Netzsicherheit – Architekturen und Protokolle
Grundlagen PKI/PMI

Vertrauen

Vertrauen ist normal im Alltagsleben(!), im Zusammenhang mit Sicherheit in Netzwerken hingegen nicht.

Was ist Vertrauen? Welche Eigenschaften hat es?

- Definition von Gambetta in „can we trust trust?“

  *“**trust** [..] is a particular level of the subjective probability with which an agent assesses that another agent [..] will perform a particular action, both **before** he can monitor such action [..] **and** in a context in which it affects **his own** action [..]”.*

Vereinfacht

- A vertraut B, wenn A davon ausgehen kann, dass B sich erwartungsgemäß verhält
- A vertraut in einen Sachverhalt, wenn es von seiner Korrektheit überzeugt ist

Eigenschaften von Vertrauen

Vertrauen ist

- subjektiv
- fuzzy (Misstrauen < Ungewissheit < blindes Vertrauen)
- gerichtet (nicht zwangsläufig gegenseitig)
- bedingt transitiv, nimmt bei Transitivität ab
- an Fragestellung gebunden
- Risiko-abhängig
- basiert auf Erfahrungen

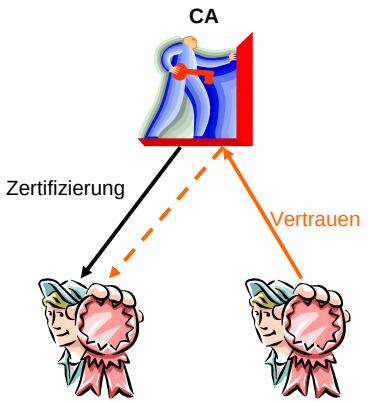
Wie Vertrauen in Zertifikate entsteht, wird durch ein Vertrauensmodell beschrieben…

Vertrauensmodelle

- Ein Vertrauensmodell (*trust model*) beschreibt,
  - welchen Zertifikaten ein Benutzer trauen kann,
  - mit welchen Elementen des Modells Vertrauen hergestellt wird,
  - wie dieses Vertrauen eingeschränkt bzw. kontrolliert werden kann.
- Vertrauen basiert meist auf einem oder mehreren Vertrauensankern (*trust anchor*)
  - Ausgangspunkte für die Validierung eines Zertifikats
  - technisch gesehen: selbstsigniertes Zertifikat
- Bei erfolgreicher Validierung überträgt sich das Vertrauen in eine Vertrauensanker in den Inhalt des von ihr ausgestellten Zertifikats (in Bildern: – – →)

Modell: Single-CA

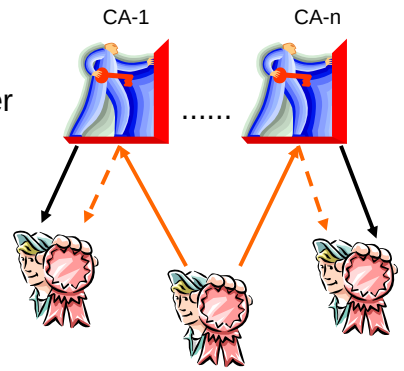
- Eine CA erstellt alle Zertifikate, d.h. ist für Registrierung und Zertifizierung zuständig
- Bewertung:
  - ☺ nur ein Vertrauensanker erleichtert Validierung
  - ☹ alle Teilnehmer müssen dieser einen CA trauen
  - ☹ Kompromittierung des CA-Schlüssels hat globale Konsequenzen
  - ☹ CA hat Monopolstellung (politischer bzw. kommerzieller Gesichtspunkt)



Welche Probleme gibt es bei Single-CA mit globaler Abdeckung?

