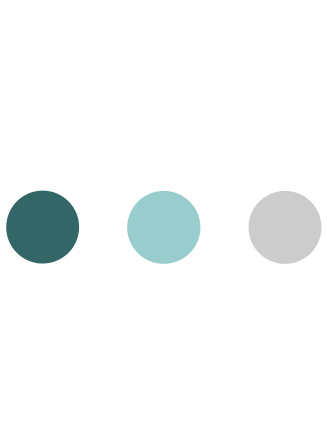
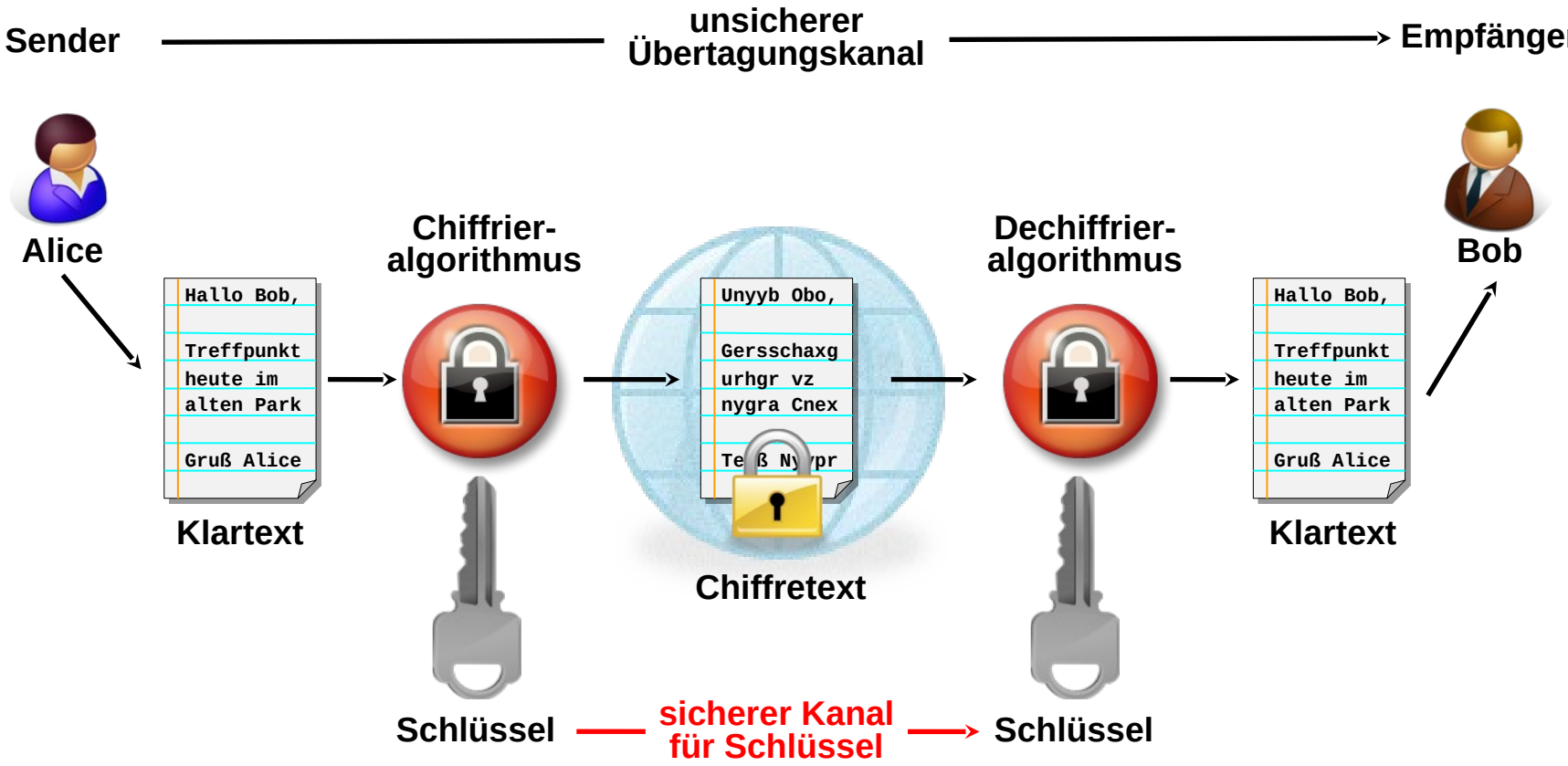


Einführung Verschlüsselung

IT-Team
Elektronikschule Tettnang
E. Dietrich, A. Grella, H. Müller

Grundprinzip der symmetrischen Verschlüsselung

- Zum Verschlüsseln und Entschlüsseln wird derselbe Schlüssel benutzt.



