CAcert, a Security Community
The Problem

- Back in 2001: Sydney had WLAN network access everywhere (Sydney Wireless)
- People were running their own mail servers at home, using the Webmail on their home-mail servers from somewhere else in Sydney
- Webmail was using plain HTTP, so they broadcasted their passwords in clear on air
Strategic goal

- Privacy through encryption
- Security through authentication
- Trust for the Internet
- Solution to the chicken-and-egg problem: Certificates and applications
Tasks of a CA

- “Certification Authority”
- A CA digitally binds the identity of people and organisations (“identity-binding”)
- Issues digital certificates
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
Identity-binding

- Until now: Verification of the identity for every certificate, costs ~ 200,- USD per certificate per year
- How 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
Web of Trust

- Was “invented” around PGP
  - If your friend trusts Bob, and your friend tells you about it, and you trust your friend, then you could trust Bob
  - People sign other people’s keys (telling the public you “trust”/... them)
- 1 Million people

Problems:
- No central authority
- No defined rules
- Quality
- Trust vs. Identity
Assurance is a service, where an Assurer verifies the identity of a person with a government issued photo-ID and affirms for CAcert, and issues points on the life-long account at CAcert.

- free market
- >4000 Assurer worldwide
**Point schema**

- With 50 points you can issue certificates.
- With 100 points you become an Assurer, you can give other people a maximum of 10 points, and you get 2 points for doing it.
- Upto 150 points, where you can give 35 points.
Community

- Where do you get your points?
- “Find an assurer” near you through the website
- Meet assurers at conferences and events
  - Linuxwochen, CeBIT, CCC Congress, Linuxworld, LinuxTag, FISL,
- ...
Certificates

- Life-long account at CAcert
- Issue certificates yourself anytime on the internet
- Certificates are free of charge
- Unlimited number of certificates
- Therefore you only have initial costs, no follow-up costs
Technology

- X.509 certificates
  - server certificates
  - client certificates
  - code-signing certificates (Java, Active-X, Cellular phones, ...)
- IDN-Domains
- OpenPGP
  - OpenPGP Signatures

- CAcert is a platform and technology neutral CA!
Security

- CAcert is being audited with a WebTrust compatible Audit, which is a worldwide recognized Audit for CA’s
- 4-eyes principle
- open and transparent structure
- sourcecode is available for audits
- instant revocation lists + OCSP
Success?

- Verified Users: > 65000
- Issued Certificates: > 150000
- Assurers: 6,691
- Assurances: 41,957
- Issues points: 1,034,107
- in more than 29 countries
- translated into 26 languages

http://www.cacert.org/stats.php
Thank you very much

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

Any questions?