Prof. Dr. Norbert Pohlmann, Malte Hesse

Kryptographie: Von der Geheimwissenschaft zur alltäglichen Nutzanwendung (VI) – Zweck und grundlegende Funktionsweise von Public-Key-Infrastrukturen

Nachdem wir im letzten Artikel die Funktionen einer digitalen Signatur kennen gelernt und den Bedarf an kryptographischen Prüfsummen und Zertifikaten erläutert haben, wollen wir diesmal auf die Infrastrukturen zur Verwaltung von Schlüsseln bzw. Zertifikaten eingehen: die so genannten Public-Key-Infrastrukturen (PKI).

Wir haben Zertifikate als von einer Ausgabestelle signierte Sammlung aus persönlichen Informationen über eine Person und deren öffentliche Schlüssel kennen gelernt. Darüber hinaus enthalten sie Angaben zu den für die Signatur verwendeten Algorithmen und Prüfsummen sowie zu ihrer eigenen Gültigkeit und zum Herausgeber. Mit Hilfe des öffentlichen Schlüssels einer Zertifizierungsstelle kann die Echtheit eines Zertifikats und seiner Inhalte verifiziert werden. Dadurch lässt sich in modernen IT-Systemen im Prinzip ein einfaches und organisationsübergreifendes Key Management realisieren. Durchgesetzt haben sich Zertifikate nach dem Standard X.509 der *International Telecommunication Union* (ITU).

Idee und Definition von Public-Key-Infrastrukturen

Public-Key-Infrastrukturen (PKI) dienen zum Verwalten von Zertifikaten mit öffentlichen Schlüsseln über deren gesamten Lebenszyklus, von der Erstellung über die Aufbewahrung und Verwendung bis hin zur Entsorgung. Dabei kommt es außer auf die sichere Erstellung gültiger Schlüssel auch auf die Verifizierung der ursprünglichen Identität ihrer Inhaber – der so genannten PKI-Teilnehmer – an.

Public-Key-Infrastrukturen bestehen aus Hardware, Software und einem abgestimmten Regelwerk, der Leitlinie. Diese definiert, nach welchen Sicherheitsregeln die Dienstleistungen um die Zertifikate erbracht werden. Dazu zählen das Betriebskonzept der PKI, die Nutzerrichtlinien sowie Organisations- und Arbeitsanweisungen.

Im Allgemeinen ist es üblich, die Registrierung der Teilnehmer und die Zertifizierung der Schlüssel voneinander zu trennen und zum Teil auch an unterschiedlichen Orten vorzunehmen.

Einsatz und Anwendungsformen

Eine PKI stellt zentrale Sicherheitsdienste zur Verfügung, schafft also die Voraussetzungen dafür, dass eine Anwendung vertrauenswürdig realisiert werden kann. Die folgende Grafik zeigt im oberen Teil den prinzipiellen Aufbau einer Public-Key-Infrastruktur sowie einige Kommunikationskanäle, die dabei benutzt werden. Im unteren Bereich ist schematisch eine Anwendung abgebildet, deren Sicherheitsmechanismen die Public-Key-Infrastruktur nutzen.

Die ***Registration Authority*** **(RA)** oder Registrierungsstelle kann als private oder öffentliche Einrichtung betrieben werden, d. h. es kommen sowohl IT-Abteilungen von Unternehmen als auch externe Dienstleister sowie Behörden für diese Funktion in Frage. Die Hauptaufgabe einer RA besteht darin, die Anträ-

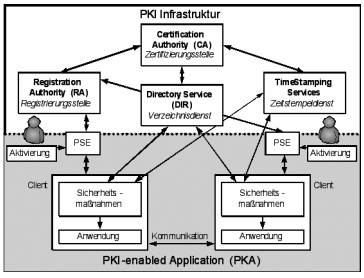

ABB. 1: Aufbau und Funktionsweise einer Public-Key-Infrastruktur (Schema)

ge auf Zertifizierung zu erfassen und die Identität der Antragsteller entsprechend der Leitlinie zu prüfen. Dies kann sehr einfach erfolgen, indem sie z. B. um die Verifikation einer E-Mail-Adresse bittet, oder auch aufwändiger und sicherer, indem sie vom Antragsteller persönliches Erscheinen und die Vorlage des Ausweises verlangt. Die RA bildet die Schnittstelle zwischen den (potenziellen) PKI-Teilnehmern und der *Certification Authority* (CA), an die sie deren Anträge weiterleitet.