Vor- und Nachteile symmetrischer Verschlüsselungsverfahren

+ relativ einfache Realisierung in Hard-oder Software (z.B. AES)
  - hohe Geschwindigkeit beim Ver- bzw. Entschlüsseln für große Datenmengen geeignet
- alle Teilnehmer müssen im Besitz desselben geheimen Schlüssels sein
  - Problem des Schlüsselaustausches bzw. der Schlüsselverteilung über sichere Kanäle

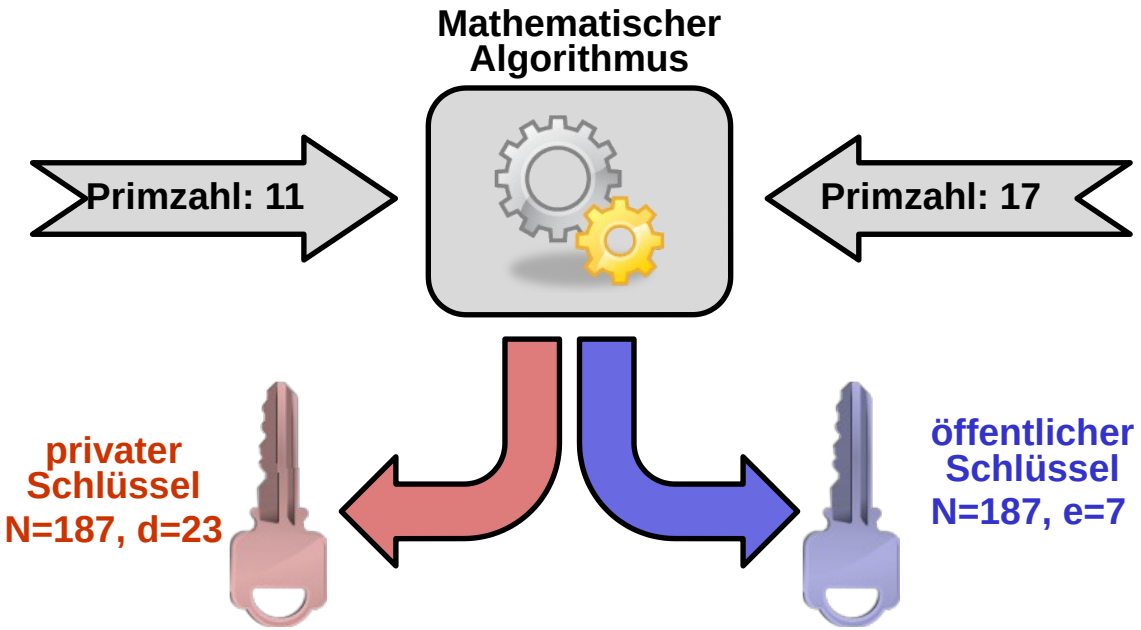
Gedankenexperiment: Geht es auch auf eine andere Weise?

- Bob hat ein Schloss mit passendem Schlüssel.
- Bob entfernt den Schlüssel und verteilt Kopien seiner geöffneten Schlösser an alle Teilnehmer. Den Schlüssel behält er bei sich.
- Will Alice eine Nachricht an Bob verschicken, verschließt sie ihre Nachricht mit einer Kopie von Bobs Schloss.
- Die Nachricht kann dann über einen unsicheren Übertragungskanal verschickt werden, denn nur Bob hat den passenden Schlüssel, um die Nachricht zu lesen.

aus Funktionsweise des RSA-Verfahrens, CrypTool-Team, Juli 2010

Schlüsselerzeugung bei asymmetrischer Verschlüsselung

- Das vorhergehende Gedankenexperiment entspricht einer asymmetrischen Verschlüsselung, die mathematisch allerdings äußerst komplex ist (Beispiel: RSA-Verfahren).
- Zum Verschlüsseln und Entschlüsseln wird jeweils ein zusammengehörendes Schlüsselpaar, bestehend aus einem öffentlichen Schlüssel (Public Key = geöffnetes Schloss) und einem privaten Schlüssel (Private Key = geheimer Schlüssel) benutzt.



