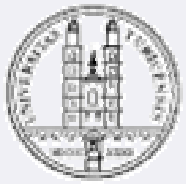
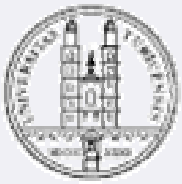
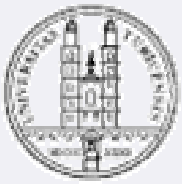


Experiences running a private PKI @University of Zurich



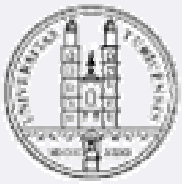
Server CA

- Running a CA for Servers since March 2001
- 233 certificates, currently 77 valid
- Mostly for internal use, avoiding costs for VeriSign Certificates
- Extended use of X509-extensions possible (webmail.unizh.ch,pop.unizh.ch)



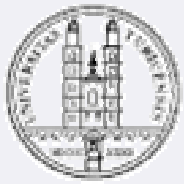
Server CA

- Move to AAI-Certificates as soon as Root-Certificates are integrated in Browsers for public sites, eg. http://webmail.unizh.ch
- Plans to keep CA for internal purposes https://www.ca.unizh.ch/server/



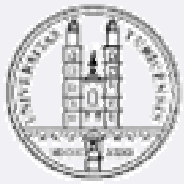
S/MIME Certificate Authority

- Based on PHPki (http://sourceforge.net/projects/phpki)
- Different CA's for managed PKI Certificates and for Server Certificates
  - Different Services
  - Different Policies
  - Keep option to integrate both CA's in CA managed by SWITCH



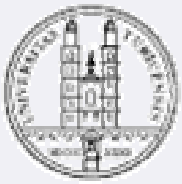
Aims running our own PKI

- Offer Certificates to ***members*** of the University of Zurich **for free**
- Distribute Certificates **signed** by the University of Zurich
- Be ready to support users as soon as a service becomes available (SWITCH or nation-wide)



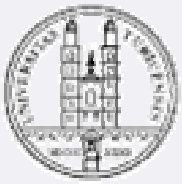
Distribution of Certificates

- Online-Service to apply for a Certificate (Validated, easy AAI enabling possible)
- Need to show up personally at our Helpdesk
- Online Renew/Revoke once a Certificate is issued



Usage

- Operational since February 2004
- 303 Certificates issued, 187 currently valid
- 59 of 187 for members of IT-Services

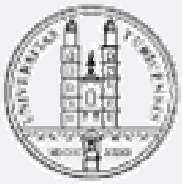


Acceptance

- 187 Certificates for > 22’000 Students and 4’000 Staff-Members
- Users accept and agree to obtain the certificate only after showing up personally
- Users even accept pass-phrases instead of passwords
- Used for e-mails only (some signing of pdf-Documents)

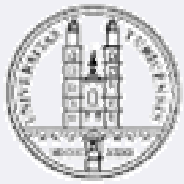
You need to

- Prepare documentation step by step for different e-mail clients on different operating systems
- Point out the reasons for different Root Certificates and the correct usage
- Explain why some e-mail partners get “Errors” when reading signed e-mails



Problems

- Wrong configuration of e-mail clients
  Outlook: Send clear text signed messages when sending signed messages
- Problems with passphrases
  - forgotten passphrase
  - Microsoft Certificate Manager will not accept passphrases longer than 32 characters



Conclusion

- Careful documentation needed
- Users are accepting identification-policies
- Users are becoming aware of different issues concerning security
- Users are willing to accept inconvenience due to our own Root-Certificates

Universität Zürich

Questions ?