CAcert Inc.

Questions

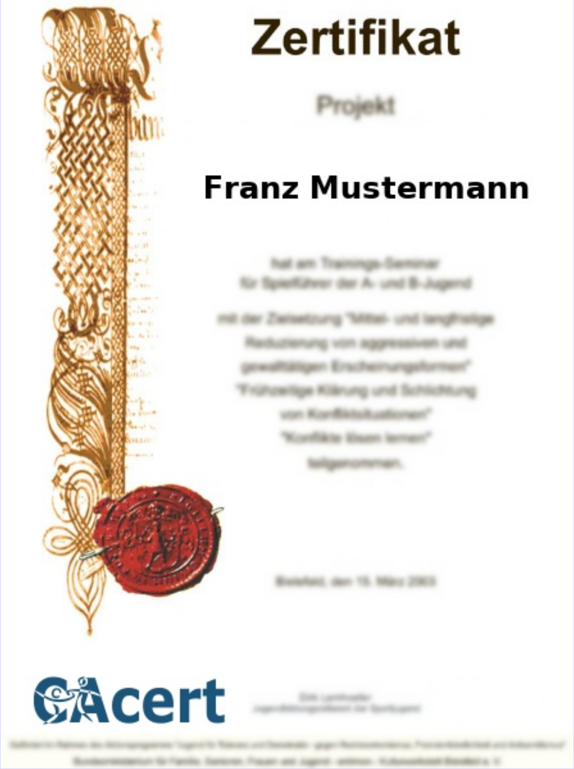
- Why are the people still using digital postcards?
- Why are the people still using passwords, and sending them in clear text?
- What can I do to protect me and my privacy?

Strategic goal

- Privacy through encryption
- Security through authentication
- Trust for the Internet
- Solution for the chicken-and-egg problem: Certificates and applications

Tasks of a CA

- „Certification Authority“
- A CA digitally binds the identity of persons and organisations („person-binding“)
- Issues digital certificates



Zertifikat

Projekt

Franz Mustermann

hat am Trainings-Seminar
für Spielführer der A- und B-Jugend

mit der Zielsetzung "Mittel- und langfristige
Reduzierung von aggressiven und
gewalttätigen Erscheinungsformen"
"Frühzeitige Klärung und Schlichtung
von Konfliktsituationen"
"Konflikte lösen lernen"
teilgenommen.

Bielefeld, den 15. März 2003

CAcert [illegible]

[illegible]

Applications

- Securing a Webserver with HTTPS
- Signing and encrypting Emails

  - SSL/TLS Server applications
  - Authentication for websites
  - Authentication for VPN´s

CAcert Inc.

- CAcert Inc. is a registered non-profit organisation based in Australia, which defines the rules and operates the servers
- Start www.CAcert.org: 2002
- Founding CAcert Inc.: 2003

Person-binding

- Until now: Verification of the identity for every certificate, costs ~ 200,- USD per certificate per year
- What does it help, if I can afford a certificate, but the rest of the world can´t?
- CAcert separates the Assurance (verification of the identity with gov. photo-ID) from the issueing of the certificates

Assurance

- Assurance is a service, where an Assurer verifies the identity of a person
- with a governmental photo-ID
- and affirms for CAcert, and issues points on the life-long account at CAcert
- free market
- >2000 Assurer worldwide

Punkteschema

- With 50 points you can issue certificates
- With 100 points you are an Assurer, you can give other people max. 10 points, and you get 2 points for it.
- Until 150 points, where you can give 35 points

Certificates

- Life-long account at CAcert
- Issue certificates yourself anytime on the internet
- certificates are free of charge
- unlimited amount of certificates
- therefore you only have initial costs, no following costs

Technology

- X.509 certificates
  - server certificates
  - client certificates
  - code-signing certificates (Java, Active-X, Cellular phones, ...)
  - IDN-Domains
- OpenPGP
  - OpenPGP Signatures
- CAcert is the first platform and technology neutral CA!

Security

- CAcert is audited with a WebTrust compatible Audit, which is a worldwide recognized Audit for CA´s
- 4-eyes principle everywhere
- open and transparent structure
- sourcecode is available for audits
- instant revocation lists

Success?

- Verified Users: > 25.000
- Issued Certificates: > 43.000
- Assurers: > 2000
- in more than 29 countries
- translated in 14 languages

- http://www.cacert.org/stats.php

Thank you very much

- http://www.cacert.org/
- http://wiki.cacert.org/

Any questions?