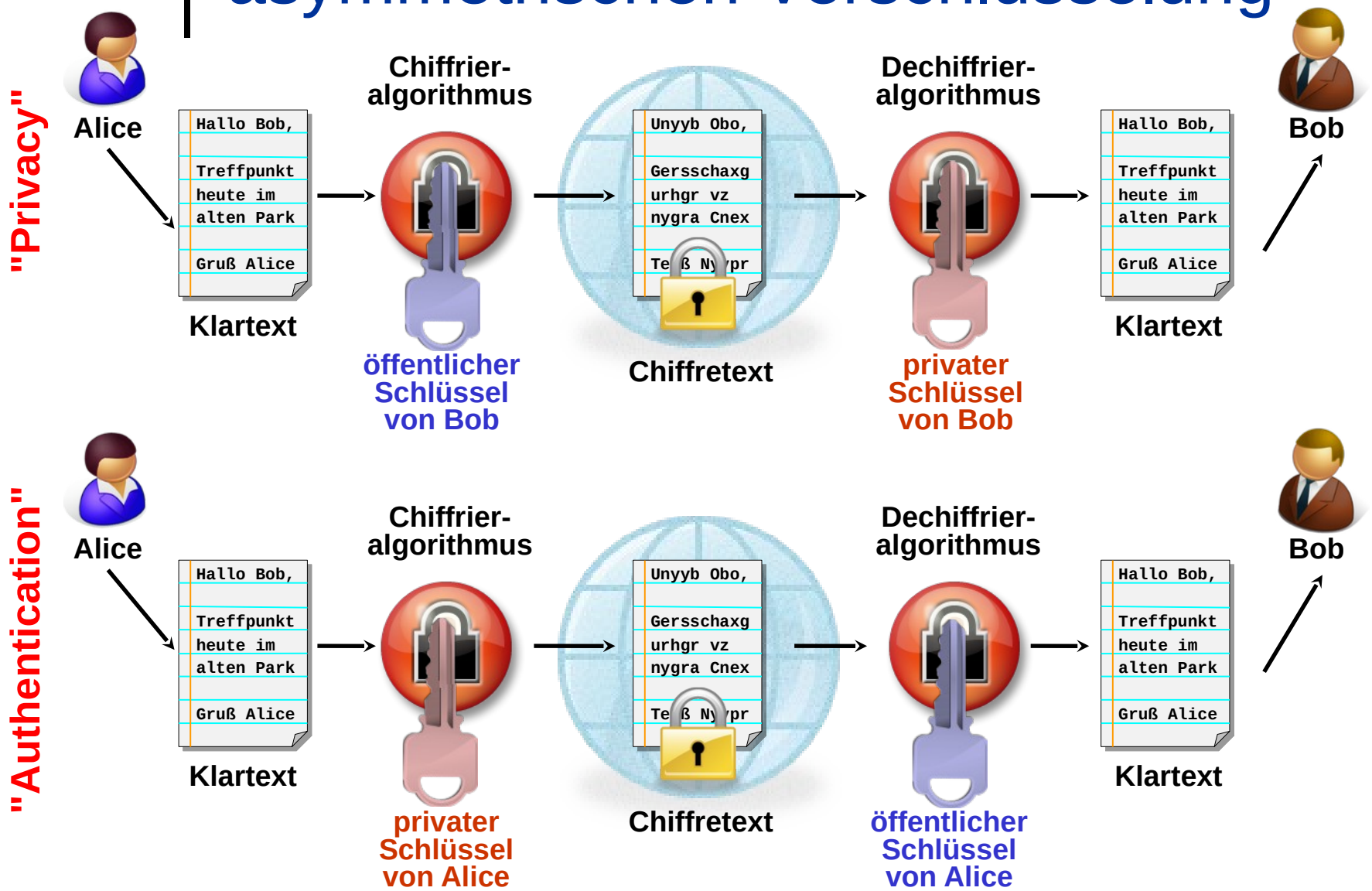
Eigenschaften des Schlüsselpaares

Privater Schlüssel

öffentlicher Schlüssel

- Es werden immer Schlüsselpaare generiert.
- Die Kenntnis eines Schlüssels reicht zur nachträglichen Berechnung des anderen Schlüssels (praktisch) nicht aus!
- Der Private-Key wird nie aus der Hand gegeben.
- Der Public-Key wird für jedermann zugänglich gemacht.
- Zum Ver- bzw. Entschlüsseln werden immer beide Schlüssel benötigt (s. nächste Folie).

Mögliche Varianten der asymmetrischen Verschlüsselung



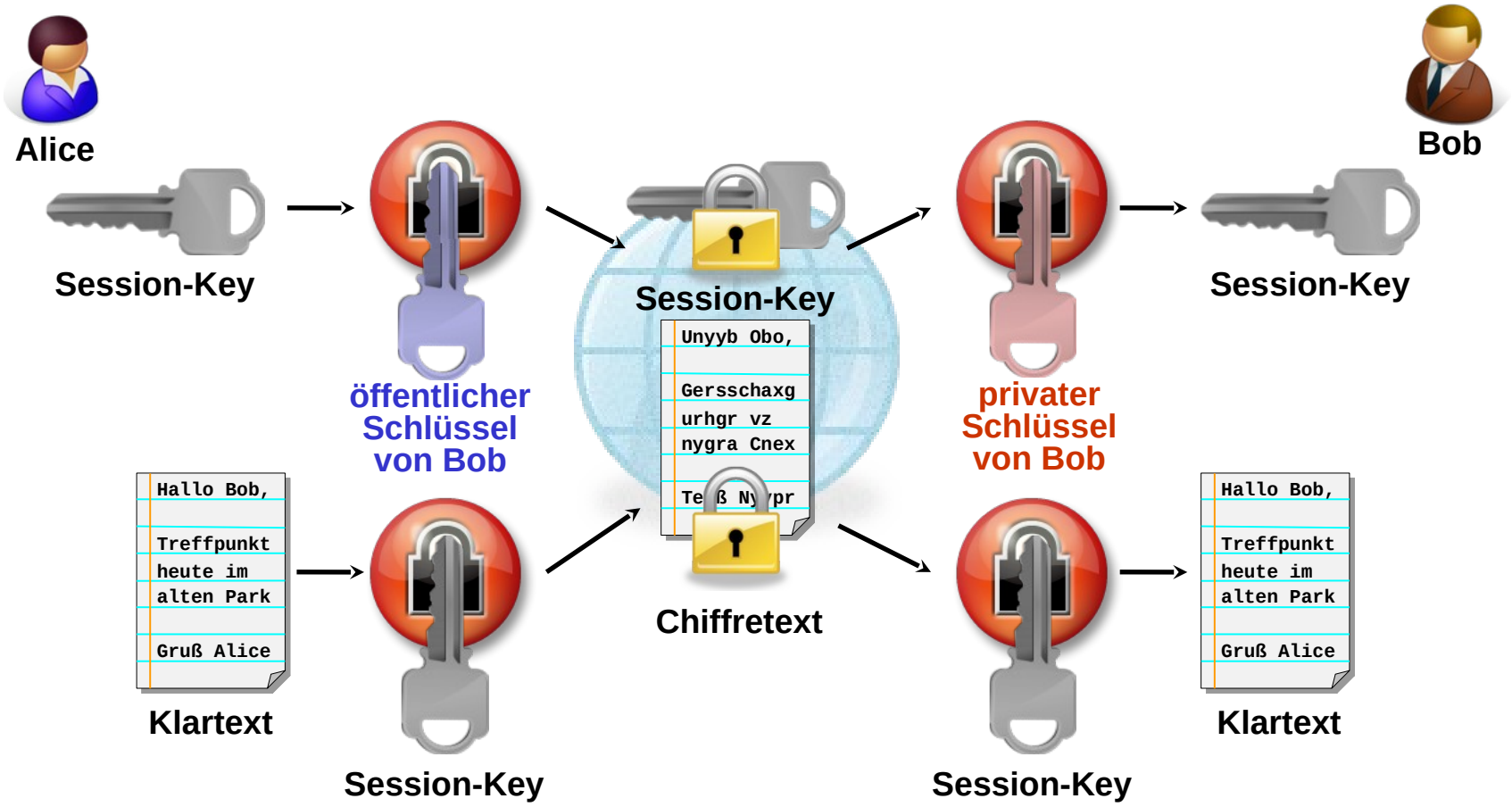
Vor- und Nachteile asymmetrischer Verschlüsselungsverfahren

