

Community Zertifizierungsstelle für Digitale Identität & Privatsphäre



SSL / S/MIME Zertifikate

Agenda

- **Identität und Vertrauen**
- **WoT und die CACert Gemeinschaft**
- **CACert - Gemeinschafts-Zertifizierungsstelle**
- **Anwendungen digitale Zertifikate**
 - **Benutzer Zertifikate**
 - **Server Zertifikate**

Agenda

- **Identität und Vertrauen**
- **WoT und die CACert Gemeinschaft**
- **CACert - Gemeinschafts-Zertifizierungsstelle**
- **Anwendungen digitale Zertifikate**
 - **Benutzer Zertifikate**
 - **Server Zertifikate**

Vertrauen ist nicht Identität

- Wer sind (oder waren) sie?
- Sind (oder waren) sie vertrauenswürdig?
- Wie identifiziert jeder den anderen?
- Ist einander "kennen" Identifikation?



Im Internet ist jeder ein Hund



Sicherheitsanforderungen Daten / Inhalte

- Vertraulichkeit
 - Daten/Inhalte nur für definierten Empfänger
- Authentifizierung/Authentizität
 - Nachweis Ursprung Daten/Inhalte und Absender
- Integrität
 - Daten/Inhalte müssen unverändert sein. Falls sie verändert wurden, muss es ersichtlich sein
- Verbindlichkeit
 - Nachweis Daten/Inhalt Ersteller und Empfänger

= Ziele Kryptografie

Digitale Zertifikate als Problemlösung

- Lösen Zertifikate die Sicherheitsanforderungen für Daten/Inhalte?
 - Digitale Identitätskarte für Personen, Organisationen oder Computer
 - Identifizierung gegenüber Dritten im Internet und im Intranet
 - Authentifizierung von Daten und Dokumenten
 - Verbindlichkeit/Schutz von Daten und Dokumenten

Was ist eine digitale Identität / Zertifikat

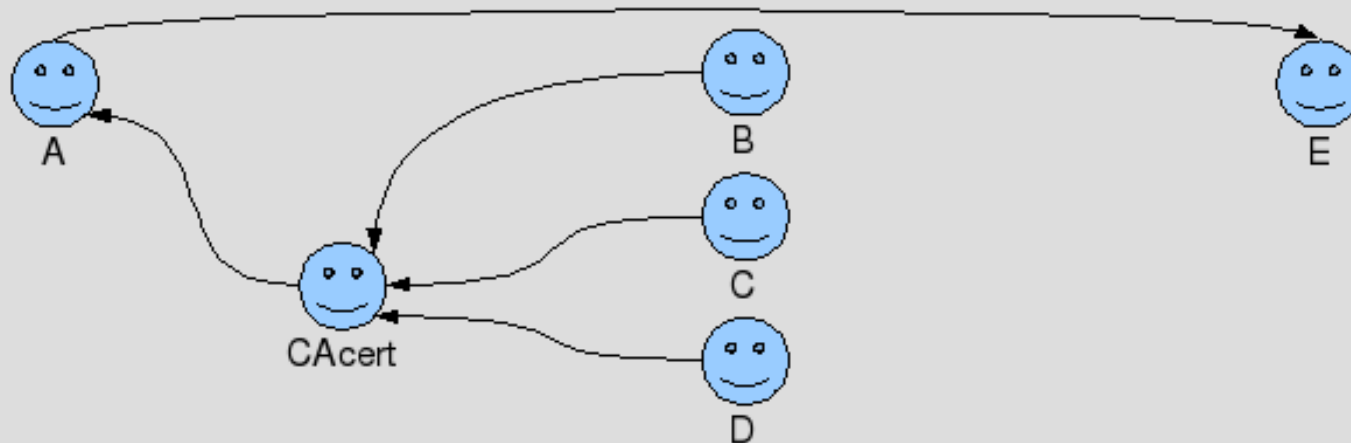
- Digitale Signatur
- X.509 Standard - PKI Infrastruktur
- Zwei Teile -
 - Privater Schlüssel
 - Öffentlicher Schlüssel - Das “digitale Zertifikat”
- X.509 und GPG / PGP können kombiniert werden

Agenda

- Identität und Vertrauen
- **WoT und die CACert Gemeinschaft**
- CACert - Zertifizierungsstelle der Gemeinschaft
- Anwendungen digitale Zertifikate
 - Benutzer Zertifikate
 - Server Zertifikate

