Detlev Spierling

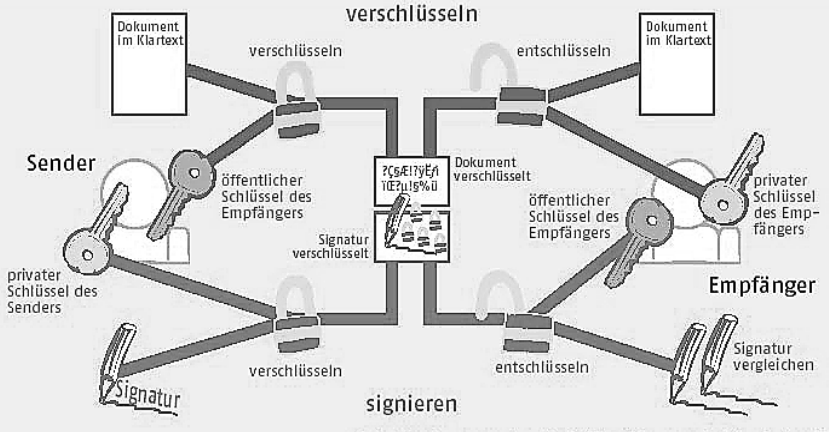
Public-Key-Infrastrukturen – ein Schlüssel zur IT-Sicherheit (Teil I)

Schätzungen des *Bundesamts für Sicherheit in der Informationstechnik* (BSI) zufolge richten digitale Bedrohungen wie so genannte „hybride Angriffe“ allein in Deutschland jährlich Schäden von mehr als einer Milliarde Euro an. Einen wirksamen Schutz der dadurch gefährdeten Unternehmensnetze und -daten verspricht die Einrichtung einer Public-Key-Infrastruktur (PKI).

Für die Übermittlung wichtiger Geschäftsdokumente per Internet, aber auch für die Anmeldung im Firmennetz und zahlreiche weitere sicherheitskritische Anwendungen wie Online-Banking ist heute die eindeutige und zuverlässige Authentifizierung der Absender bzw. Anwender erforderlich. Genau diese Eindeutigkeit und damit die erforderliche Sicherheit können die bisher gebräuchlichen Verfahren jedoch nicht bieten: Noch immer wird zum Beispiel das Gros aller E-Mails unverschlüsselt und ohne ID-Nachweis des Absenders verschickt; Benutzernamen, Passwörter und PINs (*Personal Identification Numbers*) werden ebenso oft notiert bzw. in einer zentralen Datenbank abgelegt wie gestohlen oder lassen sich je

PKI-FUNKTIONEN: KRYPTOGRAPHIE UND SIGNATUR

PUBLIK-KEY-INFRA-STRUKTUREN wie die von BMW verwenden das so genannte asymmetrische Verfahren, und zwar sowohl beim Ver- und Entschlüsseln von Dokumenten als auch für digitale Signaturen.



Ein Dokument wird mit dem öffentlich bekannten Schlüssel des Empfängers verschlüsselt. Es kann nur mit dem ihm zugeordneten, geheimen oder privaten Schlüssel des Empfängers in Klartext zurückverwandelt werden.

Beim Signieren werden die Schlüssel in umgekehrter Reihenfolge verwendet: Die mit einem geheimen Signaturschlüssel des Absenders erstellte Signatur wird vom Empfänger mit dem zugehörigen öffentlichen Schlüssel des Absenders auf Echtheit überprüft.

Quelle: CIO

nach Qualität durch simples Raten oder per Brute-Force-Attacke herausfinden. Eine zuverlässige Alternative bietet demgegenüber der Aufbau von Public-Key-Infrastrukturen, in denen u. a. die Fachleute des *TeleTrusT Deutschland e. V.* die „derzeit beste Methode für die sichere Kommunikation per Internet“ sehen.

Das Prinzip einer PKI basiert auf dem bekanntesten und gebräuchlichsten asymmetrischen Verschlüsselungsalgorithmus RSA, den Ron **R**ivest, Adi **S**hamir und Len **A**dleman 1977/78 am *Massachusetts Institute of Technology* entwickelten. Bei diesem kryptographischen Verfahren verwenden Sender und Empfänger zur Chiffrierung und Dechiffrierung ein Schlüsselpaar, das aus einem öffentlichen Schlüssel (*public key*) und seinem geheimen Gegenstück (dem *private key*) besteht. Will ein Sender *S* eine vertrauliche Information an den Empfänger *E* übermitteln, so chiffriert er sie mit dessen öffentlichem Schlüssel. Am anderen Ende dechiffriert der legitime Empfänger – und nur er – die Nachricht mit seinem geheimen Schlüssel. Auf diese Weise ist während des gesamten Vorgangs die Vertraulichkeit gesichert, denn selbst wenn es Datendieben gelingt, eine Nachricht abzufangen, können sie ohne geheimen Schlüssel nicht auf die darin enthaltenen Informationen zugreifen. Damit das funktioniert, muss der öffentliche Schlüssel allgemein zugänglich sein, der private oder geheime Schlüssel dagegen unbedingt geheim bleiben.

