

Netzicherheit – Architekturen und Protokolle Grundlagen PKI/PMI



- 1 Motivation
- 2 Digitale Zertifikate
- 3 Infrastrukturen
- 4 PKI (Bausteine)
- 5 Vertrauensmodelle



Wiederholung Kryptographie

- **Symmetrische Kryptographie**
 - 1 Schlüssel für Ver- und Entschlüsselung
 - Schlüssel muss vor Kommunikation ausgetauscht werden
 - Schlüssel muss geheim gehalten werden
 - Schlüsselanzahl wächst quadratisch mit Anzahl der Kommunikationsteilnehmer
- **Asymmetrische Kryptographie**
 - Zwei zueinander inverse Schlüssel
 - Öffentlicher Schlüssel ist nicht geheim
 - Schlüsselanzahl wächst linear

1



Diskussion

Welches **neue** Problem hat man mit
asymmetrischer Kryptographie?

2



Motivation: Authentifizierung

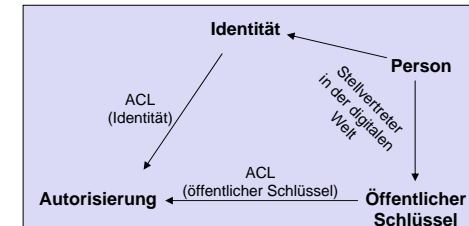
- **Frage:** woher bekommt man öffentlichen Schlüssel?
 - manueller Austausch?
 - via eMail oder Web-Site?
 - *Sichere Zuordnung Schlüssel/Kommunikationspartner?*
- Lösungsvorschlag: öffentliches Verzeichnis
 - Zuordnung: Name zu öffentlichem Schlüssel (ähnlich Telefonbuch)
 - Antworten auf Anfragen symmetrisch geschützt
 - **Probleme des Ansatz?**
- **Wie erreicht man unabhängige, transportierbare Bindung von Authentifizierungsdaten? → PKI!**

3

- Whitfield Diffie and Martin Hellman: "New Directions in Cryptography", IEEE Transactions on Information Theory, November 1976, pp. 644-654]
 - "Given a system of this kind, the problem of **key distribution** is vastly simplified. Each user generates a pair of inverse transformations, E and D, at his terminal. The deciphering transformation, D, **must be kept secret** but need never be communicated on any channel. The enciphering key, E, can be **made public** by placing it in a **public directory** along with the user's name and address. Anyone can then encrypt messages and send them to the user, but no one else can decipher messages intended for him."
- Loren Kohnfelder, "Towards a Practical Public-key Cryptosystem", 1978
 - Introduction of Certificates

4

- Autorisierung über Zugangskontrolllisten (*Access-Control-List*)
 - der via Passwort/Ticket/PKK verifizierten Identität
 - des via Signatur (mit privatem Schlüssel) bestätigten öffentlichen Schlüssels



Problem: Zuordnung von Privilegien zu Personen lokal oder zentral gespeichert

Wie erreicht man eine unabhängige, transportierbare Bindung von Autorisationsdaten? → PMI!

5

Netzicherheit – Architekturen und Protokolle Grundlagen PKI/PMI



- 1 Motivation
- 2 Digitale Zertifikate
- 3 Infrastrukturen
- 4 PKI (Bausteine)
- 5 Vertrauensmodelle



Problemstellung

- Authentifizierung eines Sachverhaltes, den man nicht selbst überprüfen kann
- man verlässt sich auf vertrauenswürdige Dritte, die ihn schon kontrolliert haben

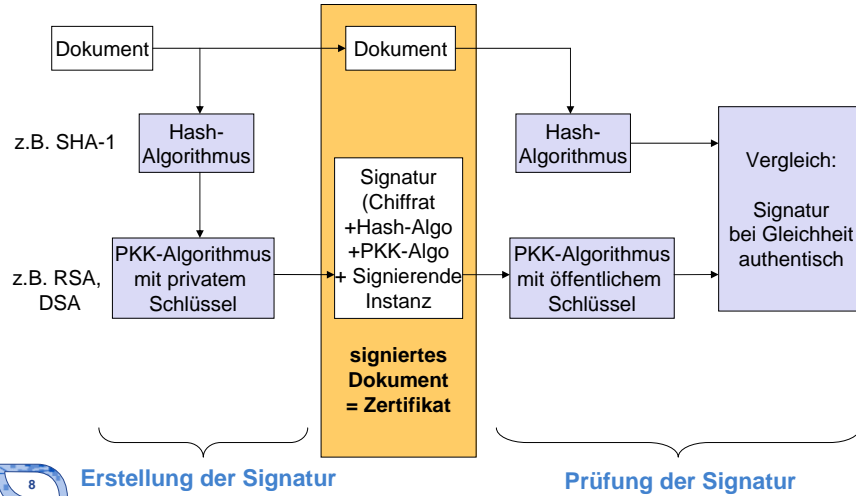
Frage: was ist ein Zertifikat?