CAcert Ansatz in der Praxis

- B, C und D - Überprüfer/Assurer - haben sich persönlich mit E getroffen, die Identität überprüft und bestätigen dies der CAcert Gemeinschaft
- A verlässt sich auf das CAcert System und kann sicher sein, dass E die Person ist, die er/ sie sagt



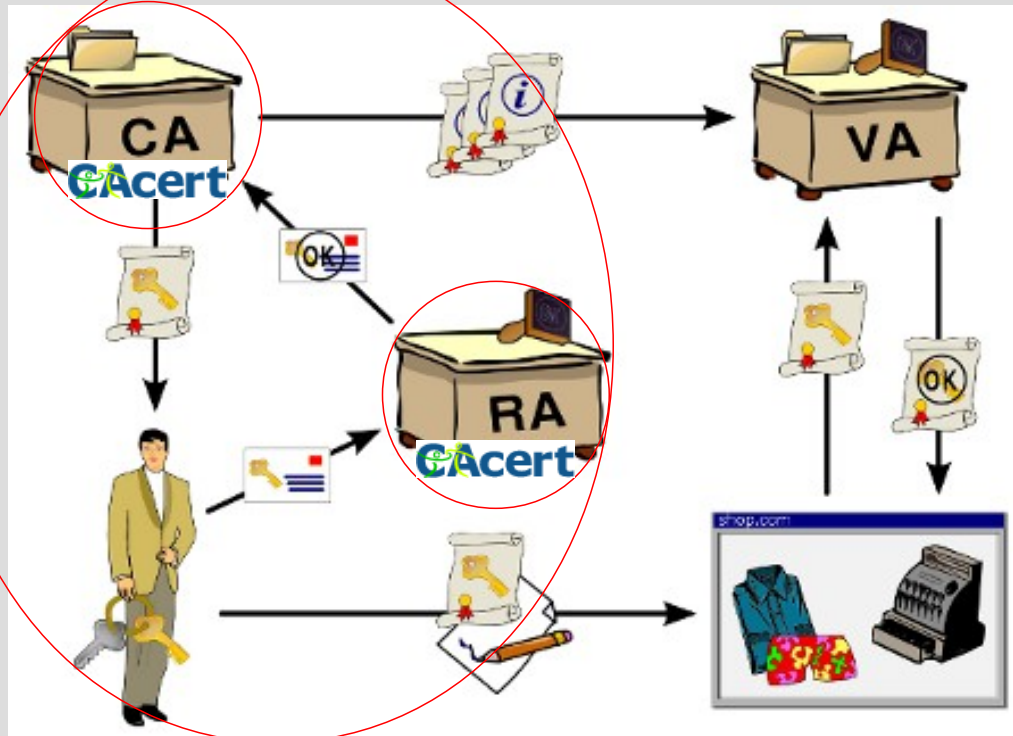
CAcert + / -

- Dafür +
 - Zertifikate sind kostenlos für die Gemeinschaft
 - Unlimitierte Anzahl an Zertifikaten
 - Überprüfung/Assurance - Bezeugung der Identität - und CAcert Konto sind lebenslänglich gültig
 - Zertifizierungsstelle von der Gemeinschaft, durch die Gemeinschaft und für die Gemeinschaft
- Dagegen –
 - Zentrale Zertifizierungsstelle
 - Arbeit um Root Zertifikat in Browser zu installieren

Agenda

- Identität und Vertrauen
- WoT und die CACert Gemeinschaft
- **CACert - Gemeinschafts-Zertifizierungsstelle**
- Anwendungen digitale Zertifikate
 - Benutzer Zertifikate
 - Server Zertifikate

