende Methode, in etwa das gleiche zu erreichen (gegebenenfalls zusammen mit der X.509-Zertifikatserweiterung "private key usage period"). Erst mit einem Zeitstempeldienst ergibt sich eine langfristige Überprüfbarkeit von Signaturen ohne gewaltige Gültigkeitsverlängerung der Schlüssel.

Literatur

[BNetzA] Bundesnetzagentur, Elektronische Signatur – FAQ, http://www.bnetza.de/

[BT 13/7385] Amtliche Begründung zum Informations- und Kommunikationsdienste-Gesetz (IuKDG), Bundestagsdrucksache 13/7385 vom 9. 4. 1997

[RFC 3161] C. Adams et al., Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), RFC 3161

[RFC 3280] R. Housley et al., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280

[SigG 97] Gesetz zur digitalen Signatur (Signaturgesetz – SigG), BGBl. I 1997 S. 1872

[SigG] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG), BGBl. I 2001 S. 876

[X.509] Public-key and attribute certification frameworks, ITU-T Recommendation X.509 (08/2005), ISO/IEC 9594:2005