

ZT IT-KOLUMNE

Kryptografie – Teil IV

Im vierten Teil der Kryptografie-Serie werden wir uns mit dem Thema „Public Key Infrastruktur (PKI)“ beschäftigen. Ein PKI-System ist in der Lage, ein digitales Zertifikat für eine sichere Daten-Kommunikation von Computersystemen auszustellen, zu verteilen und zu prüfen.

Wir haben uns im letzten Teil der Kryptografie-Serie intensiv mit den „Digitalen Zertifikaten“ beschäftigt. Hierbei werden „öffentliche Schlüssel (engl. *public keys*)“ für die Verschlüsselung der zu sendenden Daten verwendet. Digitale Zertifikate dienen dazu, die Authentizität eines öffentlichen Schlüssels und seinen zulässigen Anwendungsbereich zu bestätigen. Wir haben ebenfalls gelernt, dass dieses Verfahren zur Familie der „asymmetrischen Verschlüsselungsverfahren“ gehört. Nun kommt das Besondere: Ein weiteres digitales Zertifikat wird

heit des letzten Zertifikats in der Zertifikatskette müssen dann natürlich die Kommunikationspartner vertrauen.

Was ist eine PKI?

Als Öffentlicher-Schlüssel-Infrastruktur bzw. Public-Key-Infrastruktur (PKI, engl.: *public key infrastructure*) bezeichnet man in der Kryptologie und Kryptografie ein System, das es ermöglicht, digitale Zertifikate auszustellen, zu verteilen und zu prüfen. Die in einer PKI ausgestellten Zertifikate sind in den

stellen Zertifikate beantragen können. Die Registrierungsstelle prüft die Korrektheit der Daten im gewünschten Zertifikat und genehmigt den Zertifikatsantrag, der dann durch die Zertifizierungsstelle signiert wird. Nach erfolgreicher Prüfung und Zuordnung wird der Zertifikatsantrag von der RA an die CA weitergeleitet. Dieser Antrag kann z.B. von einem RA-Officer digital signiert und an die CA zur Ausstellung eines Zertifikats weitergeleitet werden. Die RA benötigt dann auch ein Zertifikat ihrer CA. Die Registrierungsstelle ist verant-

Zertifikatwiderrufslisten (Certificate Revocation List)

Eine Liste mit Zertifikaten, die vor Ablauf der Gültigkeit zurückgezogen wurden. Generell muss eine PKI immer auch eine Zertifikatsstatusprüfung anbieten.

Verzeichnisdienst

Ein Verzeichnisdienst ist ein durchsuchbares Verzeichnis, das die ausgestellten Zertifikate beinhaltet.

Validierungsdienst

Führt die Überprüfung von Zertifikaten in Echtzeit durch.

ANZEIGE

Unsere seit Jahren
dauerhaft günstigen
Reparatur-Festpreise.
Qualität made in Germany.
Mehr unter
www.logo-dent.de
LOGO-DENT Tel. 07663 3094

muss daher zur Überprüfung dieser Signaturen jedem Mitarbeiter vorliegen. Dieser wird aus dem Zertifikat der CA entnommen, welches sicher an die Anwender zu verteilen ist. Somit ist jeder Schlüssel einem Zertifikat und damit auch einer Person eindeutig zugeordnet. E-Mail-Programme wie z.B. Microsoft Outlook liefern in ihrer Grundeinstellung schon einige Zertifikate von Certification Authorities mit.

Revocation

Wie bei Kreditkarten kann es auch bei digitalen Zertifikaten vorkommen, dass sie zurückgerufen (*revoked*) werden müssen. Das kann nötig sein, wenn z. B.

- der private Schlüssel nicht mehr dem Eigentümer alleine bekannt ist,
- der private Schlüssel verloren ging,
- der Mitarbeiter das Unternehmen verlässt oder
- die Angaben im Zertifikat nicht mehr korrekt sind.

