

- Asymmetrische Verschlüsselung soll das Problem des Schlüsselstauschs lösen
- Aber: Das Verfahren ist anfällig für Man-in-the-Middle-Angriffe
 - Problem: Es fehlt ein “Echtheitsnachweis” für Public Keys

- Welchen Nutzen hat es, wenn Alice eine Nachricht mit ihrem eigenen, privaten Schlüssel **verschlüsselt**
 - Jede(r) kann die Nachricht mit dem zugehörigen öffentlichen Schlüssel von Alice entschlüsseln
- Echtheitsnachweis:
 - Lässt sich die Nachricht mit Alice' öffentlichem Schlüssel entschlüsseln, so wurde sie garantiert mit dem privaten Schlüssel von Alice verschlüsselt
 - Da (hoffentlich) nur Alice im Besitz ihres privaten Schlüssels ist, muss die Nachricht von ihr stammen

- Bringt uns das was für unser Man-in-the-Middle-Problem?
 - Um die Echtheit einer Nachricht von Alice zu verifizieren, braucht man bereits ihren korrekten öffentlichen Schlüssel
 - Um sicher zu sein, dass man den echten öffentlichen Schlüssel bekommen hat, müsste man die Nachricht von Alice verifizieren können
- Was tun?
 1. Zertifikate/Public-Key-Infrastruktur
 2. Web of Trust

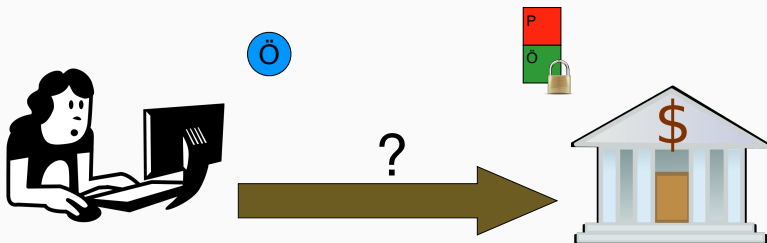
Zertifikate

- Sogenannte **Certification Authorities** (CAs) “garantieren” für die Echtheit von Schlüsseln
 - Man kann sich dort (meist gegen Geld) ein sogenanntes Zertifikat ausstellen lassen
- Zertifikat:
 - Öffentlicher Schlüssel einer Person oder Institution zusammen mit dem Namen, der URL oder anderen zugehörigen Informationen
 - Verschlüsselt mit dem privaten Schlüssel der CA, also nur mit deren öffentlichem Schlüssel entschlüsselbar

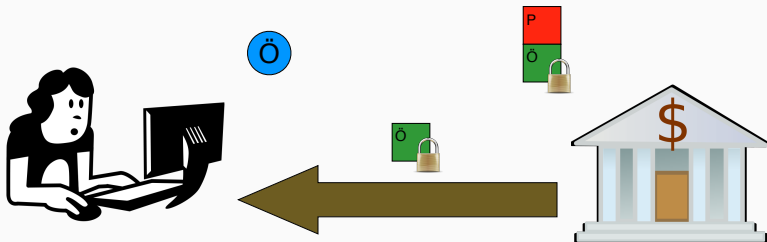
- Besteht nicht wieder das gleiche Henne-Ei-Problem?
 - Woher bekommt man den öffentlichen Schlüssel der CA?
- Betriebssysteme, Browser und dergleichen werden mit den öffentlichen Schlüsseln vieler CAs ausgeliefert (sogenannte Root-Zertifikate)



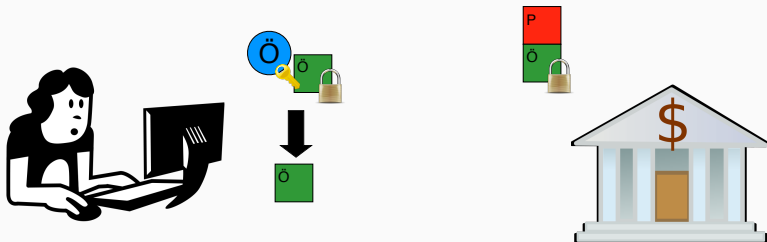
1.
Der Nutzer kennt nur den öffentlichen Schlüssel der CA.



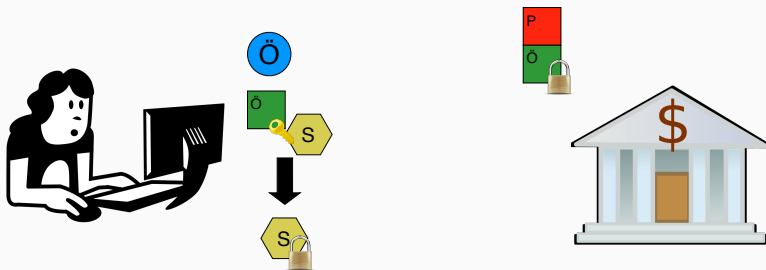
2.
Der Nutzer fragt die Bank (oder CA) nach dem Zertifikat der Bank.



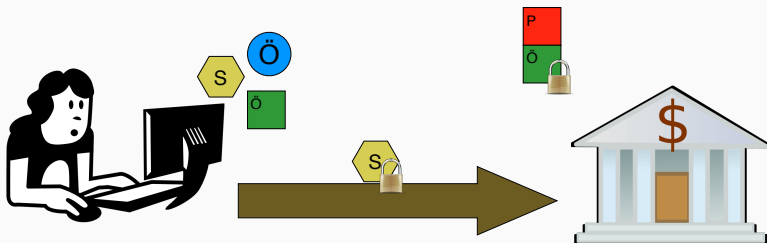
3.
Die Bank schickt das Zertifikat.



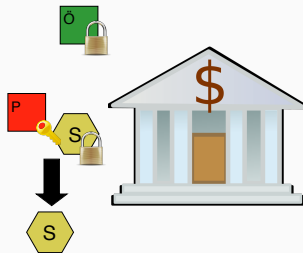
4.
Der Nutzer entschlüsselt das Zertifikat mit dem öffentlichen Schlüssel der CA.



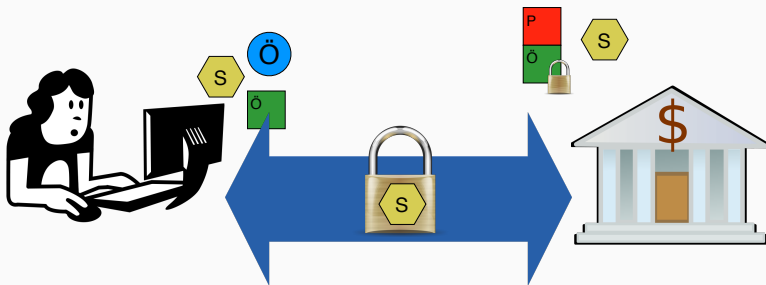
5.
Der Nutzer erzeugt einen symmetrischen Schlüssel
und verschlüsselt diesen mit dem öffentlichen
Schlüssel der Bank.



6.
Der Nutzer schickt der Bank den symmetrischen Schlüssel.



7.
Die Bank entschlüsselt den symmetrischen Schlüssel
mit ihrem privaten Schlüssel.



8.
Die weitere Kommunikation in beide Richtungen kann
mit dem symmetrischen Schlüssel verschlüsselt
werden.

- Leider nicht:
 - Vortrag
 - Liste

Web of Trust

- Erarbeitet jeweils im Zweierteam die Funktionsweise eines “Web of Trust”
- Erstellt eine kurze (!) Präsentation (vier bis fünf Folien)