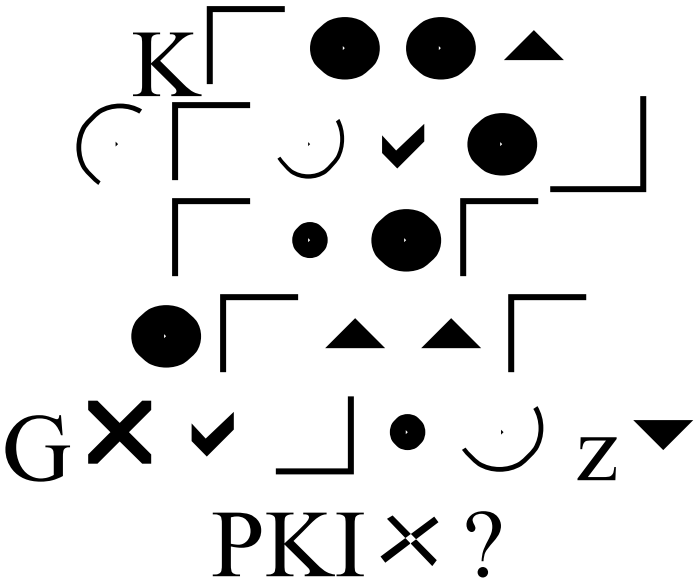
PKI – Was soll das?



LugBE 23. März 2006
Markus Wernig

- Einleitung
- Symmetrisch vs. asymmetrisch
- Trusted Third Party
- Hierarchisches Modell
- Web of Trust
- Links

Einleitung

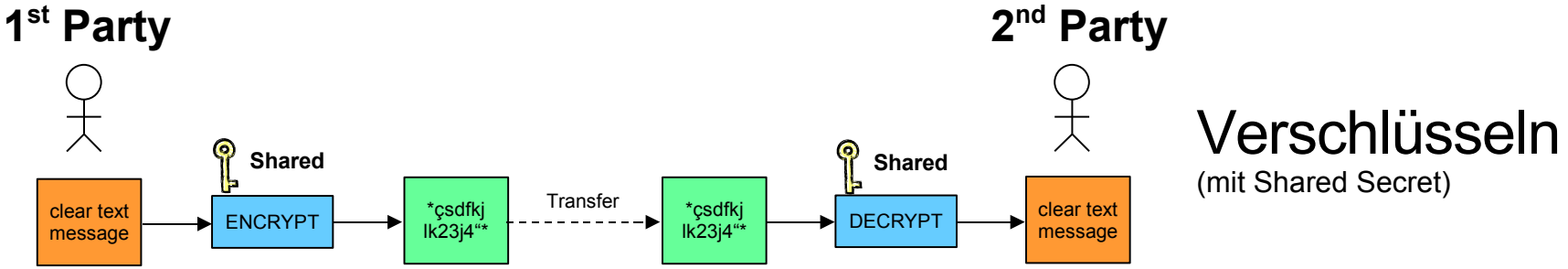
PKI (Public Key Infrastructure) sind kryptografische Systeme, die die Ausstellung, Verteilung und Prüfung von digitalen Identitätsausweisen ermöglichen.

CA (Certificate Authority) sind Hilfsdienste einer PKI, die die Authentizität von digitalen Identitätsausweisen bescheinigen.

PKI sind Software, umgeben von einer strikten Regelkette von Prozessen.

Symmetrisch vs. asymmetrisch

„Symmetrische“ Verschlüsselungsverfahren verwenden auf beiden Seiten der Leitung den selben Schlüssel. Gesamtzahl der Schlüssel: 1

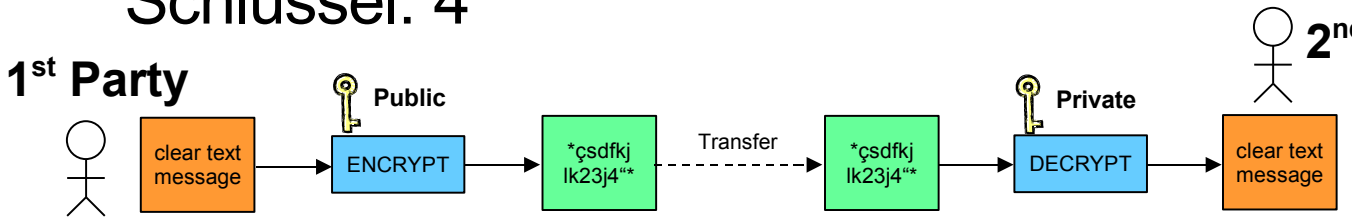


Verschlüsseln
(mit Shared Secret)