Dokumente

Eine PKI führt eines oder mehrere Dokumente, in denen die Arbeitsprinzipien der PKI beschrieben sind. Kernpunkte sind der Registrierungsprozess,



nochmals benötigt, um die Authentizität des Ausstellerschlüssels zu prüfen. Das Ganze lässt sich sozusagen zu einer Kette von Zertifikaten, der sogenannten „Zertifikatskette“ (oder auch „Validierungspfad oder Zertifizierungspfad“), zusammenbauen. Die digitalen Zertifikate bestätigen dabei die Echtheit des öffentlichen Schlüssels, mit dem das vorhergehende Zertifikat geprüft werden kann. Dem letzten Zertifikat bzw. der Echtheit

meisten Fällen auf Personen oder Maschinen festgelegt und werden für eine gesicherte Datenkommunikation in Computersystemen verwendet. Eine PKI bietet ein hierarchisches Gültigkeitsmodell an. Wird einer Zertifizierungsstelle vertraut, wird somit allen von ihr signierten Zertifikaten auch vertraut. Da eine PKI untergeordnete PKIs haben kann (eine sogenannte Mehrstufigkeit), wird prinzipiell auch den untergeordneten PKIs vertraut.

wortlich für die korrekte Identifizierung des Antragstellers. Nach der Signaturverordnung § 3 (1) [SigV] gilt: „Die Zertifizierungsstelle hat die Identifikation des Antragstellers gemäß § 5 Abs. 1 Satz 1 des Signaturgesetzes anhand des Bundespersonalausweises oder Reisepasses oder auf andere geeignete Weise vorzunehmen. Der Antrag auf ein Zertifikat muss eigenhändig unterschrieben sein. Soweit ein Antrag auf ein Zertifikat mit einer digitalen Signatur des Antragstellers versehen ist, kann die Zertifizierungsstelle von einer erneuten Identifikation und eigenhändigen Unterschrift absehen.“

Zertifizierungshierarchie

Eine Zertifizierungshierarchie ist durch eine klare Strukturierung (Baumstruktur) sehr übersichtlich. An der Wurzel sitzt die sogenannte Root CA. Man erkennt eine Root CA an dem selbst signierten Zertifikat (self-signed root certificate). Darunter liegen in der Hierarchie weitere CA-Systeme, deren Zertifikate von der Root CA ausgestellt werden, sie werden auch als „Subordinate CA“ (abgekürzt „SubCA“) bezeichnet (Abb.1).

Schlüsselverteilung

Um anderen Kommunikationspartnern eine verschlüsselte Nachricht zusenden zu können, wird von jedem Empfänger einer Nachricht dessen öffentlicher Schlüssel benötigt. Dem Sicherheitsziel der Authentizität entsprechend, muss jeder öffentliche Schlüssel (*public key*) von einer Certification Authority

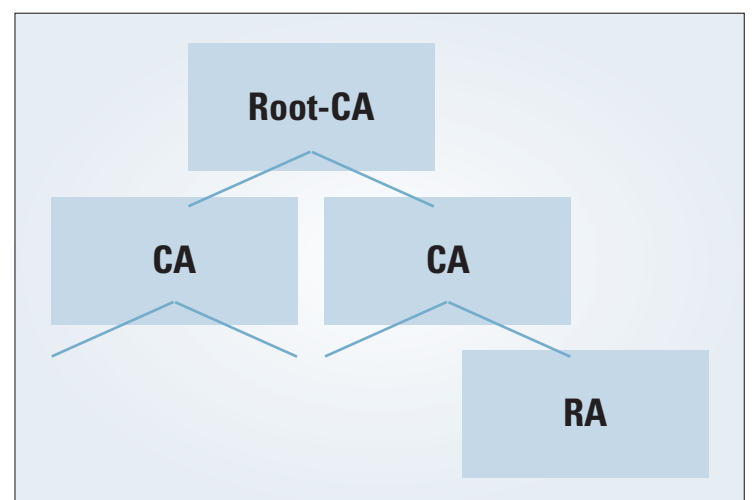


Abb. 1: Zertifizierungshierarchie

unterzeichnet worden sein, womit dann belegt wird, dass der vorliegende Schlüssel auch wirklich zu dem mutmaßlichen Empfänger gehört. Der *public key* der Certification Authority

Handhabung des Secret-Key-Materials, zentrale oder dezentrale Schlüsselerzeugung, technischer Schutz der PKI-Systeme sowie evtl. rechtliche Zusicherungen.

