

# Der Weg zum eigenen Zertifikat - CAcert

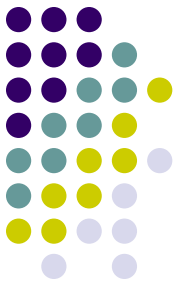
---

André Stollenwerk

CryptoParty - 16. Januar 2014

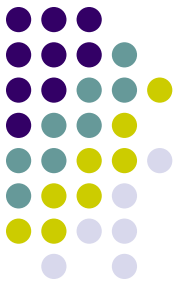
# Vertrauen, aber wem ...

---

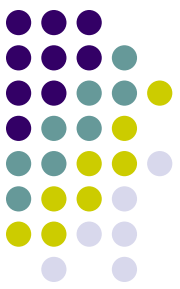


# Vertrauen, aber wem ...

---



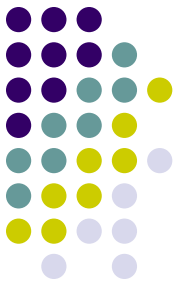
- Vertrauensnetzwerk - dezentral
  - Manuelle Pflege
  - Bedingt Endnutzerfreundlich
  - z.B. PGP



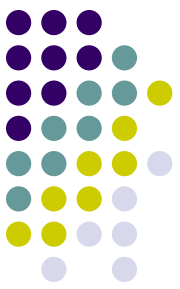
# Vertrauen, aber wem ...

- Vertrauensnetzwerk - dezentral
  - Manuelle Pflege
  - Bedingt Endnutzerfreundlich
  - z.B. PGP
- Zentrale Zertifizierungsstellen  
(**C**ertification **A**uthority)
  - Durch Zertifikatsdatenbank des Betriebssystems den meisten Nutzern implizit bekannt
  - Meist kostenpflichtig
  - z.B. SSL-Verschlüsselung von HTTP-Verbindungen

# Zertifikatskette - zentrale Vertrauensstellen

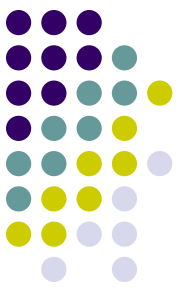


- Vertrauensstellung durch „Schlüsselbund“
  - Direkt im Betriebssystem
  - Programmspezifisch z.B. Browser
- Pfad von Basis CA zu z.B. SSL-Zertifikat
- Vertrauen durch Unterschrift des Zertifikats



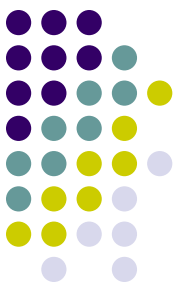
# Kostenvergleich von CAs

-  ab 250 Euro pro Jahr
-  ab 80 Euro pro Jahr
-  ab 139 US-\$ pro Jahr
-  ab 23 Euro pro Jahr
-  teils kostenlos
-  immer kostenlos



# Kostenlose CAs unter der Lupe

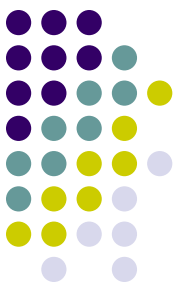
- StartCOM / StartSSL
  - Max. 1 Jahr Laufzeit
  - Klasse 1
  - In Zertifikatskette von (fast) allen Browsern
- CAcert
  - Laufzeit bis zu 2 Jahre
  - Klasse 1 & 3
  - Nicht in Windows Zertifikatskette



# CAcert - Möglichkeiten im Detail

- SSL-Zertifikate
  - 6 oder 24 Monate Laufzeit
  - Nur „CommonName“ und „SubjectAltName“
  - Domain muss validiert werden (E-Mail)
- Client-Zertifikat
  - Für validierte E-Mailadresse
    - Geschützter Login
    - S/MIME-Zertifikate (Mail)
  - 6 oder 24 Monate Laufzeit





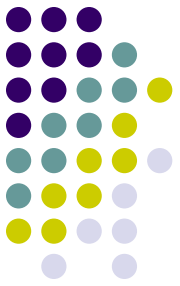
# CAcert - Möglichkeiten im Detail

---

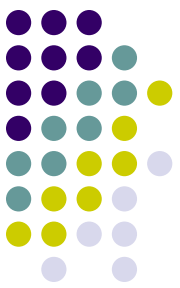
- Code-Signing Zertifikate
  - 12 Monate Gültigkeit
  - Als Spezialfall der Client-Zertifikate
- PGP-Unterschrift

# CACert Konzept

---



- Vertrauensnetzwerk durch „Assurance“
  - Überprüfung von Echtheitsdokumenten
- Wachsender Funktionsumfang mit steigendem Vertrauen
- Erste Zertifikate direkt nach Anmeldung möglich

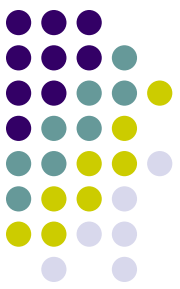


# Punktesystem

0 - 49 Punkte	Limitierte Zertifikate
50 - 99 Punkte	volle Funktionalität
100 - 150 Punkte	Assurer (nach Prüfung)

## Punktgewinn:

- Bis zu 35 Punkte je Assurance
- Maximal 100 Punkte durch Assurer
- Danach 2 Punkte pro Assurance



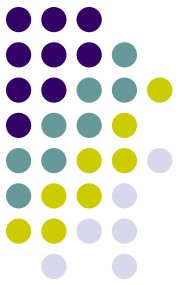
# Ablauf einer Assurance

---

- Zwei unabhängige Ausweisdokumente
  - Personalausweis
  - Führerschein
  - Reisepass
- Dokumentation des Treffens
  - Aufbewahrung durch Assurer
  - Über 7 Jahre
- Alternative Assurance durch Notar, Bank,...

# Bei Interesse...

---



- Anmeldung auf CAcert.org
- Hier direkt Assured werden
  - 2 Dokumente sind nötig
  - Vordruck zur Dokumentation vorhanden