Ernst-Günter Giessmann

X.509 und der Gültigkeitszeitraum

Die Menschheit zerfällt in 10 Teile:
der erste drückt sich falsch aus,
und der zweite missversteht es.
Alexander Roda Roda

Gültige Zertifikate

Nach §2 des Signaturgesetzes muss eine qualifizierte Signatur auf einem zum Zeitpunkt ihrer Erstellung *gültigen* qualifizierten Zertifikat beruhen.

Ein zu diesem Zeitpunkt gesperrtes Zertifikat ist sicher *ungültig*, aber ab wann und wie lange ist es eigentlich gültig?

Jedes zum Standard X.509/RFC 5280 konforme Zertifikat enthält immer zwei Datumsangaben, die als ASN.1-Variable `notBefore` und `notAfter` heißen und in einer `validity` genannten Folge zusammengefasst werden. In der deutschsprachigen Literatur wird diese Zeitspanne regelmäßig als *Gültigkeitszeitraum* übersetzt, obwohl sie formal nicht Beginn und Ende eines Zeitraums angibt, sondern nur einschränkt.

Ein Blick in den X.509, wie denn diese Zeitspanne, die Variable `validity`, tatsächlich definiert ist, lohnt sich:

- **„`validity` is the time interval during which the CA warrants that it will maintain information about the status of the certificate".**

Oder in freier Übersetzung:

- **„`validity` ist das Zeitintervall für das sich die CA verpflichtet, aktuelle Statusinformationen zum Zertifikat bereitzuhalten".**

Ein technischer *Gültigkeitszeitraum* wird dadurch sicher nicht beschrieben, sondern eher vielleicht eine *Garantiedauer* oder ein *Gewährleistungszeitraum*. Wir wollen ihn deshalb in diesem Beitrag auch so nennen.

Ein Zertifizierungsdiensteanbieter (ZDA/ CA) legt folglich bei der Erstellung eines Zertifikats fest, ab wann er *spätestens* die Informationen zum Status des Zertifikats bereitstellen wird und wie lange er das *mindestens* zu tun beabsichtigt. Diese Informationen sind für eine Nutzerin auch wichtig, denn nur in diesem Zeitraum kann sie erwarten, dass ihr die Information, ob das Zertifikat überhaupt ausgestellt wurde und ob es, und falls wann, gesperrt wurde, bereitgestellt werden. Ohne diese Informationen kann sie dem Zertifikat eigentlich nicht vertrauen und prüfen, ob eine Signatur gültig ist.

Vor notBefore

Ab dem Zeitpunkt `notBefore` ist ein Zertifikat gültig, falls es nicht schon gesperrt ist. Ob es davor schon gültig war, kann man selten direkt nachprüfen, da es dazu keine gesicherten Informationen geben muss. Es geht manchmal nur über einen Umweg, wie bei den Zertifikaten `0x313`, `0x314` und `0x315` der Bundesnetzagentur, denen jeweils die folgenden `notBefore`-Daten zugeordnet sind:

Nr	notBefore	Subj	Issu
0x313	2007-05-25 11:01:44	12R	12R
0x314	2007-05-29 07:57:50	11R	12R
0x315	2007-05-29 09:17:45	12R	11R

Signiert wurden jeweils die Schlüssel von und durch `11R-CA` und `12R-CA`. Das Zertifikat `0x313` ist also selbst-, `0x314` ist alt-von-neu- und `0x315` ist neu-von-alt-signiert. Wenn jetzt das letzte Zertifikat nicht schon vor seinem `notBefore` Zeitpunkt gültig gewesen wäre, wären die Signaturen von `0x313` und `0x314` nicht qualifiziert, weil der Schlüssel `12R-CA` bei seiner Verwendung nicht auf einem qualifizierten Zertifikat beruht hätte.

Aus der technischen Sicht des X.509 ist eine Antwort auf die Frage, ab wann ein Zertifikat zum ersten Mal gültig ist, ohne Bedeutung, entscheidend ist die Prüfbarkeit der darauf beruhenden Signaturen, und die ist verlässlich erst innerhalb des Gewährleistungszeitraums gegeben.

Im Gewährleistungszeitraum

Die Prüfung einer Signatur enthält als wesentlichen Bestandteil die Prüfung der Zertifikatskette zum Vertrauensanker, die manchmal auch als Gültigkeitsprüfung des Zertifikats bezeichnet wird. Tatsächlich wird dabei das Vertrauensniveau für das Zertifikat des Signierenden bestimmt. Eine Zertifikatskette ist „gültig", wenn das erforderliche Niveau erreicht wurde. Im Unterschied zu einer Gültigkeitsprüfung einer Signatur ist, wenn über die angegebene Kette das entsprechende Vertrauensniveau nicht erreicht wird, das geprüfte Zertifikat aber nicht gleich *ungültig*, wenn bestimmte Prüfinformationen nicht verfügbar, veraltet oder verblasst sind oder die ganze Kette ungeeignet ist, weil sie nicht in einem Vertrauensanker endet.

Da aber für den gesamten Gewährleistungszeitraum vom ZDA zugesichert wird, dass der Vertrauensstatus des Zertifikats zweifelsfrei feststellbar ist, könnte man ihn noch *Vertrauensstatusbestimmbarkeitszeitraum* nennen oder, da ja die Gültigkeit einer Signatur auf dem Vertrauensstatus des Signaturzertifikats beruht, vielleicht auch *Mindestsignaturgültigkeitsprüfzeitraum*?

Nach notAfter

Nach `notAfter` müssten Statusinformationen nicht mehr durch den ZDA zur Verfügung gestellt werden. Aber das Signaturgesetz fordert die Verfügbarkeit dieser Informationen über den Gewährleistungszeitraum hinaus, also seine Verlängerung, denn abgelaufene oder auch gesperrte Zertifikate sollen weiter zur Gültigkeitsprüfung von Signaturen und zur Bestimmung des Vertrauensstatus herangezogen werden können.

Das Signaturgesetz verwendet den Begriff des *gültigen Zertifikats* außer in §2 nur noch an einer Stelle, aber da ungenau, denn es wird in §13 bei Einstellung der Tätigkeit nur gefordert, dass die *gültigen* Zertifikate von einem anderen ZDA zu übernehmen sind. Tatsächlich müssen aber alle, auch die *gesperrten* Zertifikate übernommen werden, zumindest die, deren Gewährleistungszeitraum noch nicht abgelaufen ist.

Man könnte Missverständnisse zukünftig dadurch vermeiden, indem man grundsätzlich auf den Begriff des *gültigen* Zertifikats verzichtet, wie etwa so:

- **… Signatur, die auf einem qualifizierten Zertifikat beruht, welches zum Zeitpunkt ihrer Erzeugung nicht gesperrt und dessen Gewährleistungszeitraum zugleich auch noch nicht abgelaufen war.**

Obwohl es sich eingebürgert hat, dass man ein Zertifikat nach `notAfter` oder nach der Sperrung als *ungültig* bezeichnet, sollte man nie vergessen, dass aus technischer Sicht ein Zertifikat nur einen *Gewährleistungs-* und keinen *Gültigkeitszeitraum* enthält.