+ privater Schlüssel wird nicht übertragen und verbleibt beim Besitzer
+ Schlüsselzahl nimmt linear mit Teilnehmerzahl zu
+ spontane Kontaktaufnahme möglich
- hoher Rechenleistung erforderlich (ca. 10.000x langsamer als symmetrische Verfahren) für große Datenmengen ungeeignet
- erhöhter Aufwand bei mehreren Empfängern, da bei Privacy der jeweilige Public-Key des Empfängers benutzt wird
- basiert auf unbewiesenen Annahmen: kein effektives mathematisches Verfahren zur Faktorisierung, evtl. sind die benutzten Einwegfunktionen umkehrbar große Schlüssellänge mind. 1024 Bit
- keine Sicherheit gegen Man-in-the-Middle-Angriffe (s. später)

Hybride Verfahren (1)

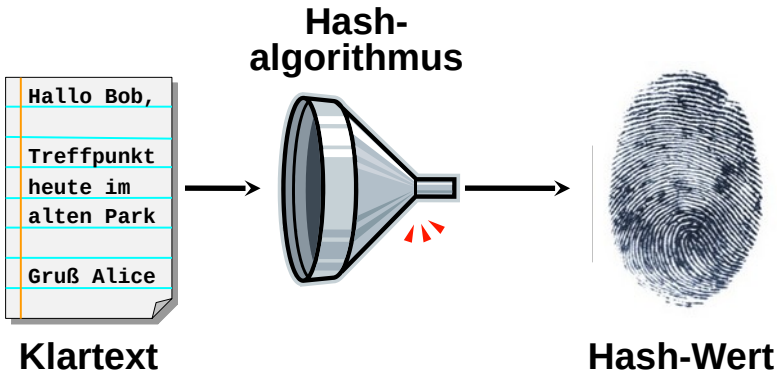
- Kombination aus symmetrischer und asymmetrischer Verschlüsselung
- Der Sender erzeugt einen zufälligen Schlüssel (auch Session-Key genannt) für den symmetrischen (schnellen) Algorithmus (z.B. AES), mit dem die eigentliche Nachricht verschlüsselt wird.
- Der benutzte Zufallsschlüssels des symmetrischen Verfahrens wird mit dem Public-Key des Empfängers asymmetrisch verschlüsselt (geht zwar lang, der Schlüssel ist aber ja verhältnismäßig klein) und zusammen mit der symmetrisch verschlüsselten Nachricht zum Empfänger geschickt.
- Der Empfänger entschlüsselt mit seinen Private-Key zunächst den vom Sender benutzten Zufallsschlüssel und kann dann damit die eigentliche Nachricht entschlüsseln.

