DuD
Datenschutz und Datensicherheit

Certificate Revocation List (CRL)

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.

Beim praktischen Einsatz von Schlüsselzertifikaten kann es erforderlich sein, dass das Zertifikat eines Teilnehmers in einer Public Key-Infrastruktur vorzeitig, d.h. noch innerhalb des Gültigkeitszeitraums für ungültig erklärt werden muss. Dieser Vorgang wird **Zertifikats-Rückruf** oder -Sperrung genannt. Da der Rückruf sich nicht auf den Schlüssel, sondern auf die Bestätigungsaussage des Zertifikats bezieht, muss er von der Zertifizierungsstelle vorgenommen werden.

Der Rückruf eines Schlüsselzertifikats wird vom Schlüsselinhaber (bzw. einem im Zertifikat explizit ermächtigten Vertreter) oder – im Fall der Kompromittierung des CA-Schlüssels – direkt von der Zertifizierungsinstanz eingeleitet. Dafür sind organisatorische Abläufe erforderlich, die eine Authentisierung des Schlüsselinhabers (bzw. des Vertreters) bei der Rückrufannahme erlauben.

Rückruflisten

Zur Verbreitung aktueller Zertifikatsrückrufe werden von einer Zertifizierungsinstanz (CA) üblicherweise regelmäßig Rückruflisten (*Certificate Revocation Lists*, CRL) veröffentlicht. Eine solche CRL enthält die Seriennummern und das jeweilige Rückrufdatum aller von der CA zurückgerufenen Schlüsselzertifikate. Sie wird von der CA digital signiert, um Integrität und Authentizität sicherzustellen.

Das Format für den Aufbau von CRLs wurde im ITU-Standard X.509v2 spezifiziert. Eine CRL muss danach die folgenden Daten enthalten:

- eine CRL-Seriennummer,
- die Seriennummern aller seit Ausstellung der letzten CRL von der CA zurückgerufenen Zertifikate mit Sperrzeitpunkt,
- die Seriennummern aller bislang zurückgerufenen und noch nicht abgelaufenen Zertifikate der CA mit Sperrzeitpunkt,
- einen Gültigkeitszeitraum.

Weiter sind optionale Ergänzungen des Rückrufeintrags möglich (Angabe des Rückrufgrunds, Referenz auf eine Rückruf-Policy).

Rückrufgründe

Damit Zertifikatsrückrufe bei einer Zertifikatsprüfung bewertet werden können, sollten in der CRL die Rückrufgründe angegeben werden. Das X.509-Format unterstützt die folgenden Rückrufgründe:

```
unspecified             (0),
keyCompromise           (1),
cACompromise            (2),
affiliationChanged      (3),
superseded              (4),
cessationOfOperation    (5),
certificateHold         (6),
removeFromCRL                (8)
```

CRL-Rückrufgründe nach X.509v2

Dabei lassen sich dringliche und weniger dringliche Rückrufgründe unterscheiden:

Ein **dringlicher Rückrufgrund** liegt vor, wenn die Gefahr besteht, dass digitale Signaturen gefälscht oder verschlüsselte Daten unberechtigt entschlüsselt werden können. Dazu zählen insbesondere die folgenden Fälle:

- Ein Schlüsselinhaber hat den Datenspeicher mit dem geheimen Schlüssel (z.B. eine Chipkarte) mglw. zusammen mit seinem Passwort verloren.
- Der Schlüssel eines Benutzers wurde kompromittiert, oder es besteht der begründete Verdacht, dass dies passiert ist.
- Der Schlüssel der Zertifizierungsstelle wurde kompromittiert, oder es besteht der begründete Verdacht, dass dies passiert ist.

Weniger dringliche Rückrufgründe liegen vor, wenn eine Nutzung des öffentlichen Schlüssels des Benutzers nicht mehr sinnvoll möglich ist, weil

- der Datenspeicher des zugehörigen geheimen Schlüssels defekt ist,
- der Datenspeicher des geheimen Schlüssels von der Registrierungsinstanz eingezogen wurde,
- der Schlüsselinhaber das Unternehmen verlassen hat, das ihm das Schlüsselpaar für Unternehmenszwecke ausgestellt hat,
- der Schlüsselinhaber seine PIN oder sein Passwort vergessen hat, oder
- der ein-eindeutige Name des Schlüsselinhabers sich geändert hat oder geändert werden muss.[1]

In diesen Fällen kann weder der Schlüsselinhaber noch ein unberechtigter Dritter digitale Signaturen mit dem zugehörigen (geheimen) Signierschlüssel erzeugen oder für den Schlüsselinhaber verschlüsselte Daten entschlüsseln.

CRL-Verteilung

Die Verteilung der CRLs erfolgt durch Veröffentlichung in einem Verzeichnisdienst (z.B. X.500-Directory) durch die CA. Der Publikationszeitraum sollte nicht zu groß gewählt werden, um die Aktualität der Zertifikatsinformationen nicht zu stark einzuschränken, aber auch nicht zu gering, um den Verteilungsaufwand zu begrenzen.

Große CRLs sollten in Teillisten aufgespalten werden. Diese Teillisten können nach unterschiedlichen Kriterien erstellt werden. Jede dieser Teil-CRLs muss einzeln von der CA signiert werden. Der X.509v3-Standard sieht ausserdem *CRL Distribution Points* vor, die für die Sperrung von Zertifikaten jeweils einer Seriennummern-Gruppe zuständig sind [ITU_93].

Literatur

[ITU_93] International Telecommunication Union: *Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*. ITU-T Recommendation X.509 (1993 E).

[1] Dies kann z.B. eintreten bei einer Änderung der Unternehmensstruktur, wenn davon der Distinguished Name (DN) betroffen ist.