# Freie Zertifikate für Schulen und Hochschulen

Dr. Thomas Bremer

CAcert Inc.

# Public Key Kryptographie

- Zwei Schlüssel:
  ein Öffentlicher und ein Privater
- Damit kann man Daten verschlüsseln und
  digital signieren
- Wer mitmacht braucht ein solches Schlüsselpaar
- Einer braucht den privaten, der andere den
  öffentlichen Schlüssel

# Öffentliche Schlüssel verbreiten

- Die Identität jedes öffentlichen Schlüssels muss klar sein
- Dazu muss ich ihn sicher übergeben
- Das geht auch über Vermittler (Trust Center / CA)
- CA macht die Verteilung einfacher:
- Ich brauche nur dem public Key der CA
- CA muss vertrauenswürdig sein

# Public Key Infrastuktur (PKI)

- Eine PKI besteht aus CA(s)
- PKI liefert mehr als nur Public Key:
  Identität, Name, Aussteller, Gültigkeitsdauer...
- Das heißt dann *Zertifikat*
- PKI stellt über Zertifikat Relation zwischen
  public Key und Eigentümer her

# Root Zertifikat

- Das Zertifikat der PKI heißt *Root-Zertifikat*
- Einige werden mit Brower / Mail Client mitgeliefert
- CAcert nicht – wir arbeiten dran!
- Root Zertifikat muss nachinstalliert werden
- Download von CAcert-Website
- Achtung: Korrektheit muss geprüft werden
- Fingerprint z.B. auf Infomaterial

# Wie bekomme ich ein eigenes Zertifikat?

- Ich melde mich bei einer PKI an
  - Ich besorge mir das Root-Zertifikat
  - Ich prüfe das Root-Zertifikat
  - Ich beweise meine Identität
- Ich generiere ein Zertifikat
- Bei CAcert einfach und gut geführt auf Website

# PKI-Dienste kann ich kaufen

- Es gibt einige kommerzielle Anbieter
- Siehe z.B. Liste von mitgelieferten Root Zertifikaten in Web Browser oder Mail Client
- Kostet Geld
- Wie sicher sind sie? Habe ich Einblick?

# PKI-Dienste gibt es auch kostenlos!

- Zum Beispiel bei CAcert Inc.
- Infrastruktur ist eine Dienstleistung
- Basiert auf Gegenseitigkeit
- Erfordert Mitarbeit – nein, nicht Vortrag halten sondern Identitäten überprüfen

# Wer ist Cacert Inc.?

- Inc. steht nicht für kommerziell
- CAcert Inc. ist ein Verein mit Sitz in Australien
- CAcert Inc. hat Mitglieder weltweit,
  viele in Europa
- Gerade wurden 3.000 Assurer erreicht
- Über 150.000 Nutzer
- Interaktive Schnittstelle ist Website
  https://www.cacert.org

# Gegenseitige Bestätigung

- CAcert- Assurern bestätigt Identität
- Persönliches Treffen
- Amtlicher Ausweis mit vollständigem Namen, Bild und Unterschrift
- Sicherheitsmerkmale des Ausweises werden geprüft
- E-Mail-Adresse

# Cacert-Punktesystem

- Pro Bestätigung (Assurance) gibt es Punkte
- Jeder Assurer hat eine Punktegrenze, max. 35
- Ab 1 Punkt: E-Mail-Zertifikate ohne Namen
- Ab 50 Punkte: E-Mail-und Server-Zertifikate
- Ab 100 Punkte: Code-Signing
- Ab 100 Punkte mit bestandener Assurer Challenge Berechtigung, andere zu bestätigen
- 150 Punkte: Maximum – mehr geht nicht

# Minderjährige

- Minderjährige sind eingeschränkt geschäftsfähig
- CAcert-Regeln dafür werden überarbeitet
- Erziehungsberechtigter muss dabei sein
- Minderjährige Assurer können höchstens 10 Punkte vergeben

# Assurer Challenge

- Qualifikationstest für Assurer
- 100 Fragen zu CAcert und Kontext
- 25 Fragen werden ausgewählt
- 80 % sind korrekt zu beantworten
- Test erfolgt online
- Kein Zeitlimit, alle Hilfsmittel erlaubt
- Dieser Test ist auch (vor allem?) Lernmotivation
- 100 Punkte + Challenge bestanden

  => Du bist Assurer!

# Schulen und Hochschulen und Cacert (I)

- Jede Schule oder Hochschule kann SSL-Zertifikate von CAcert bekommen
- Zertifikate sind kostenlos
- Individuelle Zertifikate oder Organisation Assurance (OA)
- OA: Nur ein Verantwortlicher
- Z.B.: ETH Zürich und Uni Zürich

# Schulen und Hochschulen und Cacert (II)

- Soziales Gefüge
- Viele (interessierte) Menschen treffen sich
- Man kennt sich – Ausweis ist trotzdem zu prüfen!
- Es können Assurance Offices eingerichtet werden an Lehrstühlen, in Fachschaften...
- Assurances können in Lehrbetrieb eingebunden werden
- Z.B.: Uni Karlsruhe (TH) hatte Vorlesung mit zwei Dozenten, die Assurances durchführten

# CAcert Deutschland e.V.

- Gerade in Gründung
- Sitz in Berlin
- Eigener Verein, kein Teil von CAcert Inc.
- Kooperation mit und Förderung von CAcert Inc.

# Hier und heute – BLIT 2009

- Wir habe hier auch einen Stand
- Ausweis dabei? Vorbeikommen!
  Assurance abholen!
- online-Anmeldung kann auch nachgeholt werden