- ein digitales Dokument, in dem eine Instanz einen bestimmten Sachverhalt mittels digitaler Signatur bestätigt
- erzeugt Vertrauen in den Sachverhalt

Frage: wer erstellt die Zertifikate?

- eine **vertrauenswürdige** Instanz: **Certification Authority**

7



8

Erstellung der Signatur

Prüfung der Signatur

- Klassen von Zertifikaten
 - ID-Zertifikate
 - ▶ öffentlicher Schlüssel → eindeutiger Name (*Identität*)
 - ▶ Authentifikation von öffentlichen Schlüsseln
 - Attributzertifikate
 - ▶ Attributswerte → Identität
 - ▶ Autorisation zur Nutzung von Diensten
 - Autorisierungszertifikate
 - ▶ binden Privilegien → öffentlichen Schlüssel
 - ▶ Autorisation zur Nutzung von Diensten
- Zertifikate ersetzen zentrale globale Listen
 - öffentliches Verzeichnis mit (ID, öffentlicher Schlüssel) durch ID-Zertifikat
 - ACL auf ID-Basis durch Attributzertifikate
 - ACL auf Basis des öffentlichen Schlüssels durch Autorisierungszertifikate

9

Welche Zertifikate aus der realen Welt passen in welche Klasse?

10

- Problem bei dezentraler Speicherung: **Konsistenz**
- CAP-Prinzip: 2 der 3 Punkte sind bei verteilten Anwendungen realisierbar
 - C: **strong consistency**
 - ▶ Konsistenz der verteilten Daten
 - A: **high availability**
 - ▶ Hohe Verfügbarkeit der Daten
 - P: **partition-resilience**
 - ▶ Ausfallsicherheit bei Netzwerkpartitionierung
- Beispiele? In welche Klasse fallen Zertifikate?

11

Problem

Zertifikate können ungültig werden, wenn die Informationen im Zertifikat nicht mehr zutreffen (z.B. ID stimmt nicht mehr, Privileg wird entzogen)

Lösungen

- Gültigkeitsdauer
- Offline-Prüfung durch Widerrufslisten (*certificate revocation list* – CRL)
- Online-Prüfung (in welche CAP-Klasse fallen Zertifikate dann?)

12

- **Validierung** eines Zertifikates
 - syntaktische und semantische Prüfung seiner Gültigkeit
- **Vorraussetzung** für den Validierenden
 - vertraut einer Menge von CAs
 - ist im Besitz der Zertifikate dieser CAs
 - hat die Integrität und Authentizität dieser Zertifikate geprüft
- **Ablauf:** der Prüfende verifiziert, ob das zu prüfende Zertifikat
 - zeitlich noch gültig ist
 - widerrufen wurde
 - alle Parameter für die Anwendung gültig sind (z.B. Sicherheitsrichtlinie)
 - aufgrund des eingesetzten Vertrauensmodells als vertrauenswürdig gilt
 - ▶ z.B. ausgestellt durch eine vertrauenswürdige CA
 - eine gültige Signatur hat

13

Netzicherheit – Architekturen und Protokolle Grundlagen PKI/PMI



- 1 Motivation
- 2 Digitale Zertifikate
- 3 Infrastrukturen
- 4 PKI (Bausteine)
- 5 Vertrauensmodelle



- **Kerndienste** des Management von Zertifikaten
 - Registrierung, Zertifizierung, Publizierung
 - Widerruf, Re-Zertifizierung
- **Infrastrukturen** zum Management von Zertifikaten
 - ID-Zertifikaten
 - ▶ **Public Key Infrastructure** (PKI)
 - Attributzertifikaten
 - ▶ **Privilege Management Infrastructure** (PMI)
 - **Autorisierungszertifikate:** ?
 - ▶ (bisher kein Begriff geprägt, jedoch starke Parallelen zur PMI vorhanden)

