LU07a - Digitale Zertifikate Grundlagen

Lernziele

- Wissen was unter *Digitalen Zertifikaten* im Allgemeinen verstanden wird.
- Potentielle Einsatzgebiete von digitalen Zertifikaten nennen können.

Einleitung

Ein digitales Zertifikat ist ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten.

Weit verbreitet sind Public-Key-Zertifikate nach dem Standard X.509, welche die Identität des Inhabers und weitere Eigenschaften eines öffentlichen kryptographischen Schlüssels bestätigen.

Attributzertifikate enthalten dagegen keinen öffentlichen Schlüssel, sondern verweisen auf ein Public-Key-Zertifikat und legen dessen Geltungsbereich genauer fest.

Motivation

Ein **Public-Key-Zertifikat** ist ein digitales Zertifikat, das den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels bestätigt. Durch ein Public-Key-Zertifikat können Nutzer eines asymmetrischen Kryptosystems den öffentlichen Schlüssel einer Identität (z. B. einer Person, einer Organisation oder einem IT-System) zuordnen und seinen Geltungsbereich bestimmen. Damit ermöglichen Public-Key-Zertifikate den Schutz der Vertraulichkeit, Authentizität und Integrität von Daten durch die korrekte Anwendung der öffentlichen Schlüssel.

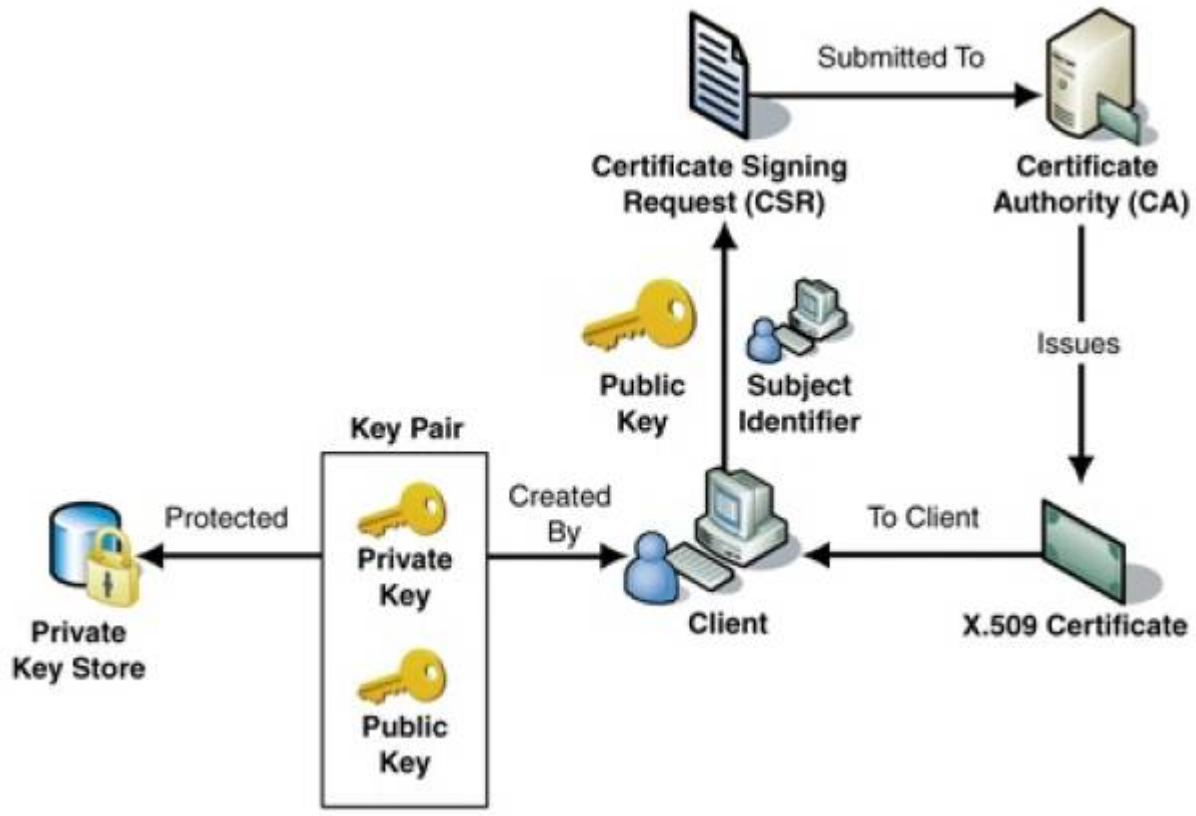
Um beim Einsatz von asymmetrischen Kryptosystemen falsche (z. B. untergeschobene) von echten Schlüsseln zu unterscheiden, wird ein Nachweis benötigt, dass der verwendete öffentliche Schlüssel auch zum designierten Empfänger der verschlüsselten Nachricht bzw. zum Sender einer digital signierten Nachricht gehört. Ausserdem muss bei der Verschlüsselung und Prüfung der digitalen Signatur sichergestellt werden, dass der Schlüssel auch mit diesem kryptographischen Verfahren und für den gedachten Anwendungsbereich verwendet werden darf. Diese Nachweise werden durch digitale Zertifikate geleistet.