Modell: Oligarchie von CAs

- Zertifizierung durch mehrere CAs:
  → distributed trust architecture
- Bewertung: Wie „Single-CA“, aber
  - ☺ keine Monopolstellung einer CA mehr, Wettbewerb
  - ☺ Kompromittierung hat begrenzte Auswirkung
  - ☹ initiale Prüfung mehrerer CA-Schlüssel
  - ☹ Validierung mittels mehrerer CA-Schlüssel
  - ☹ mehrere CA-Schlüssel müssen geschützt werden
  - ☹ falsche CA einfacher in Software implantierbar



Beispiel: CA-Zertifikate im Firefox

- Welche der folgenden Institutionen haben kein Zertifikat im Firefox Browser (Windows, Version 3.0.8) eingebaut?
  - Go Daddy
  - VeriSign
  - Staat der Nederlanden
  - TURKTRUST
  - AddTrust
  - Microsoft ← einziges Zertifikat, welches nicht im Firefox ist
  - NetLock
  - VISA
  - beTRUSTed
- Welches ist der richtige SHA1-Fingerprint des Entrust-Zertifikats?
  - 99:A6:9B:E6:1A:FE:88:6B:4D:2B:82:00:7C:B8:54:FC:31:7E:15:39
  - FC:31:7E:15:5A:51:BC:8A:7C:B8:DE:F1:00:F1:4D:2B:82:00:54:7A
  - 2B:82:DF:11:99:A6:6D:4A:10:0A:61:AF:FE:9A:AA:8A:7C:31:7E:51

Verbindungsmöglichkeiten zwischen Ankern

- Problem
  - Prüfung eines *fremdsignierten* Zertifikats
- Folgende Möglichkeiten zur Zusammenarbeit mehrerer Vertrauensanker existieren
  - Cross-Certification
  - Certificate Trust List
  - Bridge-CA

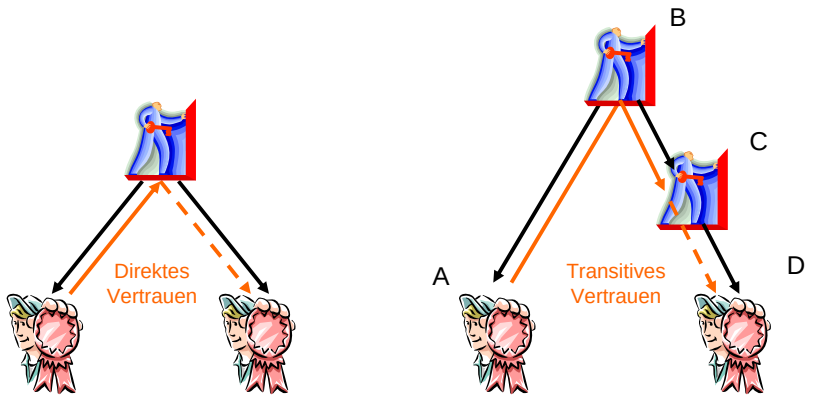
Transitivität von Vertrauen

- Vertrauen
  - bisher basierten alle Modelle auf *direktem Vertrauen*
  - für komplexere Modelle ist jedoch *transitives Vertrauen* notwendig
- Frage: Was ist Transitivität von Vertrauen?
  - wenn A Vertrauen in B (und seine Zertifizierungen) hat, und B Vertrauen in C (und seine Zertifizierungen) hat, so kann A auch C (und seinen Zertifizierungen) vertrauen

→ ist transitives Vertrauen ein *sinnvolles Konzept?*
→ warum bzw. warum nicht?
→ *wieviele Hops* würden Sie zulassen?

- Notwendig für transitives Vertrauen: *Delegierung*

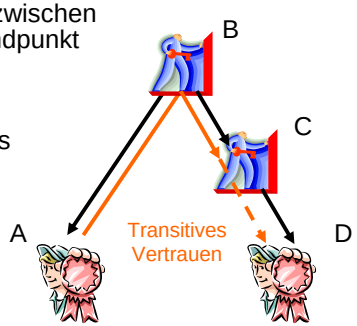
Direktes und transitives Vertrauen



Validierung bei Transitivität

Bei Transitivität spaltet sich Validierung eines Zertifikats in

- Konstruktion: Zertifikatskette bzw. Zertifikatspfad
  - Ausgangspunkt: Vertrauensanker
  - Endpunkt: zu validierendes Zertifikat
  - Aufgabe: suche nach Zertifikaten, die mittels transitivem Vertrauen einen Pfad zwischen dem Vertrauensanker und dem Endpunkt herstellen
- Validierung der Zertifikatskette
  - Prüfung der Korrektheit des Pfades (Verkettung, Delegierung)
  - Validierung jedes einzelnen Zertifikats