Die ***Certification Authority*** (auch: Zertifizierungsstelle) vergibt eindeutige Identitäten und verwaltet für jeden Teilnehmer eines oder mehrere Schlüsselpaare mit den dazugehörigen Zertifikaten. Jedes von ihr erzeugte Zertifikat verbindet den öffentlichen Schlüssel des Teilnehmers mit dessen Namen und zusätzlichen Daten (Gültigkeitszeitraum, Seriennummer, evtl. weiteren Attributen). Die CA gibt die Zertifikate aus und verwaltet sie, damit die öffentlichen Schlüssel und Attribute der Teilnehmer (Position im Unternehmen, Rechte usw.) möglichst einfach verifiziert werden können.

Zur Verwaltung der Zertifikate unterhält jede PKI einen ***Directory Service*** oder Verzeichnisdienst. Hier werden die gültigen zertifizierten öffentlichen Schlüssel der Teilnehmer veröffentlicht. Zurückgezogene oder kompromittierte Schlüssel hält der Verzeichnisdienst in einer Sperrliste (*Certificate Revocation List,* CRL) zum Abruf bereit.

Ein **Zeitstempeldienst** dient dazu, gesicherte Zeitsignaturen gemäß der Leitlinie zu erstellen. Dabei wird ein Dokument oder eine Transaktion mit der je aktuellen Zeitangabe verknüpft und diese Gesamtinformation anschließend digital signiert.

Das ***Personal Security Environment*** **(PSE)** ist die Sammlung aller sicherheitsrelevanten Daten eines Teilnehmers. Dazu gehören seine geheimen Schlüssel, die Zertifikate seiner Kommunikationspartner sowie der öffentliche Schlüssel der Zertifizierungsinstanz.

Standesamt und Einwohnermeldeamt als Analogie zu Public-Key-Infrastrukturen

Standes- und Einwohnermeldeämter sichern die eindeutige und überprüfbare Identität von Personen. Sie fungieren demnach als dritte Instanz, der wir und andere vertrauen. Das Standesamt sorgt dafür, dass wir über unsere Vor- und Nachnamen, den Geburtsort und das Geburtsdatum eindeutig identifizierbar sind, erledigt also die Aufgaben einer Registrierungsstelle. Das Einwohnermeldeamt gibt Ausweise heraus, die es ermöglichen, diese eindeutige Identität zweifelsfrei zu beweisen, fungiert mithin als Zertifizierungsstelle.

PKI-enabled Application (PKA)

Als *PKI-enabled Application* (PKA) wird eine Anwendung bezeichnet, die auf Grundlage der durch die PKI zur Verfügung gestellten Sicherheitsdienste (Zertifikate, Verzeichnisdienst etc.) eine vertrauenswürdige Nutzung ermöglicht. Eine PKA enthält selbst unterschiedliche Sicherheitsmechanismen (für Authentisierung, Verschlüsselung usw.), mit denen Vertrauenswürdigkeit (Authentizität, Integrität, Verbindlichkeit, Einmaligkeit und Vertraulichkeit) erzielt wird.

Eine PKI bildet die Sicherheitsgrundlage für die vertrauenswürdige Nutzung von Anwendungen wie:

- E-Mail,
- Dokumentverschlüsselung,
- Programmen für Online-Banking und Online-Broking,
- SSL-Kommunikation,
- VPN-Kommunikation,

- Identifikations- und Authentisierungsprozesse,
- Zahlungssysteme.