Problem: Schlüsselaustausch, Authentizität
Beispiele: 3DES, AES, Blowfish

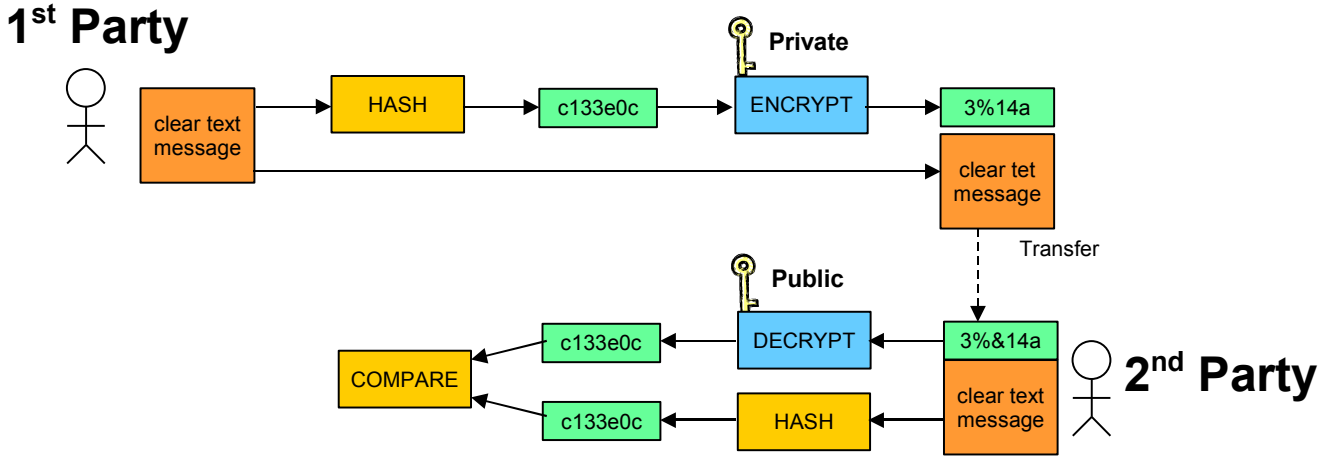
Symmetrisch vs. asymmetrisch

„Asymmetrische“ Verfahren verwenden auf jeder Seite je einen öffentlichen und einen geheimen Schlüssel. Gesamtzahl der Schlüssel: 4



Verschlüsseln

(mit Public Key des Partners)



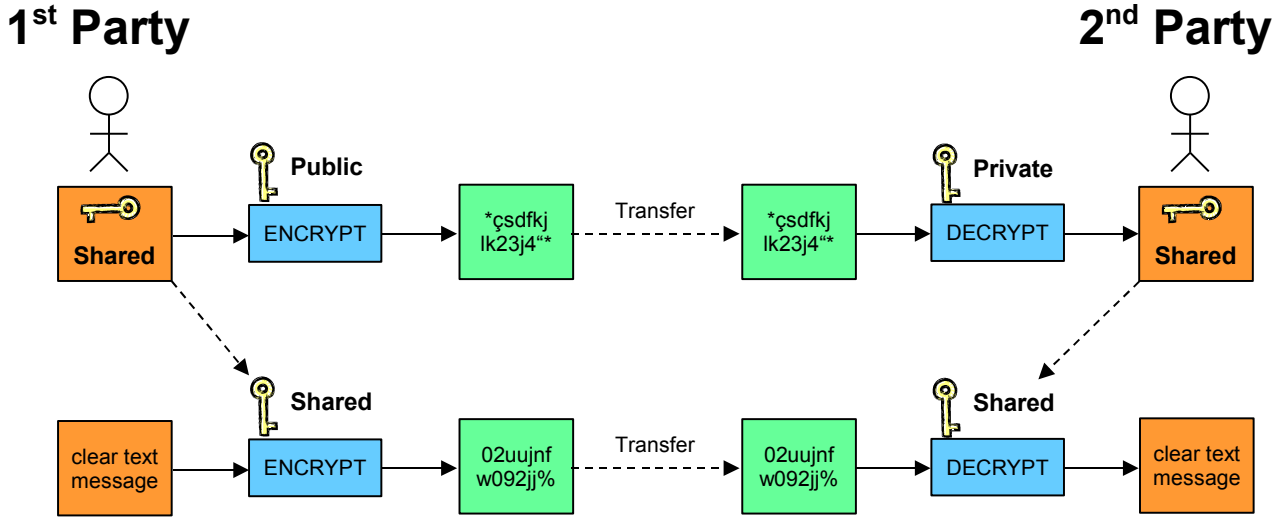
Signieren

(= Verschlüsseln mit eigenem Private Key)

Problem: Authentizität, Performance
Beispiele: RSA

Symmetrisch vs. asymmetrisch

„Hybrides“ Verfahren: Schlüsselaustausch und -verhandlung asymmetrisch, Verschlüsselung selbst symmetrisch.



