

Ernst-Günter Giessmann

Fortgeschrittene Signaturen und qualifizierte Zertifikate

Stille Betrachtung

Es gibt Zertifikate und elektronische Signaturen.

Es gibt fortgeschrittene Signaturen und qualifizierte Zertifikate.

Es gibt auch qualifizierte Signaturen und sogar fortgeschrittene Signaturen, die auf einem qualifizierten Zertifikat beruhen.

Ein fortgeschrittenes Zertifikat aber gibt es nicht.

nach Alexander Roda Roda

Hintergrund

Eine Internet-Suche nach „fortgeschrittenen Zertifikaten“ liefert ungefähr 200 Treffer. Das ist nicht sehr viel, aber es finden sich darunter einige (auch akkreditierte) Zertifizierungsdiensteanbieter und seriöse IT-Firmen: Der IT-Dienstleister des Landes Brandenburg klassifiziert gleich alle Zertifikate der Verwaltungs-PKI als fortgeschritten, unabhängig davon für welche Schlüssel sie ausgestellt wurden. CA-Cert behauptet, dass es in der EU einfache, fortgeschrittene und qualifizierte Zertifikate gäbe und manche setzen sogar Signaturen und Zertifikate gleich.

Zur Erinnerung: Die Signatur-Richtlinie der EU [1] definiert allgemein den Begriff der elektronischen Signatur und zusätzlich die fortgeschrittene (advanced) Signatur. Letztere muss vier Eigenschaften erfüllen:

- ♦ sie ist ausschließlich dem Unterzeichner zugeordnet;
- ♦ sie ermöglicht die Identifizierung des Unterzeichners;
- ♦ sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;
- ♦ sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Signaturen, die eine dieser Eigenschaften nicht haben, werden mitunter als einfache Signaturen bezeichnet. Dazu gehören beispielsweise Signaturen, die nicht von natürlichen Personen geleistet werden, die auf schwach werdenden Algorithmen beruhen oder die nur an die Person, nicht aber an die signierten Daten gebunden sind. Elektronische Daten, die zur Verschlüsselung oder zur Schlüsselvereinba-

rung dienen, gehören jedoch auf keinen Fall in diese Kategorie. Die so genannten „eingescannt“ Signaturen haben keine einzige der genannten Eigenschaften und sollten daher eher als Zierschleifchen und nicht als Signaturen bezeichnet werden.

Qualifizierte Signatur

Für die in Artikel 5 (2) der Richtlinie [1] genannten fortgeschrittenen Signaturen, die auf einem qualifizierten Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt wurden, hat sich inzwischen die Bezeichnung „qualifizierte Signatur“ eingebürgert. Diese kurze Bezeichnung ist auch sinnvoll. Sie ist klar, eindeutig und durch das Signaturgesetz [2] sogar gesetzlich festgelegt.

„Qualified Certificates“ sind durch die Anforderungen des Anhangs I der Richtlinie [1] definiert, eine etwas andere Definition für „qualifizierte Zertifikate“ findet sich im Signaturgesetz § 7. Grundsätzlich wird mit einem Zertifikat ein bestimmter Schlüssel mit einem Inhaber verbunden; und bei qualifizierten Zertifikaten ist diese Zuordnung eines Signaturschlüssels zu einem Signierenden besonders vertrauenswürdig.

Begriffsverwirrungen

„Fortgeschrittene Zertifikate“ gibt es jedoch nicht, auch keine „Zertifikate für fortgeschrittene Signaturen“. Denn auch ein qualifiziertes Zertifikat kann nämlich einem Inhaber einen Schlüssel zuordnen, mit dem man gar keine fortgeschrittenen Signaturen (mehr) erstellen kann; alle ehemals ausgestellten qualifizierten Zertifikate für RSA-1024-Schlüssel zählen heute dazu. Die Eigenschaften „Schlüssel für fortgeschrittene Signaturen“ und „qualifiziertes Zertifikat“ sind sogar unabhängig von einander. Eine fortgeschrittene elektronische Signatur kann „verblassen“, wenn man sie nicht konserviert. Ein qualifiziertes Zertifikat wird sich schwerlich mit der Zeit in ein „unqualifiziertes“ verwandeln.

Die Verwirrung in den Bezeichnungen belegt die Verwirrung in den Köpfen und führt zu krausen Formulierungen wie „eine fortgeschrittene elektronische Signatur ist technisch ein Softwarezertifikat, wel-

ches ein Schlüsselpaar und den Namen seines Inhabers enthält“ [3], die vor allem technisch keinen Sinn haben.

Mit der Harmonisierung elektronischer Signaturen und elektronischer Identifizierung im Rahmen grenzüberschreitender Dienste (CROBIES) werden jetzt fortgeschrittene Signaturen, die auf einem qualifizierten Zertifikat beruhen, ins Gespräch gebracht. Damit wird die bisher suggerierte „Hierarchie“ der einfachen, fortgeschrittenen, qualifizierten und „akkreditierten“ Signaturen aber nun erst recht zerstört. Es rächt sich jetzt die Vermischung der Begriffe und man kann ihr nur durch Rückbesinnung auf die Ursprünge des Standards X.509 begegnen. Dazu müssen wir wieder lernen, zwischen technischen, juristischen und umgangssprachlichen Begriffen zu unterscheiden.

Im Zweifelsfall muss man gemeinsam nach einer Lösung suchen und sich selbst fragen, welchen Begriff man gerade verwenden will. Geht es um einen Schlüssel oder ein Zertifikat, meint man eine Signatur oder ein signiertes Dokument?

Der Grad der Vertrauenswürdigkeit eines Zertifikats lässt sich den Richtlinien (der Policy) des Zertifizierungsdiensteanbieters entnehmen. Wenn man sich darauf bezieht, kann man neben den qualifizierten Zertifikaten auch von NCP-Zertifikaten oder EV-Zertifikaten [5] sprechen. Und vielleicht wäre dafür der Begriff eines normalisierten Zertifikats passend. Fortgeschrittene Zertifikate aber – die gibt es nicht.

Literatur

- [1] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen.
- [2] Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Art. 4 des Gesetzes vom 26. Februar 2007.
- [3] Welche zusätzlichen Anforderungen sind von öffentlichen Auftraggebern bei Verwendung von fortgeschrittenen elektronischen Signaturen in Vergabeverfahren zu stellen?, Kurzzugachten des Beschaffungsamts des Bundesministeriums des Innern, 2006.
- [4] Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market, COM(2008) 708, 28. November 2008.
- [5] ETSI TS 102042: Policy requirements for certification authorities issuing public key certificates, Technical Specification V2.1.1 (2009-05).