



Trust Problem

- Sicherheit der Anwendung von 2-Schlüsselverfahren hängt ganz wesentlich von **richtiger Zuordnung** der öffentlichen Schlüssel zu den Teilnehmern ab
- Gelingt es Angreifer, seinen öffentlichen Schlüssel für den eines Teilnehmers auszugeben, dann kann
 - Angreifer alle an den eigentlichen Adressaten verschlüsselt zugesandten Nachrichten entschlüsseln und lesen (dem eigentlichen Adressaten ist das nicht mehr möglich)
 - Angreifer Nachrichten im Namen des Adressaten signieren
- Die sichere und vertrauenswürdige Zuordnung von öffentlichen Schlüsseln zu ihren Besitzern werden über **Zertifikate** hergestellt

- Bei Aufbau einer HTTPS Verbindung ist es erforderlich, die Identität des Kommunikationspartners (Internetdienst) mit Hilfe von Zertifikaten zu überprüfen
 - Geschieht dies nicht, kann ein Man-in-the-Middle Angriff durchgeführt werden, bei dem sich der Angreifer als legitimer Internetdienst ausgibt
- Besonders wichtig ist Überprüfung des Kommunikationspartners bei kritischen Internetdiensten
 - Bankseiten (Online-Banking)
 - Buchungsportalen
 - Email Portalen
 - ...

Zertifikat ist ein von einem vertrauenswürdigen Dritten („**Trust Center**“) signiertes Dokument, in dem der Zusammenhang zwischen einer Person/ Entität und deren öffentlichen Schlüssel bezeugt wird

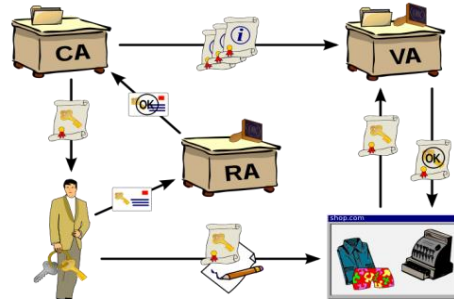
- Vertraut man Trust Center, das ein Zertifikat signiert hat, dann kann man sich auf die im Zertifikat bezeugte Zuordnung des öffentlichen Schlüssels zu seinem Inhaber verlassen
- Zertifikate enthalten Informationen über
 - Inhaber des Zertifikats (Person, Firma, Webserver, ...),
 - dessen öffentlichen Schlüssel und
 - digitale Signatur des Trust Centers, das Zertifikat ausgestellt hat
- Trust Center, das Zertifikat signiert, garantiert Richtigkeit der Angaben

- Mit Hilfe von Zertifikaten können Nutzer authentifiziert werden:
 - Nutzer sendet eine von ihm signierte Nachricht zusammen mit seinem Zertifikat an einen Partner/ Dienst
 - Partner/ Dienst validiert zunächst Signatur des Zertifikats und prüft so dessen Echtheit
 - Partner/ Dienst überprüft (entschlüsselt) mit öffentlichem Schlüssel aus dem Zertifikat die Signatur der vom Nutzer gesendeten Nachricht
- Kann Signatur des Nutzers verifiziert werden (d.h. ist Entschlüsselung möglich), ist sichergestellt, dass Nachricht wirklich vom behaupteten Absender kommt

- Um 2-Schlüssel Verschlüsselung sicher anwenden und Trust Problem mit Hilfe von Zertifikaten lösen zu können, braucht es eine komplette Infrastruktur
→ „**Public-Key Infrastruktur – PKI**“
- PKI umfasst Software- und Hardwarekomponenten sowie Personal, um Bereitstellung, Verteilung, Verwendung, Annullierung von Zertifikaten zu regeln
- Im Zentrum einer PKI steht das **Trust Center** mit den Komponenten
 - Registrierungsstelle – Registration Authority
 - Zertifizierungsstelle – Certification Authority
 - Validierungsstelle – Validation Authority