„Key Exchange“, „Phase 1“
Asymmetrisch

„Encryption“, „Phase 2“
Symmetrisch

Es bleibt das Problem: Authentizität.
Wie stelle ich sicher, dass der öffentliche Schlüssel wirklich zu dem Partner gehört, mit dem ich kommunizieren will?

Trusted Third Party

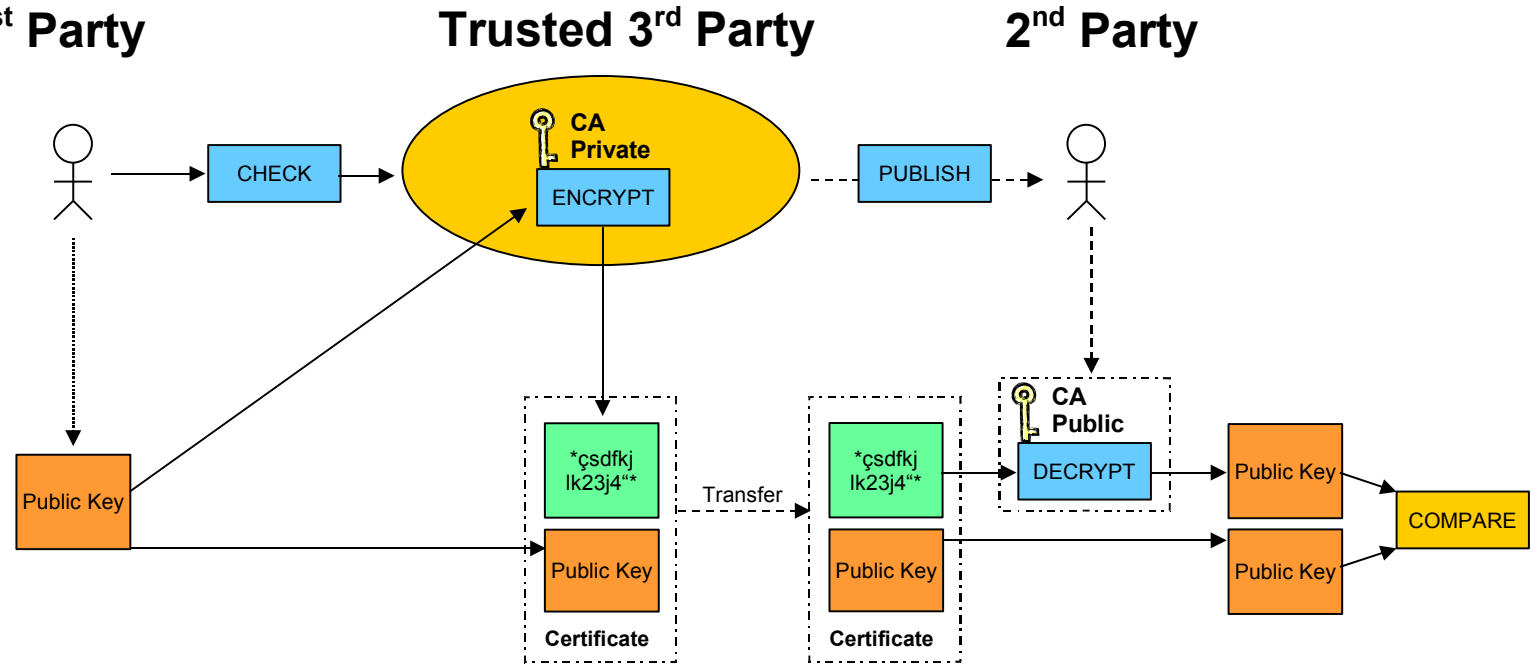
Die Lösung: Beide Seiten vertrauen einer „Trusted Third Party“, die bestätigt, dass der Schlüssel wirklich demjenigen gehört, auf den er ausgestellt ist.

Die wichtigste Eigenschaft einer solchen 3rd Party ist, dass sie gewissenhaft die Identität des Schlüsseleigners überprüft.