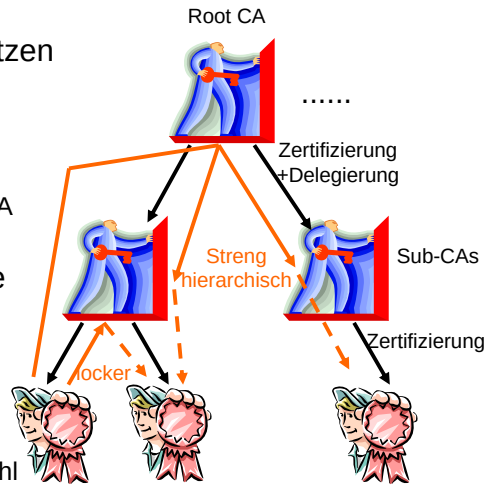


Weitere Modelle

- Bereits behandelte, nicht-transitive Modelle
  - Single-CA
  - Oligarchie von CAs
- Im Folgenden: komplexere, transitive Modelle
  - Oligarchie von CAs + Delegierung
  - Top-Down
  - Anarchie

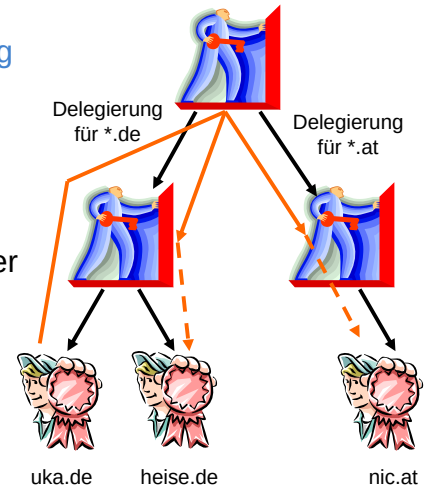
Modell: Oligarchie von CAs + Delegierung

- Delegierung: CAs können untergeordnete CAs einsetzen
- CA-Bezeichnungen
  - Root-CA: Vertrauensanker
  - Parent-CA: direkt übergeordnete CA
  - Sub-CA: untergeordnete CA
- Bewertung: wie „Oligarchie von CAs“, aber
  - ☺ Kompromittierung eines Sub-CA-Schlüssels hat beschränkteren Wirkungsbereich
  - ☺ Skalierbarkeit
  - ☹ höhere CA-Schlüsselanzahl
  - ☹ Validierung aufwändiger



Modell: Top-Down

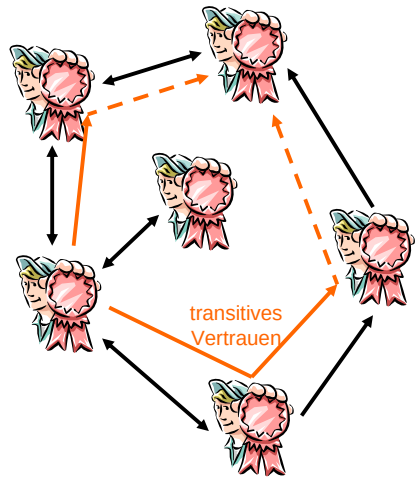
- Single-CA mit Delegation und Einschränkung der Delegierung auf Teilbereich eines hierarchischen Namensraums (name subordination)
  - Beispiele: DNS oder X.500
- Bewertung: wie Single-CA, aber
  - ☺/☹ Delegation (siehe letztes Modell)
  - ☺ kontrollierte Delegation
  - ☹ Validierung des ganzen Pfades (nie One-Hop)



Modell: Anarchie

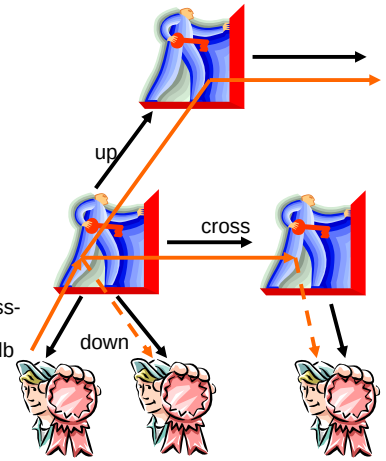
Jeder Benutzer ist eine CA und kann je nach Vertrauen eingesetzt werden (auch transitiv)