Sicherheits-Framework

Der Begriff PKI bezeichnet den technischen und organisatorischen Rahmen, innerhalb dessen auf asymmetrischer Verschlüsselung basierende Sicherheitsfunktionen bereitgestellt werden. Neben Protokollen, Diensten und Standards, die eine einheitliche Umsetzung garantieren, bedarf es zu ihrem Aufbau vor allem zweier Kerninstanzen, der Zertifizierungsstelle (Certification Authority – CA) und der Registrierungsstelle (Registration Authority – RA), welche die eindeutige Zugehörigkeit eines Schlüsselpaares zu einem User bestätigen (zertifizieren) und so die notwendige Vertrauensbasis schaffen. Im Einzelnen haben sie folgende Aufgaben:

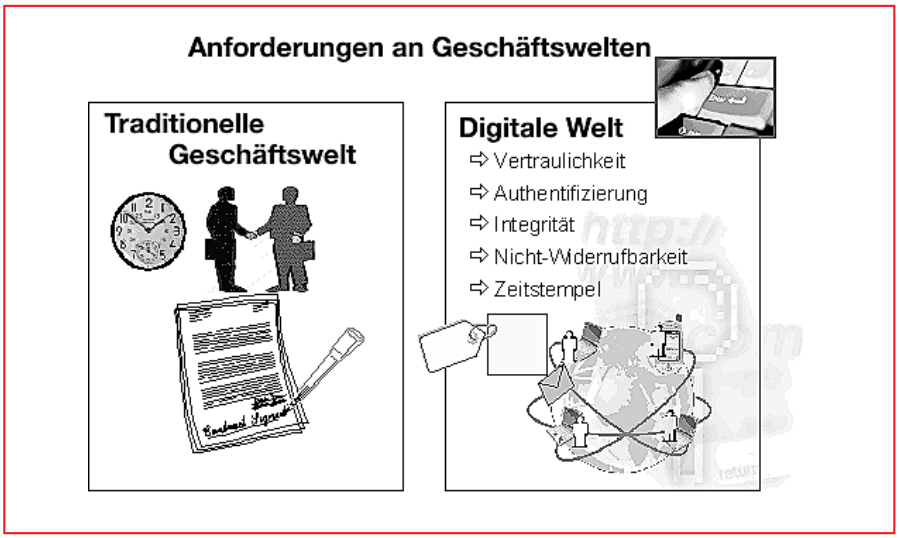
- Die **Registration Authority** nimmt Anträge auf Erteilung eines digitalen Zertifikats entgegen, überprüft die Identität eines jeden Antragstellers (Name, E-Mail-Adresse, Postanschrift) und leitet den Antrag und das Ergebnis der Prüfung an eine CA weiter.
- Die **Certification Authority** ist dazu da, die gewünschte Bescheinigung auszustellen und an den Antragsteller zu übermitteln. Im Rahmen einer PKI gewährleistet sie die Zuordnung öffentlicher Schlüssel zu ihren Inhabern und steht für deren Richtigkeit gerade. Bei der Generierung eines Zertifikats bedient sich die CA vorgegebener Policies (Richtlinien), die etwa die Gültigkeitsdauer oder zusätzliche Einsatzzwecke eines Schlüssels festlegen – beispielsweise wenn dieser außer zur Anmeldung im Netz auch zum Signieren von E-Mails dienen soll. Nach der Zertifizierung legt die CA den *public key* in einer frei zugänglichen Datenbank bzw. auf einem Verzeichnis-Server (Repository) ab. Der *private key* dagegen darf, wie bei RSA, nur dem Benutzer

bekannt sein und sollte aus Sicherheitsgründen auf einer Smartcard oder einem Token gespeichert werden.