15

- PKI und PMI
 - X.509
 - ▶ Authentifizierung und Autorisation für X.500 Standard
 - X.500
 - ▶ Globales verteiltes Verzeichnis, Internet-Telefonbuch
 - PKI wesentlich durch X.509-Standard geprägt
 - PMI ebenfalls, jedoch noch relativ neu, daher wenig verbreitet
 - PKI-/PMI-Architektur dennoch von X.509 unabhängig, daher
 - ▶ erst neutrale Einführung
 - ▶ dann Vorstellung der X.509-spezifischen Formate

16

- Weitere Standards
 - SDSI/SPKI (nicht behandelt)
 - ▶ zu X.509 alternative Architekturen und Formate
 - ▶ unvollendete Standardisierung, dennoch interessante Konzepte
 - PGP (wird anschließend behandelt)
 - ▶ ID-Zertifikatsystem, das mit minimaler Infrastruktur auskommt

17

Netzicherheit – Architekturen und Protokolle Grundlagen PKI/PMI



- 1 Motivation
- 2 Digitale Zertifikate
- 3 Infrastrukturen
- 4 PKI (Bausteine)
- 5 Vertrauensmodelle



- Public Key Infrastructure (PKI)
 - ist eine Infrastruktur zum Management von ID-Zertifikaten
 - ermöglicht somit Authentifikation öffentlicher Schlüssel
- Bausteine einer PKI
 - Organisatorische Bausteine
 - ▶ Zertifizierungsrichtlinie (Certification Policy)
 - ▶ Dokumentation interner Abläufe (Certification Practice Statement)
 - ▶ Zugrundeliegendes Vertrauensmodell
 - Technische Bausteine
 - ▶ Zertifikatsformat (z.B. X.509), das das Vertrauensmodell unterstützt
 - ▶ Managementprotokolle zur technischen Umsetzung der PKI-Dienste

Wie und von wem werden diese Bausteine eingesetzt und umgesetzt?

19

Eine PKI besteht aus folgenden Elementen

- **Benutzer** (subject, end entity)
 - Mensch, Maschine oder Prozess
 - meldet sich bei der PKI an (*enrollment*) und lässt sich ein Zertifikat ausstellen
 - will andere öffentliche Schlüssel authentifizieren
- **Registration Authority** (RA)
 - Implementiert administrative Aspekte der PKI
 - Schnittstelle zwischen Benutzer und CA
 - Entkopplung (CA i.d.R. offline)
 - evtl. direkt Teil der CA



20

- **Certification Authority** (CA)
 - Implementiert Zertifizierung
 - folgt technischen Standards, die Formate spezifizieren
 - erzeugt durch Signatur Zertifikate
 - Schutz dieses Signaturschlüssels
 - Erstellung von Widerrufslisten
- **Speicher/Verzeichnis** (directory)
 - für ausgestellte Zertifikate, gültige und historische
 - Abruf von Zertifikaten über diverse Protokolle möglich
 - Publizierung der Gültigkeit von Zertifikaten über Widerrufslisten



21

Eine CA kann ein Zertifikat (evtl. vom Benutzer ausgelöst) vor Ablauf seiner Gültigkeitsdauer widerrufen, wenn

- das Zertifikat **nicht mehr benutzt** wird
- der private Schlüssel **nicht mehr nutzbar** ist
- der zu einem Zertifikat gehörige private Schlüssel sicher oder eventuell **kompromittiert** wurde
- Angaben in dem Zertifikat **nicht mehr stimmen**
- Parameter des Schlüsselpaares **nicht mehr adäquat** sind

22

Anforderungskatalog

- Sicherheit interner Abläufe
- Sicherheit der Signaturschlüssel der CA
- Effizienz: Validierung eines Zertifikates
- Skalierbarkeit
- Komfort: vertretbarer Aufwand für Benutzer
- **Vertrauenswürdigkeit**

23

- **Vertrauen, Vertrauenswürdigkeit**
 - bereits mehrfach erwähnt, aber was ist das?
 - Wie wird Vertrauen in einer PKI hergestellt?
 - ▶ z.B. Vertrauen in die Gültigkeit eines Zertifikats

→ nächste Vorlesungseinheit

Historisch

- Loren Kohnfelder: Towards a practical public-key cryptosystem. Bachelor Thesis, MIT, Cambridge, 1978.

Aktuelles Buch

- Carlisle Adams, Steve Lloyd: Understanding PKI, Addison Wesley, 2003

Aktuelle Online-Dokumente

- PKI-Forum: CA-CA Interoperability; 2001
 - guter Überblick über das Thema, dabei recht kurz gefasst
- The Open Source PKI Book, online verfügbar