Hybride Verfahren (2)



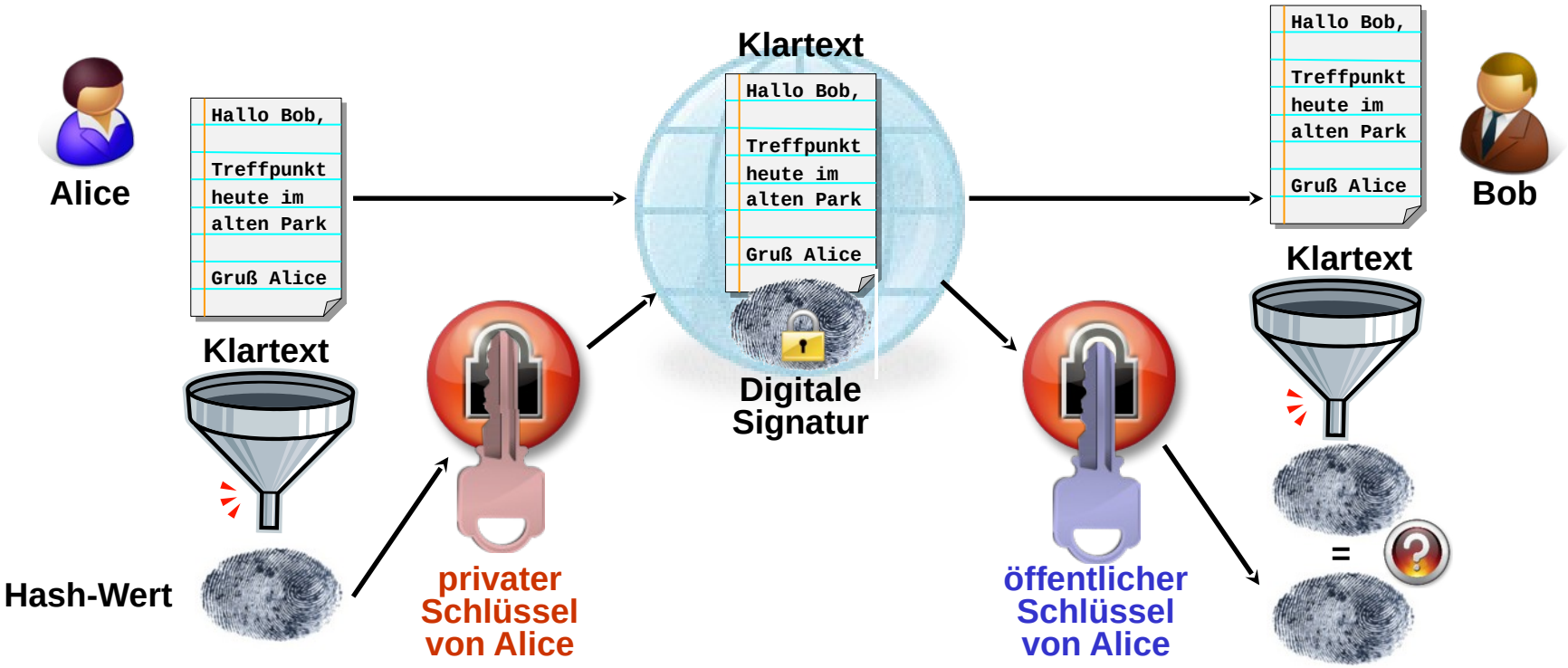
Hash-Funktionen

- Hash-Funktionen (z.B. SHA-1, MD5) sind mathematische Einwegfunktionen, die aus einem beliebigen Klartext eine Prüfsumme (Hash-Wert, Fingerprint, Message-Digest) fester Länge erzeugen.
- Anforderungen an Hash-Funktionen:
  - Kleinste Änderungen am Klartext müssen zu anderen Hash-Werten führen (kollisionsresistent).
  - Der ursprüngliche Klartext darf aus dem Hash-Wert nicht berechenbar sein.