ANZEIGE

LABOR-TRÄUME

Ein **TRAUM**, wenn man in das Richtige investiert. Über 100 Jahre Erfahrung sind dabei ein guter Garant für das Richtige: Legierungen, Galvanotechnik, Discs/Fräser, Lasersintern, Experten für CAD/CAM u. 3shape. Das alles mit dem Plus an Service! Tel. 040/860766 · www.flussfisch-dental.de

since 1911
FLUSSFISCH



Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=AT, ST=Steiermark, L=Graz, O=TrustMe Ltd, OU=Certificate Authority, CN=CA/Email=ca@trustme.dom

Validity

Not Before: Oct 29 17:39:10 2000 GMT

Not After : Oct 29 17:39:10 2001 GMT

Subject: C=AT, ST=Vienna, L=Vienna, O=Home, OU=Web Lab, CN=anywhere.com/Email=xyz@anywhere.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

```
00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
f0:b4:95:f5:f9:34:9f:f8:43
```

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Alternative Name:

email:xyz@anywhere.com

Netscape Comment:

mod_ssl generated test server certificate

Netscape Cert Type:

SSL Server

Signature Algorithm: md5WithRSAEncryption

```
12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
ff:8e
```

Abb. 2: Strukturaufbau eines X.509-Zertifikats.

(Quelle: Wikipedia)

Aufbau eines Zertifikats

Was genau beinhaltet denn nun ein digitales Zertifikat? In der Abbildung 2 sehen Sie als Beispiel den Strukturaufbau eines X.509-Zertifikats.

Erklärung des X.509 Beispielzertifikats von Abbildung 2


Die *Version* bestimmt die Versionsnummer des Zertifikates. Je nach Versionsnummer ändern sich auch Inhalt und Anzahl der Felder des Zertifikates.

Die *Serial Number* in Verbindung mit dem Ausstellernamen ist ein eindeutiges Indiz für jedes Zertifikat und bezieht sich nur auf ein einziges Zertifikat.

Der *Issuer* (Name der Aussteller) bezieht sich auf den Namen der Zertifizierungsstelle (CA = *Certification Authority*, deutsch Zertifizierungsstelle), die das Zertifikat erzeugt und signiert hat. Der Name des Subjekts bzw. *Subject* bezieht sich hingegen auf den Benutzer, also dem Eigentümer des Zertifikats. Das Zertifikat besitzt außerdem ein Feld, das das Gültigkeitsinter-

vall (*Not Before* und *Not After*) des Zertifikates angibt.

Zusätzlich informiert es über die Namen (*Public Key Algorithm*) der Algorithmen, mit denen der öffentliche Schlüssel des Eigentümers signiert wurde. In diesem Beispiel „rsaEncryption“.

Am Ende beinhaltet das Zertifikat ein Feld, das alle anderen Felder des Zertifikats abdeckt. Dieses stellt eine digitale Signatur der anderen Felder dar, die von der CA erzeugt und dem Zertifikat angehängt wird. 

ZT Adresse

Thomas Burgard Dipl.-Ing. (FH)
Softwareentwicklung
& Webdesign
Bavariastraße 18b
80336 München
Tel.: 089 540707-10
info@burgardsoft.de
www.burgardsoft.de
burgardsoft.blogspot.com
twitter.com/burgardsoft



Infos zum Autor

VERTRAUEN DURCH KOMPETENZ

FACH DENTAL



SÜDWEST 2014

Über 200 Aussteller präsentieren ihr umfangreiches Produkt- und Dienstleistungsportfolio für Zahntechnik und Zahnmedizin. Sammeln Sie bis zu zehn Fortbildungspunkte auf dem Symposium des Dental Tribune Study Clubs und informieren Sie sich über die Top-Themen:

- > **Prophylaxe – gesunde Zähne durch gute Vorsorge.**
- > **Ästhetische Zahnheilkunde – das i-Tüpfelchen hochwertiger Zahnmedizin.**
- > **Kinderzahnheilkunde – so macht der Zahnarztbesuch Kindern Spaß!**

10. – 11. OKTOBER MESSE STUTTGART

www.fachdental-suedwest.de

Eintrittskarten-Gutscheine erhalten Sie bei Ihrem Dental-Depot!