Trusted Third Party

Die „Bestätigung“ erfolgt mittels einer digitalen Signatur, d.h. Verschlüsselung mit dem 3rd Party Private Key. Dieser Key muss absolut sicher sein! Gesamtzahl der Schlüssel: 6

Die signierten Public Keys enthalten die Angaben, die von der 3rd Party überprüft wurden (E-Mail-Adresse, Host-/Domainname ...)



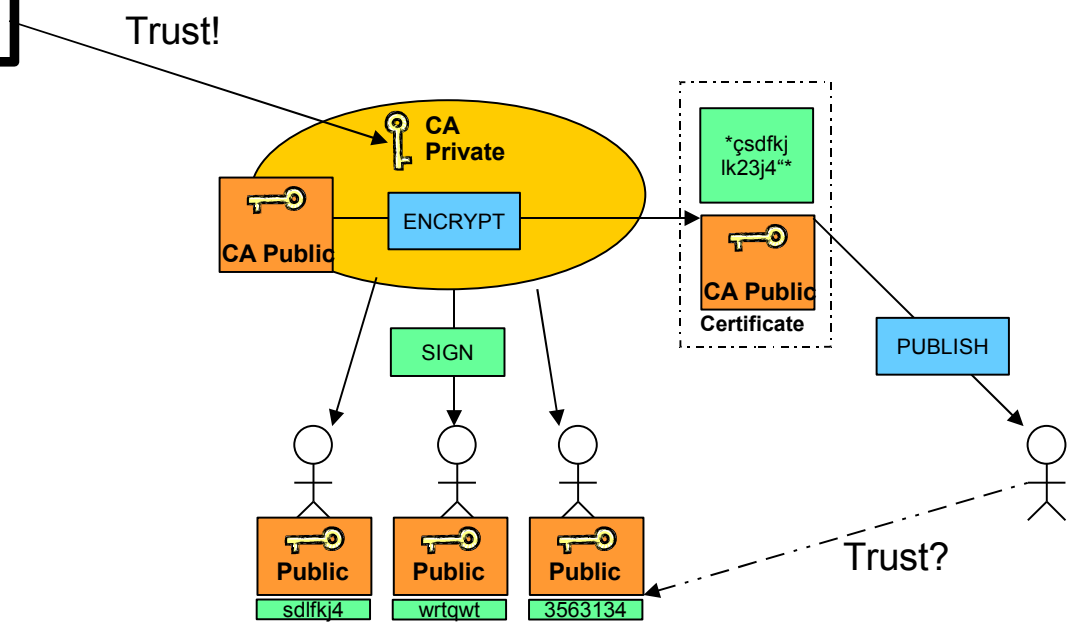
Hierarchisches Modell

Trusted 3rd Parties nehmen also eine zentrale Rolle in PKIs ein.
Wie aber wird ihre eigene Legitimität sichergestellt?

Das Hierarchische Modell (z.B. x.509: Verisign etc.):
Wird legitimiert per Dekret. Signiert eigenen Public Key.