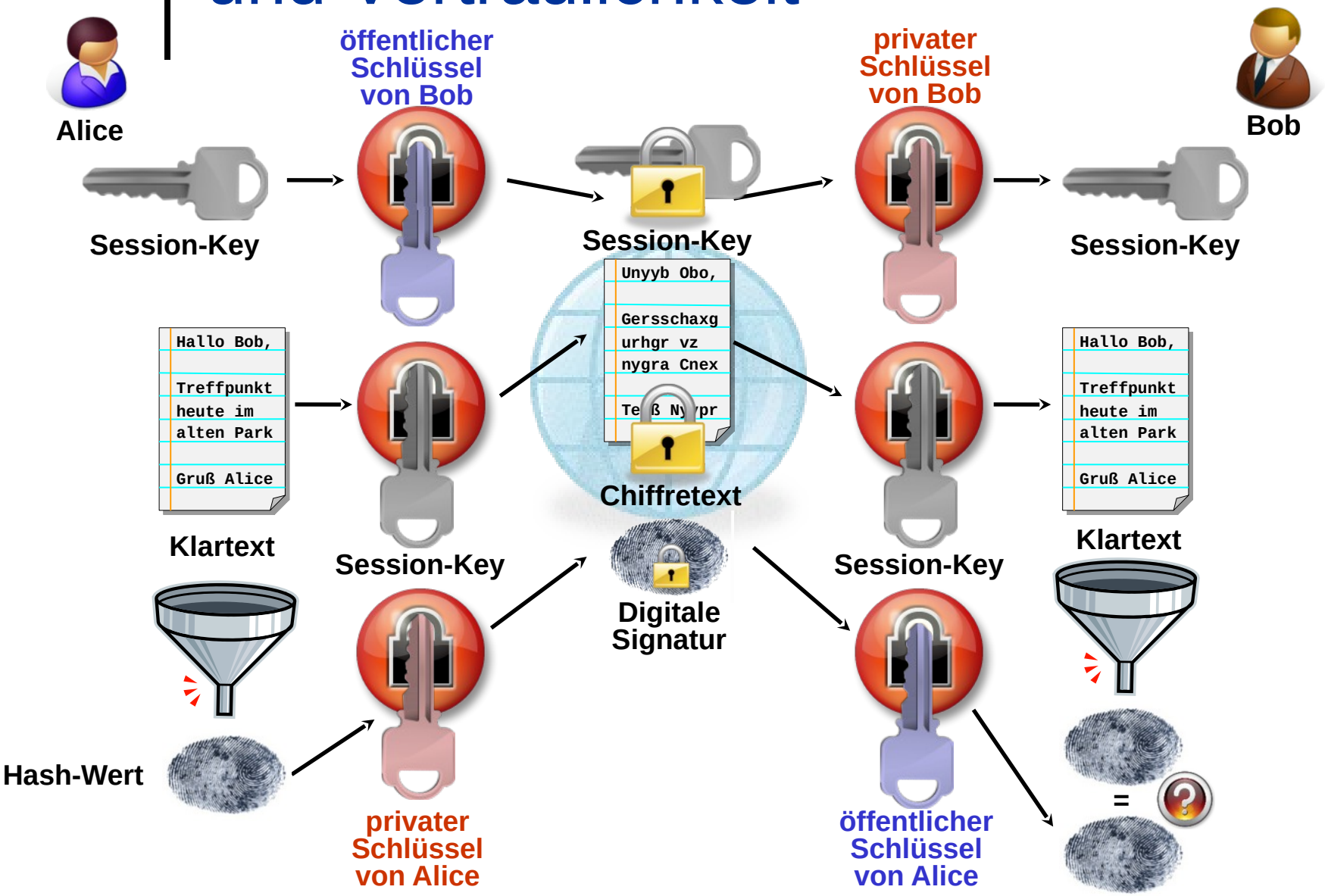


Digitale Signatur

- Hash-Wert des Klartextes wird mit Private-Key des Senders verschlüsselt und zusammen mit Nachricht (hier unverschlüsselt) zum Empfänger übertragen.
- Empfänger bildet eigenen Hash-Wert und überprüft, ob entschlüsselter Hash-Wert und eigener Hash-Wert übereinstimmen.



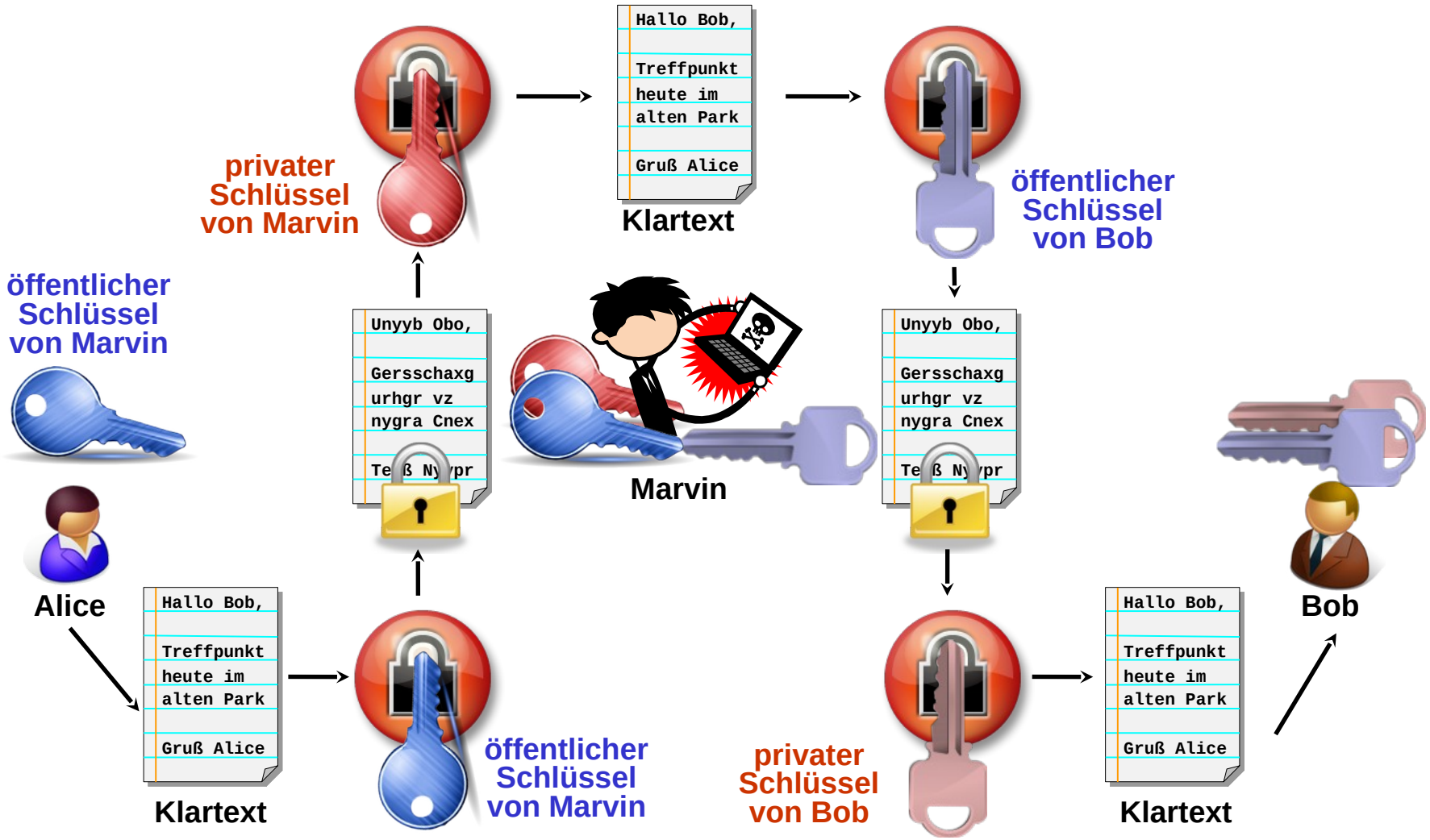
Authentifizierung, Integritätscheck und Vertraulichkeit



