LU07b - Die Schlüsselverteilung

Lernziele

- Die zwei grundlegenden Verteilungssysteme für digitale Schlüssel nennen und erläutern können.
- Die Vor- und Nachteile zwei Varianten kennen.
- Den Ablauf der Echtheitsüberprüfung von digitalen Zertifikaten

Einleitung

Verschlüsselung schützt Daten und ermöglicht die sichere Identifikation von Kommunikationspartnern. Damit das funktioniert, müssen Kryptoschlüssel zuverlässig verteilt werden. Digitale Zertifikate binden dabei einen öffentlichen Schlüssel an eine eindeutige Identität (z. B. Person, Server, Organisation).

Die Herausforderung: Der Schlüssel muss so verteilt werden, dass er nicht manipuliert werden kann. Dafür existieren verschiedene Vertrauensmodelle, etwa die Public Key Infrastructure (PKI) mit zentralen Zertifizierungsstellen oder das Web of Trust (WoT) mit dezentraler gegenseitiger Bestätigung. Ziel beider Systeme bleibt immer: sichere und überprüfbare Schlüsselverteilung.

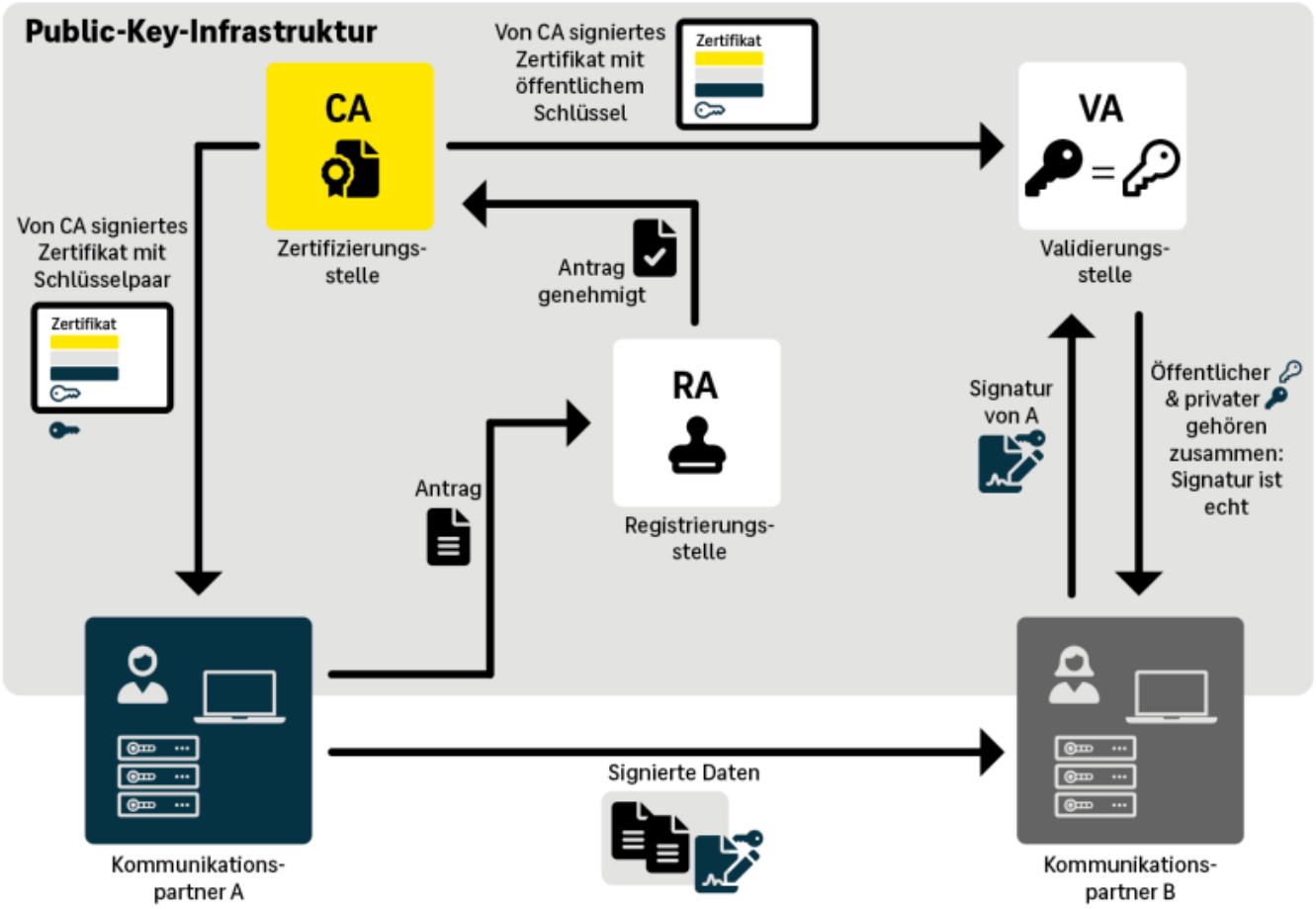
Konzepte der Schlüsselverteilung

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

PKI = Public Key Infrastructur

Mit Public-Key-Infrastruktur (PKI) bezeichnet man in der Kryptologie ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann. Die innerhalb einer PKI ausgestellten Zertifikate werden zur Absicherung rechnergestützter Kommunikation verwendet rechnergestützter Kommunikation verwendet.