Authority

Die Mutter aller Zertifikate

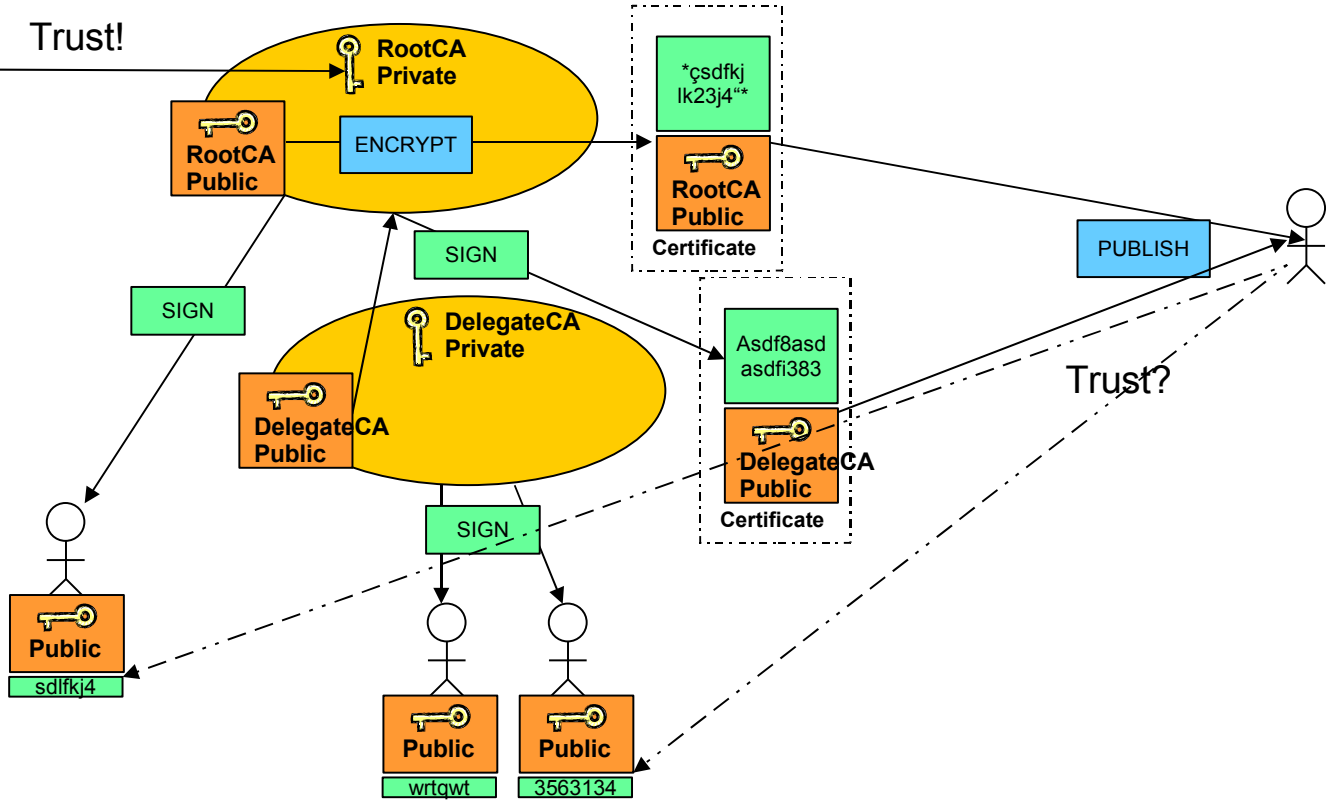


Hierarchisches Modell

CAs können die Public Keys anderer CAs signieren. Die dabei entstehende Kette nennt man „Trust Chain“. Die Kette endet bei der obersten, der Root CA.

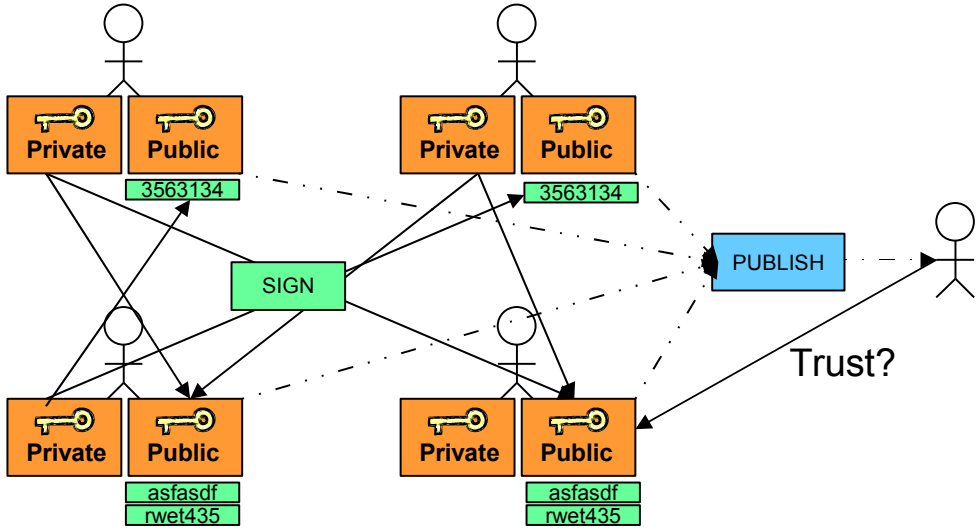
Authority

Die Mutter aller Zertifikate



Web of Trust

Web of Trust (z.B. PGP)
Im Web of Trust ist jeder Teilnehmer eine CA oder Trusted 3rd Party.
Wird legitimiert durch die Anzahl Signaturen. Public Key durch andere Teilnehmer signiert.



Links

Lust auf mehr?

http://cacert.org
http://openssl.org
http://lugbe.ch/projects/wot/
http://www.nissle.ch/ssl/PKI-OpenSSL.pdf

http://www.google.ch/search?q=PKI+howto
http://de.wikipedia.org/wiki/PKI