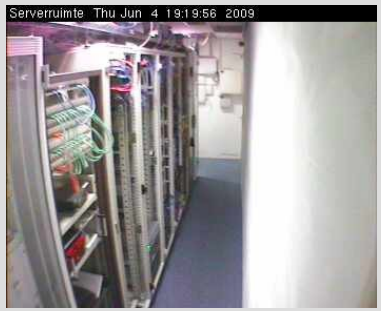
CAcert

A Communities Way To Professionalism

What's CAcert?

- 2002 Start CAcert Org → CAcert Community
- 2003 Start CAcert Inc. → Non-Profit Association located in NSW Australia
- CAcert Inc. Runs PKI Infrastructure servers for their Community Members
- Based on OpenSource thoughts



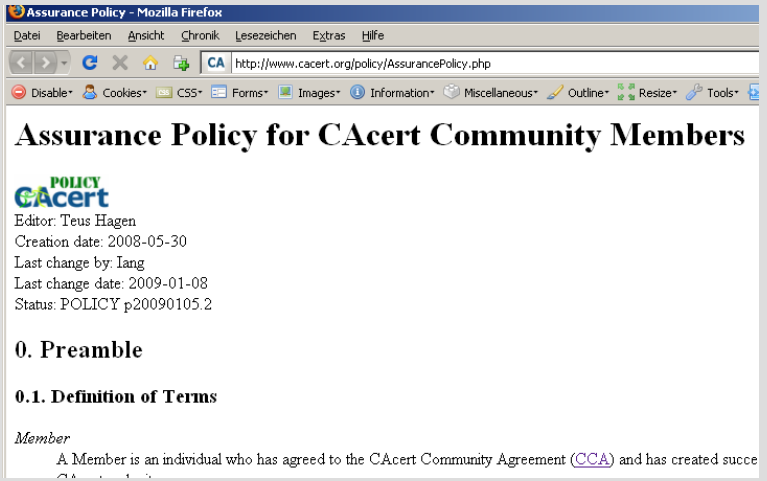
What's CAcert?

- Security and Privacy may not cost anything
- CAcert offers for free …
  - ✔ Certificates for Email Signing
  - ✔ Certificates for Email Encryption
  - ✔ Certificates for Server SSL
  - ✔ Certificates for Code-Signing and Document Signing

CAcert and the Audit

- To get CAcert Root Certs. into Browsers
- → Audit is required
- → which requires:
  - management
  - policies + practices
  - review of business & systems

… against policies and practices



CAcert and the Audit

- CAcert Audit starts in about 2005
  by David Ross (builds an audit plan → DRC)
- Ian Grigg stepped in Jan. 2006
- March 2008: 18 months business plan
  funding by NLnet, (3x 6 months)
- Audit effects CAcert's two major business areas:

  - Assurance
  - Systems

CAcert and the Audit

- a. Assurance review
- Assurance Policy is in full POLICY status

➔ It is **binding** on all Assurers

- The process of Assurance can be reviewed.

CAcert and the Audit

- b. Systems review
- Review of the systems was delayed by lack of a secure hosting service.
  - The systems were moved 1st October, 2008
  - from Vienna
  - to the secure data center at BIT, a company in Ede, NL.

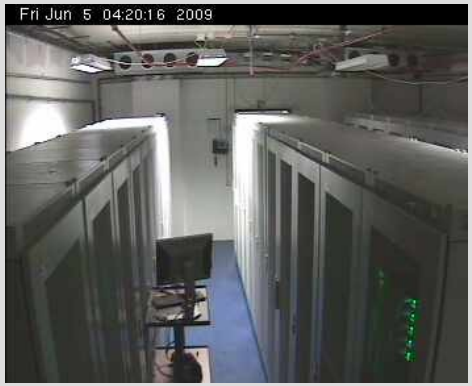
CAcert and the Audit

- b. Systems review (cont.)
  - A new team of systems administrators
  - Approval of the Security Policy to DRAFT mode

    => Binding on the systems administrators and the Access Engineers

    => now possible to review the systems against the policy.

CAcert and the Audit



- b.i On-Site Inspection
- 1st visit on 4, 5, 6th May, 2009
  warm-up: personnel, Roots, Access, inventory
- probably 1st of 3 visits.
- Next scheduled mid-June

CAcert and the Audit

b.ii We still lack the CPS
(Certification Practice Statement)

(which is nearly ready)

CAcert and the Audit

- b.iii Review of the software

- Innsbruck software camp
  Week 20th April

- Serious difficulties in maintenance, improvement and securing
- Cannot form a conclusion over software

- New software development team, new design, new build

Audit Background

Audit Background

- One big result of the thinking process
- we required:

➔ a CAcert Community Agreement

- and it had to do following things:

Audit Background

a. make Members a mutually binding Community.

b. to state the Risks/Liabilities/Obligations

c. to limit the liabilities

- ➔ 1000 Euros
- ➔ to *allocate the liabilities* back to the Members

Audit Background

- How do we allocate the liabilities?
- ➔By making our own „forum of dispute resolution“,
- ➔agreeing to be bound to that resolution,
- ➔writing a Policy to control that process:
- ==> Arbitration.

Audit Background

- Summary: The original “Why” of Arbitration:
  - ➔ Audit (DRC) forced *disclosure* of Liabilities
  - ➔ simple fix: *limiting*
  - ➔ complex fix: *allocation*
  - ➔ the safe and cheap way to allocate is:
  - ➔ to use our own Arbitration
- (Last section discusses „How“.)

Summary

Remember: This Is All About …

- To get CAcert Root Certs. into Browsers
- → Audit is required
- → which requires:
  - ….

And the Practice?

- modified CAP forms
- Assurer Training Events (audited Assurances)
- Mailings to inform their members about changes and changed procedures
- CAcert Community Agreement translations

apart from that

- much paperworks (Policies, Handbooks)

Thanks, Questions & Answers

- http://www.CAcert.org
- Ulrich Schroeter
  ulrich@CAcert.org
- Questions ?