- Bewertung:
  - ☺ Auswirkung bei Kompromittierung beschränkt
  - ☹ alle Schlüssel sind CA-Schlüssel
  - ☹ Skalierbarkeit
  - ☹ keine einheitliche Zertifizierungspolitik, somit Transitivität von Vertrauen problematisch
  - ☹ Zertifizierungen schwer kontrollier- bzw. einschränkbar



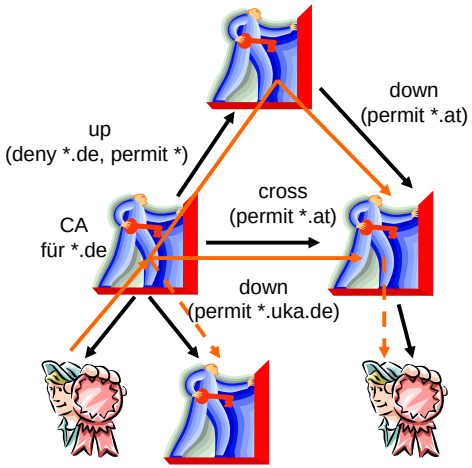
Modell: Up-Cross-Down

- Jeder Knoten kann 3 Typen von Zertifikaten besitzen:
  - ***Down***: Zertifikat eines Kindknoten
  - ***Up***: Zertifikat des Elternknotens
  - ***Cross***: Zertifikat eines beliebigen anderen Knotens
- Bewertung von „Up-Cross-Down“
  - ☺ Teilbäume sind unabhängig, funktionieren auch ohne Vaterknoten
  - ☺ keine Root-CA als globalen Single Point of Failure
  - ☺ lose Kopplung von Teilbäumen mittels Cross-Zertifikate möglich
  - ☺ Kompromittierung von Zertifikaten außerhalb eines Teilbaumes beeinflussen nicht die Sicherheit zwischen Knoten im Teilbaum
  - ☹ Unkontrolliert
  - ☹ Komplexere Prüfoperation, Pfadfindung
  - ☹ Anzahl der Zertifikate



Modell: Flexibles Bottom-Up

- Wie Up-Cross-Down, aber kontrollierter durch name constraints
  - permit/deny schränken den delegierten Namensraum beliebig flexibel ein
  - kein eindeutiger Pfad, sondern mehrere mögliche Pfade
- Bewertung von „ Flexibles Bottom-Up“
  - ☺ sehr flexibles Modell
  - ☺ hohes Maß an Kontrolle
  - ☹ Skalierbarkeit aufgrund mehrerer Pfade



Zusammenfassung Modelle

- Abschließende Bewertung
  - Single-CA nur in kleinen Umgebungen realisierbar, sonst Oligarchie
  - Skalierbarkeit durch Verteilung/Delegierung möglich
  - Anarchie leicht einsetzbar, aber schwer kontrollierbar
- Implementierung des gewünschten Vertrauensmodells über einen technischen Zertifikats-Standard
  - **X.509** (siehe Abschnitt PKI)
  - **PGP** (siehe Abschnitt über PGP-Mail)

Aus der Praxis

- Bisher präsentiert: Vertrauensmodelle
  - mit binären Vertrauensentscheidungen
    - Alice vertraut Bob voll oder gar nicht
      - ist das eine sinnvolle Modellierung?
      - lassen sich Zwischenstufen finden?
    - Abweichende Lösung: PGP-Vertrauensmodell
    - Zwischenweg: Beispiel EV-SSL-Zertifikate
  - die sich nur auf Identitäten beziehen
    - Wiederum: PGP-Vertrauensmodell weicht ab
  - die direkt in Zertifikaten abgebildet sind
    - Alice vertraut Bob ⇔ Alice stellt Bob Zertifikat aus

Literatur

Buch (wie auch für das vorige Kapitel)

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

Artikel:

- R. Perlman: An Overview of PKI Trust Models, IEEE Network 13(6):38-43, 1999.
  - Wie der Titel sagt: Überblick über (theoretische und praktisch eingesetzte) Vertrauensmodelle.
- PKI-Forum: CA-CA Interoperability, 2001
  - online verfügbar