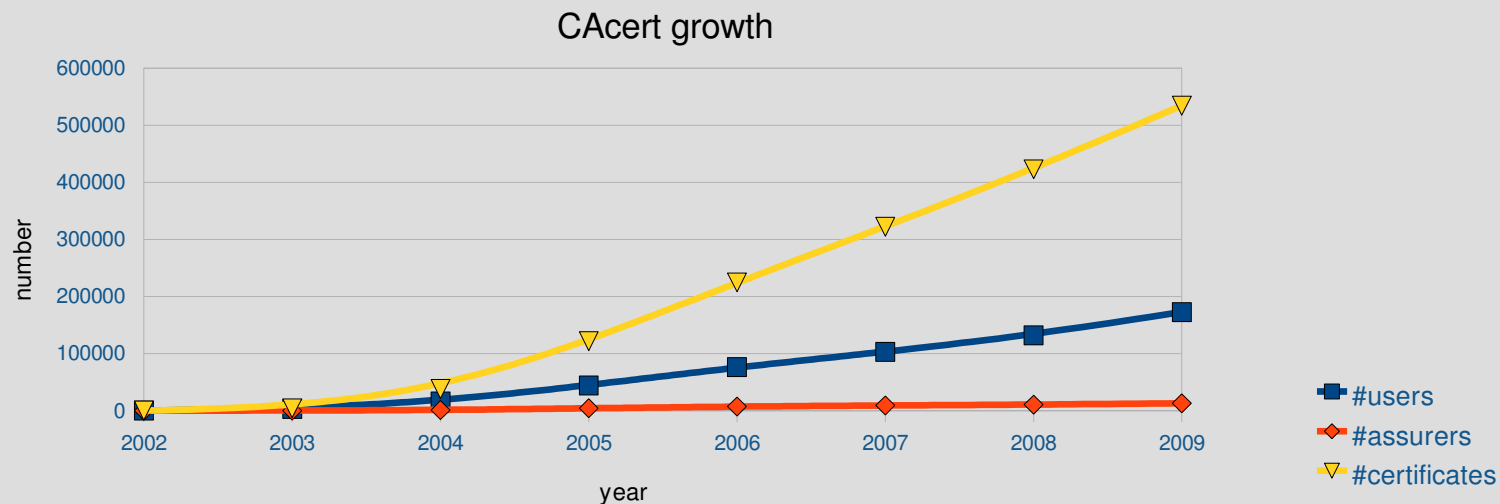
Was ist eine CA oder Zertifizierungsstelle?



- Hauptteil der PKI - Public Key Infrastructure (Verwaltung der öffentlichen Schlüssel)
- Ausgabe X.509 Zertifikate im Namen der Gemeinschaft
- Verbindet mit RA - Registration Autorität
- RA Funktion durch CAcert Assurer

CAcert Gemeinschaft im Überblick

- 2002 in Australien durch Duane Groth gestartet
- 2004 CAcert Inc. - gemeinnützige Organisation
- ~157.000 Zertifikats Nutzer, davon >3000 CAcert Assurers
- > 517.000 Zertifikate im Benutzung



CAcert Regelwerk der Gemeinschaft

- CCA - CAcert Vereinbarung der Gemeinschaft
 - Die CAcert "Verfassung"
- Set von CAcert Regeln, beispielsweise:
 - CPS - Erklärung Handhabung Zertifikate
 - SP - Sicherheits Regeln
 - PP - Datenschutz Regeln
 - DRP- Streit Lösungs Regeln
 - AP - Assurance Regeln
- Handbücher für Assurance von Personen und Organisationen

Organisations Assurance/Überprüfung

- Organisationen können der CACert Gemeinschaft auch beitreten
 - Firmen, Universitäten, Schulen, usw.
- Vorteile sind
 - Zertifikate mit dem Namen der Organisation
 - System Administrator verwaltet die Zertifikate der Organisation
- Organisation Assurance wird durch CACert ORGA-Assurers gemacht

Agenda

- Identität und Vertrauen
- WoT und die CACert Gemeinschaft
- CACert - Gemeinschafts-Zertifizierungsstelle
- **Anwendungen digitale Zertifikate**
 - **Benutzer Zertifikate**
 - Server Zertifikate

Anwendungen Benutzer Zertifikate

- Einwahl/Authentifizierung bei Web oder Intranet Seiten oder Web Anwendungen - z.B. moodle.org
 - OpenID mit Zertifikat - z.B. certifi.ca
- Signieren und verschlüsseln von E-Mail
 - S/MIME - X.509 Format - aber auch GPG/PGP
- Signieren of Software / Macros / Applets mit Zeitstempel
- Dokumente - PDF, Ooo, etc. - digital signieren mit Zeitstempel

Agenda

- Identität und Vertrauen
- WoT und die CACert Gemeinschaft
- CACert - Gemeinschafts-Zertifizierungsstelle
- **Anwendungen digitale Zertifikate**
 - Benutzer Zertifikate
 - **Server Zertifikate**

Anwendungen Server Zertifikate

- Web Server - https:// - SSL geschützt
- Mail Server
- VPN Zugang - SSL gestützt und geschützt
- SSL/TSL gestützte und geschützte Kommunikation

Das war's

Danke für ihre Zeit

Fragen?

oder

www.cacert.org