Offene und geschlossene PKI-Systeme

Ein geschlossenes PKI-System betreibt eine Organisation, wenn sie ihre PKI für eine oder mehrere Anwendungen (PKAs) nutzt, die vollständig in ihrem eigenen Verantwortungsbereich liegen. Sicherheitsdienste wie z. B. gesicherte Kommunikation oder Authentisierung stehen dann nur innerhalb der eigenen Infrastruktur zur Verfügung. Im Klartext bedeutet dies, dass die PKI nur für interne Zwecke und nicht für die Kommunikation nach außen genutzt werden kann. Da jedoch in der Praxis viele organisationsübergreifende Prozesse stattfinden, schränkt dies ihren Nutzen sehr stark ein.

Im Alltag trifft man daher meist auf offene PKI-Systeme: Dabei betreiben mehrere Organisationen jeweils eigene PKIs für eine oder mehrere Anwendungen, die in ihren Verantwortungsbereichen liegen. So ist z. B. die gesicherte Kommunikation zwischen den Teilnehmern des offenen Systems möglich. Der Austausch beruht auf gegenseitigem Vertrauen sowie auf kompatiblen Technologien und Verfahren. Allerdings muss zum Aufbau einer organisationsübergreifenden Kommunikation ein Abgleich der verschiedenen organisationsspezifischen Leitlinien erfolgen. Ziel ist ein die Schaffung einer gemeinsamen, verbindlichen Vertrauensbasis (*Level of Trust*). Hier sind geeignete Instrumente zu implementieren, um die unterschiedlichen organisatorischen und infrastrukturellen Konzeptionen zu bewerten, zu analysieren und zu gewichten.

Gerade bei der Nutzung für personenbezogene organisationsübergreifende Prozesse stellt sich aus ökonomischer Sicht und aus den tatsächlichen Anforderungen heraus die Frage, ob das Gesetz über Rahmenbedingungen für elektronische Signaturen (kurz: Signaturgesetz, SigG) die Grundlage für eine PKI und die zum Einsatz kommenden PKAs bilden muss. Hierbei ist zu berücksichtigen, dass viele organisationsübergreifende Prozesse automatisiert sind und somit nicht mehr personenbezogen ablaufen. Die Kardinalfrage in diesem Zusammenhang ist, ob innerhalb des Sicherheitskonzepts der PKI beispielsweise der Verantwortungsbereich für von Servern erstellte Signaturen geregelt ist (Haftungsausschluss).

Hinzu kommt, dass eine Vielzahl unterschiedlicher, teilweise sehr komplexer Standards für den Aufbau von PKIs existiert, die ständig weiterentwickelt werden. Die Ursache hierfür liegt in der großen Vielfalt der Anwendungen (SSL, E-Mail etc.), die mit ihrer Hilfe abgesichert werden, und den daraus resultierenden Anforderungen. Ein weiteres Problem, dem insbesondere große Organisationen gegenüberstehen, besteht darin, dass die PKAs und PKIs zwar voneinander abhängig sind, die Zuständigkeit für Entwicklung und Verwaltung aber häufig organisatorisch getrennt wird. In solchen Fällen müssen sich dann verschiedene Abteilungen auf gemeinsame Ziele und Vorgehensweisen verständigen, um die entsprechenden technischen Grundlagen zu erarbeiten.

Ausblick

In den letzten Jahren haben viele Unternehmen PKIs eingerichtet. Zu Beginn dieser Entwicklung standen dabei die Grundlagen im Vordergrund. In den letzten Jahren hat sich der Akzent auf die Interoperabilität der Systeme verschoben. Um dieses Ziel zu erreichen, waren jedoch noch einige technische und organisatorische Hürden zu überwinden. Wie dabei vorgegangen wurde und welche Standards sich herausgebildet haben, ist Thema der nächsten Folge im Mai.

Zu den Autoren: Prof. Dr. Norbert Pohlmann ist Geschäftsführender Direktor des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen. E-Mail-Kontakt: norbert.pohlmann@informatik.fh-gelsenkirchen.de

Malte Hesse ist Mitarbeiter am Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen. E-Mail-Kontakt: hesse@internet-sicherheit.de