DuD
Datenschutz und Datensicherheit

Cross-Zertifikat

Dirk Fox

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

Die Idee der Cross-Zertifizierung findet sich schon in der ersten Version des X.509-Standards von 1989 [CCIT_98] und ist seitdem systematisch verfeinert worden [ITU_00]. Cross-Zertifikate sind dafür gedacht, originär hierarchische X.509-Zertifizierungsinfrastrukturen zu verknüpfen. Mit Cross-Zertifikaten lassen sich so „vermaschte" Infrastrukturen aufbauen, deren Zertifikatsketten („Gültigkeitspfade") über die Grenzen der beteiligten Infrastrukturen hinweg reichen.[1]

Im Kern ist ein Cross-Zertifikat ein Paar von CA-Zertifikaten, die sich zwei unterschiedliche Zertifizierungsinstanzen (CAs) gegenseitig zu ihren öffentlichen Schlüsseln ausstellen. Auf diese Weise können Zertifikate einer Infrastruktur von externen Nutzern, deren CA über ein Cross-Zertifikat angebunden ist, automatisch verifiziert werden.

Nicht notwendig werden mit einer Cross-Zertifizierung automatisch alle Zertifikate unterhalb der zertifizierten Cross-CA anerkannt: Die Anerkennungswirkung von Cross-Zertifikaten auf Zertifkate einer fremden Infrastruktur kann durch geeignete Wahl der Attribute im Cross-Zertifikat in vielfältiger Weise eingeschränkt werden.

- Sollen ausschließlich solche externen Nutzer-Zertifikate anerkannt werden, die von einer Cross-CA selbst ausgestellt wurden, kann dies durch die Nutzung des Attributs `pathLenConstraint` im Cross-Zertifikat erzwungen werden (Wert 0).
- Die Anerkennung fremder Zertifikate kann auch durch die Festlegung zulässiger Namensanteile beschränkt werden. Dafür sind die Parameter `permittedSubtrees` und `excludedSubtrees` des Attributs `NameConstraints` im Cross-Zertifikat geeignet zu wählen.
- Das Attribut `CertificatePolicy` erlaubt weiter eine Beschränkung der Wirkung der Cross-Zertifizierung auf Zertifikate, die unter einer bestimmten Policy ausgestellt wurden. Dazu wird im `policyIdentifier` der für die gewünschte Zertifizierungs-Policy vergebene weltweit eindeutige `ObjectIdentifier` eingetragen.
- Über das Feld `policyMapping` können zudem zwei prinzipiell unterschiedliche Zertifizierungs-Policies als gleichwertig anerkannt werden, wenn eine Festlegung einer gemeinsamen Policy nicht möglich oder nicht opportun ist.

Cross-Zertifikate haben eine Reihe sehr wichtiger praktischer Vorzüge gegenüber anderen technischen Lösungen zur Anerkennung fremder Zertifikate:

- Sie können, anders als Zertifikate mit „direct trust" oder Root-Zertifikate, zentral zurückgerufen werden, ohne dass dadurch Sicherheit oder Verfügbarkeit der eigenen Infrastruktur betroffen wäre.
- Sie erlauben eine kontrollierte Anerkennung fremder Zertifikate.

Praktische Schwierigkeiten

Ein zentrales praktisches Problem ist das Fehlen vereinheitlichter Zertifizierungspolicies, z.B. in Gestalt von Zertifikatsklassen. Die heute in der Praxis verwendeten Certification Policies entscheiden sich nicht nur konkret inhaltlich, sondern auch strukturell (Detaillierungsgrad, Verbindlichkeit, Regelungsgegenstand) erheblich und sind daher praktisch kaum vergleichbar.

Da X.509-Zertifikate sehr komplexe Festlegungen enthalten können, ist ein Policy-Vergleich sehr zeitaufwändig. Außerdem sind dort nicht nur Zertifikatsattribute wie Schlüssellänge, Hashfunktion, verwendeter Signieralgorithmus und Gültigkeitszeitraum festgelegt, sondern üblicherweise auch Angaben über die Sicherheitsmaßnahmen in der Zertifizierungsstelle selbst oder Festlegungen wie die Häufigkeit der Verbreitung von Sperrinformationen oder maximale Zeiträume zwischen Sperrantrag und Veröffentlichung der Sperrinformation, die stark differieren können. Ein regelbasierter, automatischer Vergleich zweier Policies ist daher sicher auf absehbare Zeit nicht zu erwarten.

Da eine Cross-Zertifizierung in der Regel zwischen bereits produktiven Zertifizierungsstellen erfolgt, kann die existierende Belegung einzelner Zertifikatsattribute der jeweiligen CA-Zertifikate eine Cross-Zertifizierung verhindern: Wurde beispielsweise durch das Attribut `pathLenConstraint` die Anzahl maximal nachfolgender Zertifizierungsinstanzen in einem CA-Zertifikat auf *n* begrenzt – eine Festlegung, die aus Sicherheitsgründen sinnvoll sein kann –, dann gilt ein Cross-Zertifikat für maximal *n-1* nachgeordnete CAs.

Eine wichtige Voraussetzung für die Nutzung von Cross-Zertifikaten ist weiter die externe Verfügbarkeit von Sperr-Informationen der Cross-CA (OCSP-Responder oder CRLs) und ggf. nachgeordneter CAs, damit die Gültigkeitsprüfung fremder Zertifikate durchgeführt werden kann. Dies kann in der Praxis schwierig zu realisieren sein.

Eine derzeit erhebliche Einschränkung für den Einsatz von Cross-Zertifikaten ist die unvollständige oder fehlerhafte Auswertung in existierenden Client-Komponenten. Diese müssen beispielsweise aus mehreren möglichen Zertifikatsketten einen gültigen Zertifizierungspfad herausfinden können.

Literatur

[CCIT_89] CCITT Recommendation X.509: *The Directory: Authentication Framework*. Genf 1989.

[ITU_00] International Telecommunication Union: *Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks,* ITU-T Recommendation X.509 (2000).

[Hamm_01] Hammer, Volker: *Cross-Zertifikate verbinden*. DuD 2/2001 (in diesem Heft).

[1] Genauer siehe [Hamm_01], in diesem Heft.