Public Key Infrastruktur – PKI Beantragung eines Zertifikates

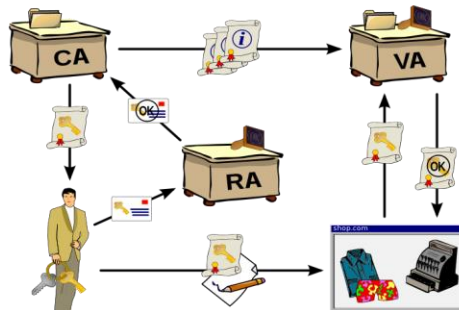
1. Nutzer weist bei Registrierungsstelle RA seine Identität nach und reicht seinen öffentlichen Schlüssel ein
2. RA übergibt Anmeldedaten – Identitätsdaten, öffentlicher Schlüssel – an Zertifizierungsstelle CA
3. Zertifizierungsstelle CA erstellt und signiert Zertifikat für Nutzer und schickt es dem Nutzer
4. Zertifikatsinformationen werden bei Validierungsdienst VA hinterlegt



<http://de.wikipedia.org/wiki/Datei:Public-Key-Infrastructure.svg>

Public Key Infrastruktur – PKI Anwendung des Zertifikates

1. Nutzer schickt Zertifikat an Kommunikationspartner
2. Der Kommunikationspartner validiert Zertifikat mit Hilfe des Validierungsdienstes VA
3. Der VA überprüft Zertifikat anhand der gespeicherten Informationen und bestätigt Gültigkeit

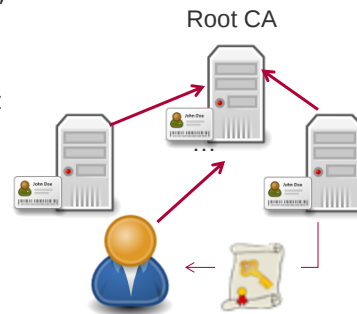


<http://de.wikipedia.org/wiki/Datei:Public-Key-Infrastructure.svg>

Lösung des Trust Problems: Hierarchische PKI

Typischerweise ist eine PKI hierarchisch organisiert:

- Hierarchische PKI haben initiale CA-Instanz „**Root CA**“, der alle untergeordneten Instanzen (CAs) vertrauen. Root CA signiert Zertifikate der untergeordneten CAs
- Will Nutzer Identität einer CA prüfen, validiert er deren von der Root CA signiertes Zertifikat
- Da Nutzer Root CA vertraut, vertraut er deren Signatur und somit dem Zertifikat



Hierarchische PKI in der Praxis

TLS/SSL basierte Verbindungen basieren auf hierarchischer PKI

- „Root CA“ Zertifikate sind im Browser bzw. Betriebssystem hinterlegt

Beispiel: Aufbau einer HTTPS basierten Verbindung zur Sparkasse

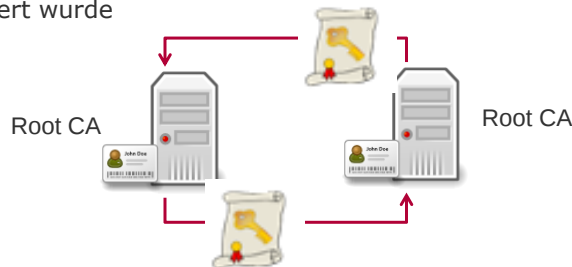
- Überprüfung der Signatur des Zertifikats auf www.sparkasse.de mit Hilfe von übergeordnetem Zertifikat (Symantec)
- Signatur des Symantec Zertifikats wird mit Hilfe des bereits hinterlegten und vertrauten Root CA Zertifikats (VeriSign) überprüft
- Damit kann Vertrauenskette bis zum Zertifikat der Sparkasse hergestellt werden

Zertifikatshierarchie

▲ VeriSign Class 3 Public Primary Certification Authority - G5
▲ Symantec Class 3 Secure Server CA - G4 www.sparkasse.de

Lösung des Trust Problems: Cross-Zertifizierung

- Verschiedene PKIs können über eine **Cross-Zertifizierung** mit einander verknüpft werden
- Dabei stellen sich die Root CAs der beiden PKIs gegenseitig Zertifikate aus und signieren diese
- Somit vertrauen die Instanzen der einen Seite denen der anderen, da deren Zertifikat von ihrer eigenen Root CA signiert wurde



Lösung des Trust Problems: Web of Trust

- Nutzer lässt sein Zertifikat von vielen anderen Nutzern signieren bzw. signiert viele Zertifikate anderer Nutzer
- Je mehr Nutzer sein Zertifikat signiert haben, desto vertrauenswürdiger ist sein Zertifikat
- Wenn Nutzer A Nutzer B vertraut und das Zertifikat von C von Nutzer B signiert wurde, kann A auch Zertifikat von C vertrauen

