PKI

Weitere Bezeichnungen: Public Key Infrastructure, Public-Key-Infrastruktur, Infrastruktur für öffentliche Schlüssel

Rubrik: IT-Sicherheit

Eine PKI (Public Key Infrastructure), auf Deutsch Public-Key-Infrastruktur, ist ein System zur Verwaltung digitaler Zertifikate und kryptografischer Schlüssel. Sie bildet eine wichtige Grundlage für die sichere Kommunikation und die Überprüfung digitaler Identitäten in Computernetzwerken. Mithilfe einer PKI lässt sich beispielsweise feststellen, ob ein öffentlicher Schlüssel tatsächlich zu einer bestimmten Person, Organisation oder einem Server gehört. Die Technologie wird unter anderem bei verschlüsselten Internetverbindungen, digitalen Signaturen und der sicheren E-Mail-Kommunikation eingesetzt.

Das grundlegende Funktionsprinzip einer PKI basiert auf der asymmetrischen Kryptografie. Dabei besitzt jeder Teilnehmer ein zusammengehöriges Schlüsselpaar aus einem öffentlichen Schlüssel (Public Key) und einem privaten Schlüssel (Private Key). Der öffentliche Schlüssel darf weitergegeben werden, während der private Schlüssel geheim bleiben muss. Je nach kryptografischem Verfahren können diese Schlüssel zur Verschlüsselung, zur sicheren Vereinbarung von Sitzungsschlüsseln oder zur Erstellung und Überprüfung digitaler Signaturen verwendet werden.

Eine zentrale Rolle innerhalb der PKI spielt die Zertifizierungsstelle (Certificate Authority, CA). Sie stellt digitale Zertifikate aus und bestätigt damit die Zuordnung eines öffentlichen Schlüssels zu einer bestimmten Identität oder einem anderen festgelegten Merkmal. Vor der Ausstellung eines Zertifikats führt die Zertifizierungsstelle je nach Zertifikatstyp entsprechende Prüfungen durch. Das ausgestellte Zertifikat wird anschließend von der CA digital signiert, sodass seine Echtheit überprüft werden kann.

Besonders verbreitet sind digitale Zertifikate nach dem Standard X.509. Sie enthalten unter anderem einen öffentlichen Schlüssel, Angaben zum Zertifikatsinhaber, eine Seriennummer, einen Gültigkeitszeitraum und Informationen über die ausstellende Zertifizierungsstelle. Zusätzlich enthält das Zertifikat eine digitale Signatur des Ausstellers. Mithilfe dieser Signatur können Anwendungen feststellen, ob das Zertifikat unverändert ist und von der angegebenen Zertifizierungsstelle stammt.

Die Vertrauenswürdigkeit einer PKI wird häufig durch eine Zertifikatskette (Certificate Chain) hergestellt. Dabei wird ein Zertifikat von einer Zwischenzertifizierungsstelle ausgestellt, die ihrerseits durch eine übergeordnete Zertifizierungsstelle bestätigt wird. Am Ende dieser Kette steht normalerweise ein Stammzertifikat (Root Certificate), dem das Betriebssystem oder die jeweilige Anwendung vertraut. Dieses Verfahren wird als Vertrauenskette (Chain of Trust) bezeichnet. Die Überprüfung umfasst neben den Signaturen auch weitere Bedingungen wie Gültigkeitsdauer, zulässige Verwendung und gegebenenfalls den Widerrufsstatus.

Ein wichtiges Einsatzgebiet ist die Absicherung von Webseiten durch HTTPS und TLS (Transport Layer Security). Beim Aufbau einer verschlüsselten Verbindung übermittelt der Webserver normalerweise ein digitales Zertifikat. Der Browser prüft unter anderem, ob das Zertifikat für die aufgerufene Domain gültig ist und eine vertrauenswürdige Zertifikatskette besitzt. Dadurch kann die Identität des Servers im Rahmen der durchgeführten Prüfungen bestätigt werden. Anschließend wird eine verschlüsselte Verbindung aufgebaut, die übertragene Daten vor unbefugtem Mitlesen und Manipulation schützen soll.

Digitale Zertifikate besitzen eine begrenzte Gültigkeitsdauer und können unter bestimmten Umständen vorzeitig widerrufen werden. Das ist beispielsweise notwendig, wenn ein privater Schlüssel kompromittiert wurde oder ein Zertifikat nicht mehr verwendet werden darf. Zur Überprüfung des Widerrufsstatus können Zertifikatsperrlisten (Certificate Revocation Lists, CRL) und das Online Certificate Status Protocol (OCSP) eingesetzt werden. Ob und wie diese Prüfungen durchgeführt werden, hängt von der jeweiligen Anwendung und Sicherheitskonfiguration ab.

Neben der Zertifizierungsstelle können weitere Komponenten zu einer PKI gehören. Eine Registrierungsstelle (Registration Authority, RA) übernimmt beispielsweise Aufgaben bei der Identitätsprüfung und der Bearbeitung von Zertifikatsanträgen. Darüber hinaus werden Verfahren zur sicheren Schlüsselerzeugung, Zertifikatsverteilung, Erneuerung und Sperrung benötigt. Besonders sensible private Schlüssel können in speziellen Sicherheitsgeräten, sogenannten Hardware Security Modules (HSM), gespeichert und verwendet werden.

PKI-Systeme kommen in zahlreichen Bereichen der IT-Sicherheit zum Einsatz. Dazu gehören die Authentifizierung von Webservern, die Absicherung von Unternehmensnetzwerken, digitale Dokumentensignaturen, die Signierung von Software sowie die sichere E-Mail-Kommunikation mit S/MIME. Auch bei VPN-Verbindungen und der Authentifizierung von Geräten können digitale Zertifikate verwendet werden. Unternehmen betreiben dafür teilweise eigene interne PKI-Systeme, während öffentliche Zertifizierungsstellen vor allem bei allgemein zugänglichen Internetdiensten eine wichtige Rolle spielen.

Die Sicherheit einer PKI hängt wesentlich vom Schutz der privaten Schlüssel und von der Vertrauenswürdigkeit ihrer Zertifizierungsstellen ab. Werden Schlüssel gestohlen oder Zertifikate fehlerhaft ausgestellt, können erhebliche Sicherheitsrisiken entstehen. Deshalb sind zuverlässige Identitätsprüfungen, sichere Schlüsselverwaltung und klar geregelte Zertifikatsprozesse erforderlich. Eine PKI stellt dabei die technische und organisatorische Vertrauensinfrastruktur bereit, ersetzt jedoch nicht sämtliche anderen Sicherheitsmaßnahmen.

Heute gehört die Public Key Infrastructure zu den grundlegenden Technologien moderner IT-Sicherheitsarchitekturen. Sie ermöglicht es, öffentliche kryptografische Schlüssel überprüfbaren Identitäten zuzuordnen und dadurch sichere Kommunikations- und Authentifizierungsverfahren zu unterstützen. Ohne PKI wären viele heute selbstverständliche Sicherheitsfunktionen des Internets und betrieblicher Netzwerke nur eingeschränkt oder mit anderen Vertrauensverfahren umsetzbar.

Weiterführende Informationen

Asymmetrische Verschlüsselung, Public Key, Private Key, digitales Zertifikat, X.509, Certificate Authority, Root Certificate, Zertifikatskette, digitale Signatur, TLS, HTTPS, OCSP, CRL, HSM, S/MIME