Mit Hilfe eines asymmetrischen Verfahrens können Nachrichten in einem Netzwerk digital signiert und verschlüsselt werden. Sichere Kryptosysteme können bei geeigneter Wahl der Parameter, wie z. B. der Schlüssellänge, auch bei Kenntnis des Verfahrens nicht in überschaubarer Zeit gebrochen werden.

Grundkonzept

In asymmetrischen Kryptosystemen benötigt der Sender für eine verschlüsselte Übermittlung den

öffentlichen Schlüssels (Public Key) des Empfängers. Dieser könnte z. B. per E-Mail versendet oder von einer Web-Seite heruntergeladen werden. Dabei muss sichergestellt sein, dass es sich tatsächlich um den Schlüssel des Empfängers handelt und nicht um eine Fälschung eines Betrügers. Hier kommt die Zertifizierung (Echtheits-Nachweis) von PublicKeys in Spiel.



Hierzu dienen digitale Zertifikate, die die Authentizität eines öffentlichen Schlüssels und seinen zulässigen Anwendungs und Geltungsbereich bestätigen. Das digitale Zertifikat ist selbst durch eine digitale Signatur geschützt, deren Echtheit mit dem öffentlichen Schlüssel des Ausstellers des Zertifikates geprüft werden kann.

Um die Authentizität des Ausstellerschlüssels zu prüfen, wird wiederum ein digitales Zertifikat benötigt. Auf diese Weise lässt sich eine Kette von digitalen Zertifikaten aufbauen, die jeweils die Authentizität des öffentlichen Schlüssels bestätigen, mit dem das vorhergehende Zertifikat geprüft werden kann. Eine solche Kette von Zertifikaten wird *Validierungspfad* oder *Zertifizierungspfad* genannt. Auf die Echtheit des letzten Zertifikates (und des durch diesen zertifizierten Schlüssel müssen sich die Kommunikationspartner ohne ein weiteres Zertifikat verlassen können.

Anwendungsbereiche

Typische Anwendungen von Public Key Zertifikaten sind:

- Digitale Signaturen
- Sicherheit in Netzwerkprotokollen (B. SSL, darunter HTTPS für Webbrowser , IPSec oder SSH
- Schutz von E Mails (z. B. mit S/MIME oder PGP
- Authentisierung und Zugriffskontrolle bei Chipkarten.

Konzepte der Schlüsselverteilung

Unabhängig von der gewählten Verschlüsselungsart (Symmetrisch oder Asymmetrisch), müssen die Schlüssel verteilt werden. Grundsätzlich stehen uns hier zwei Konzepte bzw. Architekturen zur Verfügung.

- PKI = **P**ublic **K**ey **I**nfrastructure
- WoT = **W**eb **o**f **T**trust