WoT = Web of Trust

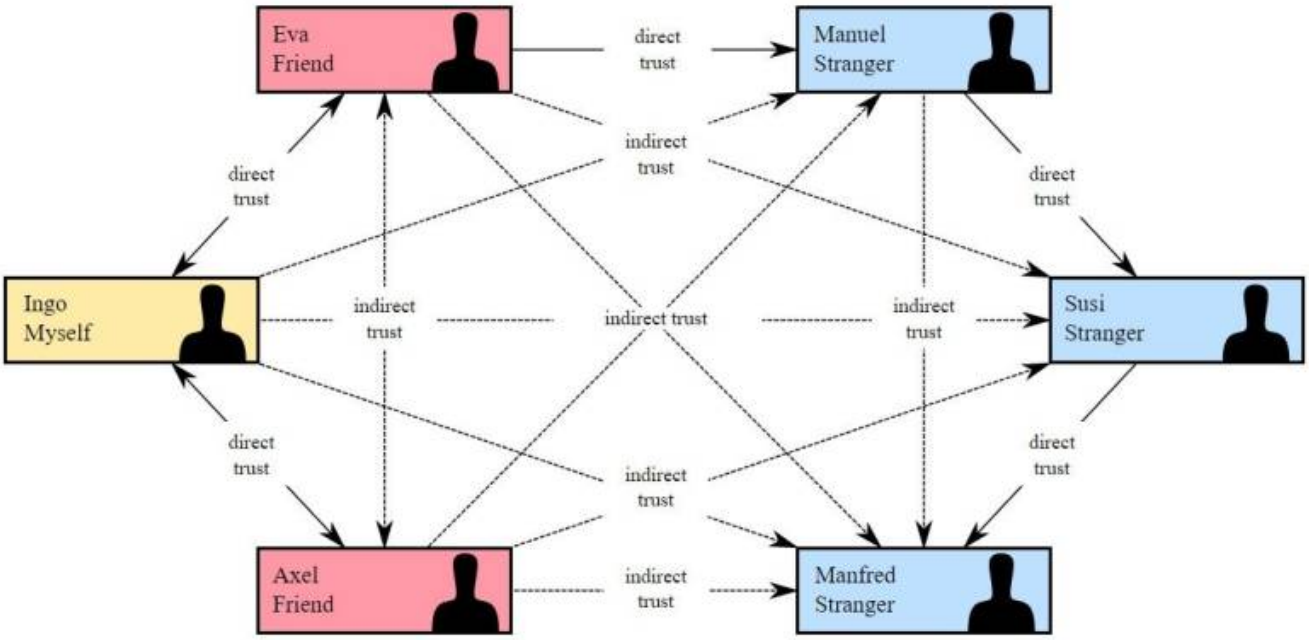
Problemstellung

Die Verschlüsselung mit öffentlichen Schlüsseln bietet (gegenüber der symmetrischen Verschlüsselung) den Vorteil, dass der auszutauschende Schlüssel nicht über einen sicheren Kanal übertragen werden muss, sondern öffentlich ist. Zur Übertragung des Schlüssels kann man sich daher eines Verbunds von Schlüsselservern bedienen, auf die jeder seine öffentlichen Schlüssel hochladen kann und von denen jeder die jeweiligen Schlüssel der Person abrufen kann, mit denen man kommunizieren möchte.

Daraus ergibt sich aber ein Problem: Eine Person könnte einen Schlüssel veröffentlichen, mit welchem sie sich als jemand anderes ausgibt. Es muss also eine Möglichkeit zur Verfügung stehen, die Authentizität eines Schlüssels zu prüfen.

Lösungs(-Ansatz) Bei der PKI wird dieser Echtheitsüberprüfung durch die Zertifizierungstelle (CA = Certification Authority). Im Web of Trust hingegen übernehmen alle Teilnehmer diese Funktion.

WOT® WEB OF TRUST	*Netz des Vertrauens* bzw. Web of Trust (WOT) ist in der Kryptologie die Idee, die Echtheit von digitalen Schlüsseln durch ein Netz von gegenseitigen Bestätigungen (Signaturen), kombiniert mit dem individuell zugewiesenen Vertrauen in die Bestätigungen der anderen („Owner Trust“), zu sichern. Es stellt eine dezentrale Alternative zum PKI-System dar.




```
Alice signiert den Schlüssel von Bob und vertraut Bobs Schlüsselsignaturen

Bob signiert den Schlüssel von Carl. Bobs Vertrauen in Carls Schlüssel ist
weder bekannt, noch relevant.

Somit betrachtet Alicen den Schlüssel von Carl als gültig.
```

—-