So war es eigentlich gedacht!

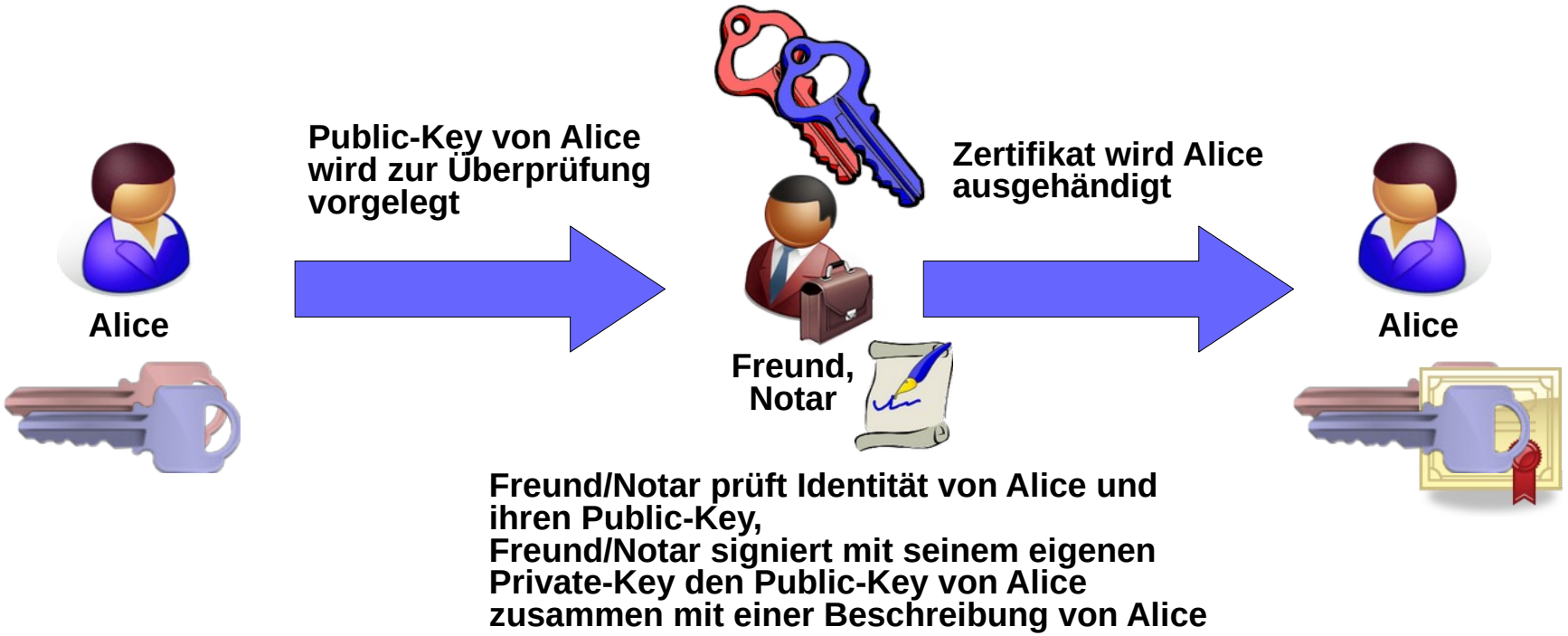
- Alice besorgt sich den öffentlichen Schlüssel von Bob.
- Alice verschlüsselt mit dem öffentlichen Schlüssel von Bob ihre Nachricht.
- Nur Bob kann mit seinem privaten Schlüssel die Nachricht entschlüsseln.