Digitales Zertifikat

Das digitale Zertifikat ist also nichts anderes als eine Art Ausweis, der den Anwender z. B. im Internet eindeutig identifiziert. Damit es diesen Zweck erfüllt, muss es aber neben Angaben zum Schlüsselpaar und seinem Inhaber noch weitere Informationen enthalten, ganz wie ein „normaler“ Reisepass oder Personalausweis auch. In diesem Fall gehören dazu das Ablaufdatum, der Name der zertifizierenden CA und eine eindeutige Seriennummer. Der wichtigste Bestandteil ist jedoch die digitale Signatur der CA – sie entspricht gewissermaßen dem Stempel des Einwohnermeldeamts.

Am Zertifizierungsvorgang selbst sind grundsätzlich zwei Parteien beteiligt, der Antrag- und der Aussteller, die zu diesem Zweck wiederum asymmetrische Schlüsselpaare einsetzen: Will ein Antragsteller zertifiziert werden, übergibt er seinen öffentlichen Schlüssel dem Aussteller, also der CA. Diese bildet einen Daten-



satz, der sich aus ihrem Namen, dem Namen des Antragstellers und dessen öffentlichem Schlüssel zusammensetzt, und signiert diesen anschließend mit *ihrem* privaten Schlüssel. Zusammen mit der Signatur bildet dieser Datensatz das Zertifikat. Mit dem öffentlichen Schlüssel der CA kann der elektronische Ausweis jetzt jederzeit auf seine Unverfälschtheit (Gültigkeit und Echtheit) überprüft werden.

Optimale Sicherheit für vielfältige Anwendungen

Mit ihren charakteristischen Eigenschaften erfüllt eine PKI die vier Grundanforderungen an einen zeitgemäßen, gesicherten Datenverkehr:

- Durch den Einsatz von Verschlüsselungsmechanismen gewährleistet sie **Vertraulichkeit**.
- Nachträgliche Veränderungen an einem Dokument beschädigen die digitale Signatur; umgekehrt beweist deren Intaktheit, dass es sich tatsächlich um das Original handelt – also die **Integrität** der übermittelten Information.
- Die Anmeldung am Netz via Smartcard/Token (oder bei E-Mails die Verwendung der digitalen Signatur) bewirkt, dass ein Anwender (Absender) eindeutig bestimmbar ist – garantiert also **Authentizität**.
- Dank des gleichen Mechanismus können Arbeiten an einem Dokument Usern eindeutig zugewiesen werden – somit ist **Unwiderrufbarkeit** gegeben.

Zusätzlichen Sicherheitsgewinn verspricht darüber hinaus die Hardware-Implementierung einer PKI: Anders als der eingangs erwähnte berüchtigte Notizzettel mit wichtigen Passwörtern bleiben Chipkarten oder RSA-Token in Form eines USB-Sticks nur selten offen liegen, und anders als Passwortdateien auf dem PC oder entsprechende Datenbanken im Firmennetz können sie auch nicht gehackt werden. In beiden Fällen finden die Verschlüsselungs-/Authentifizierungsoperationen auf einem internen Prozessor statt; der private Schlüssel des Benutzers wird in einem einbruchs-, manipulations- und auslesesicheren Bereich des verwendeten Mediums erstellt, gespeichert und verwaltet. Im Normalfall sollten Anwender RSA-Token bevorzugen, da diese robuster als Chipkarten sind und zudem kein eigenes Lesegerät benötigen, sondern einfach in den entsprechenden USB-Port des PC gesteckt werden.

Die vielfältigen positiven Merkmale qualifizieren PKI für den Einsatz mit allen Anwendungen, bei denen die Sicherheit im Vordergrund steht. Dazu gehören nach Ansicht des *TeleTrusT* zum Beispiel:

- sichere Internet-Verbindungen (z.B. SSL/TLS, HTTPS);
- sichere E-Mail (z.B. S/MIME);
- sicherer Zahlungsverkehr (z.B. SET, EDIFACT);
- Unterschreiben von elektronischen Formularen;
- Elektronische Signatur (als Äquivalent zur eigenhändigen Unterschrift);
- Bankanwendungen (z.B. HBCI/Online-Brokerage);
- Urheberrechtsschutz/digitale Wasserzeichen;
- sicherer Datentransfer;
- Virtual Private Networks (z. B. IPSec);
- Mobile Commerce.

Wie der Aufbau einer PKI praktisch funktioniert, zeigt Teil 2 dieses Artikels im nächsten Heft.

Zum Autor:
Detlev Spierling ist freier IT-Fachjournalist und Inhaber des *Redaktions- & PR-Büros Spierling*. Er schreibt für die Tages- und Fachpresse und berät IT- und Telekommunikationsunternehmen bei ihrer Presse- und Öffentlichkeitsarbeit. E-Mail-Kontakt: ds@spierling.de.