Aber es könnte schlimmsten Falls so aussehen: Man-in-the-Middle



Vertrauensbildung mit Hilfe von Zertifikaten

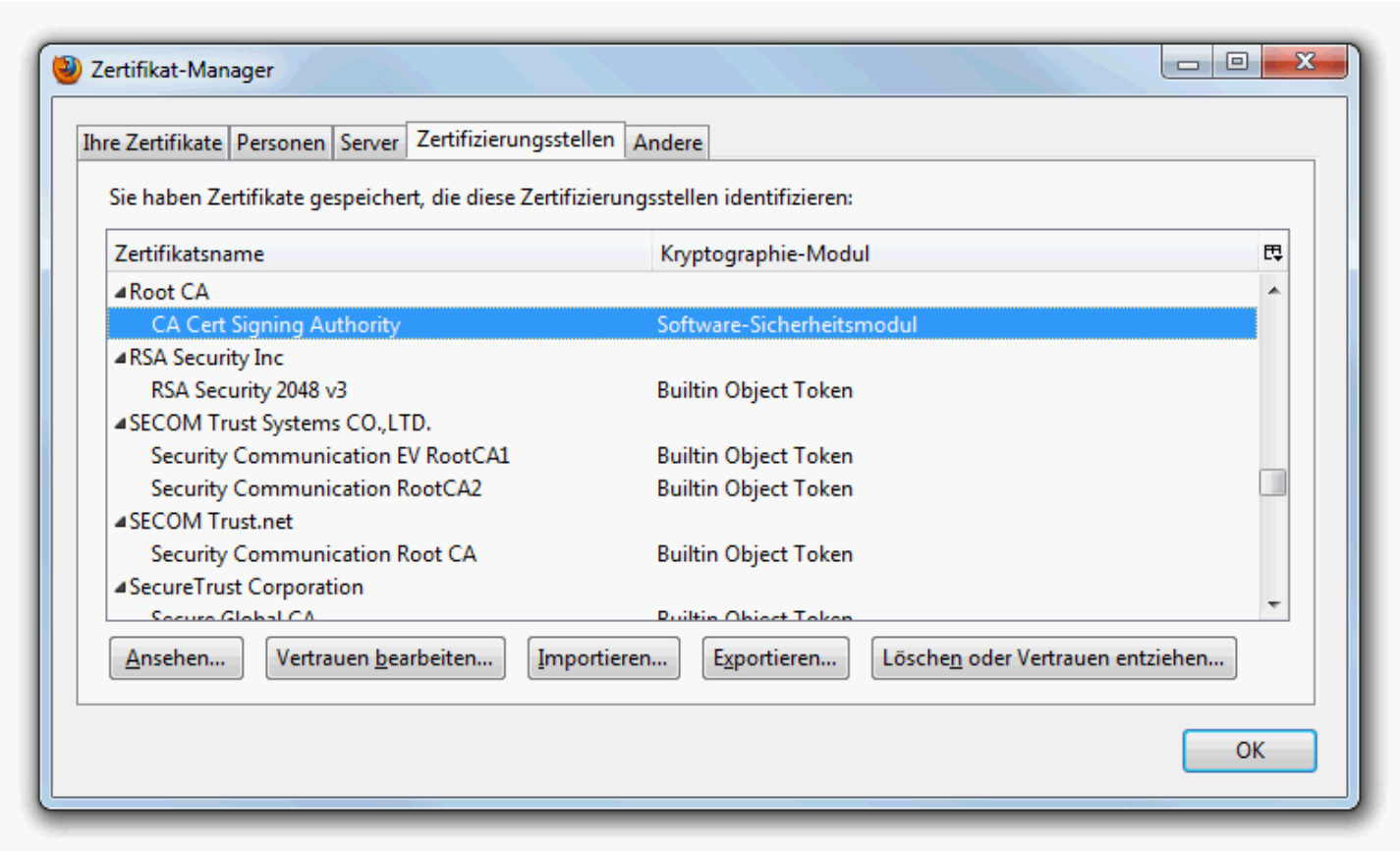
- Ein Zertifikat entsteht, wenn der Public-Key einer Person durch die digitale Signatur einer anderen Person (Freund/Notar) bestätigt wird.



Certification Authority (CA), das digitale Notariat

- CA = zentrale vertrauenswürdige Instanz zur Erstellung/Vergabe von Zertifikaten (z.B. VeriSign Inc.)
- CAs zertifizieren sich auch gegenseitig Cross-Zertifizierung
- in den meisten Ländern durch Signaturgesetze geregelt
- sinnvolle Voraussetzung: CA-Public-Keys sollten in den Applikationen bereits vorinstalliert sein

Beispiel:
CA-Zertifikate im Firefox



Public-Key-Infrastruktur

- Organisationen können eigene Zertifizierungshierarchien einrichten:
  PKI (Public Key Infrastucture) sorgt für die Verwaltung der Public-Key-Zertifikate:
  - Zertifizierungsstellen werden geschaffen und Hierarchien werden festgelegt
  - Policies regeln, auf welche Zertifikate in welchem Maß vertraut werden kann
  - Revocation-Listen erklären Zertifikate für ungültig
  - …

X.509 Zertifikate

- ITU-T-Standard für PKI-Zertifikate, aktuell X.509v3
- für den Internet-Bereich mit RFC 5280 spezifiziert
- Öffnet standardisierten Anwendungen die Tür
  - Secure Socket Layer (SSL)
  - Transport Layer Security (TLS)
  - S/MIME (quasi Nachfolgerf v. PGP, GnuPG bei Mail)
  - …
- Regelt beispielsweise, welche Klartextdaten in einem Zertifikat zusammen mit dem Public-Key enthalten sein müssen!
- Weitere Regelungen zu PKIs und Key-Revocation

Beispiel eines X.509-Zertifikats