Introducing the DFN-PCA

OpenCA Workshop 2004
12.10.2004
Munich

Reimer Karlsen
DFN-CERT Services GmbH
Hamburg

dfnpca@dfn-pca.de
http://www.dfn-pca.de/

Overview

- What / Who is the DFN-PCA?
- Current PKI services
- New DFN-PKI strategy

What / Who is the DFN-PCA?

- **P**olicy **C**ertification **A**uthority and PKI knowledge center for the German national research and education network **DFN**
- Providing certificates and PKI support for our constituency
- Main constituency: Member organisations of the DFN, G-WiN costumers, orgs from the research & educational sector, public & non-profit orgs / associations / societies
- We are part of the DFN-CERT Services GmbH which is also operating the CERT for the DFN

Certificates issued by our CAs

- PGP “certificates” for (Sub-)CAs and users
- X.509 certificates for (Sub-)CAs, servers and soon users

CAs operated directly by the DFN-PCA:

- PGP Root CA
- PGP User CA
- X.509 Root CA
  - Root certificate is not pre-installed in browsers and other client applications
- X.509 Server CA

Current certification policies

- PGP Low-Level Policy for PGP certificates
- WWW-Policy for X.509 certificates

- General conditions
  - **Personal** registration and identification by identity-card / passport
  - **No** key escrow, **no** key recovery
  - **No** full-automatic certificate generation

Current model of operation

- Only limited resources at DFN-PCA

Therefore the DFN-PCA itself

- provides **no direct bulk / mass** certification services
- provides **only restricted end-user** certification services, e.g. only PGP User certificates
- provides only X.509 server certificates but no S/MIME certificates
- promotes the setup of Sub-CAs and their RAs **within** the participating organisations

New DFN-PKI strategy

- X.509
  - Directed at DFN G-WiN customer organisations
  - *“Advanced electronic signatures”* in terms of German el. signature law
  - Two new RFC 3647 compliant certification policies (primary language German, English versions will follow):
    - ***Basic***
    - ***Classic***
  - Sub-CA and RA hosting at DFN-PCA
  - Bulk / mass certification services by DFN-PCA
- PGP
  - PGP CA services are continued as of today

Classic Policy

- Similar to WWW-Policy
- New root certificate ? Not pre-installed in browsers, possibly at a later time
- Migration path from current hierarchy
- More identification and authentication methods allowed e.g. via
  - Personal identification (identity-card / passport)
  - PostIdent
- If properly identified, full-automatic certificate issuance possible
- Key escrow of encryption-**only** keys is possible

Basic Policy

- Less strict than Classic- and current WWW-Policy
- New root certificate, not pre-installed in browsers
- Key escrow allowed
- If properly identified, full-automatic certificate issuance possible
- More identification and authentication methods e.g. via
  - Personal identification (identity-card / passport)
  - PostIdent
  - Traditional letter by postal service (only if existing internal relationship between host organisation and subscriber, e.g. student to university)

CA & RA organisation

- Sub-CA & RA within the organisation (as now)
- RA within the organisation, Sub-CA hosted at DFN-PCA
- Sub-CA and RA both hosted at DFN-PCA
- Personal bulk / mass S/MIME and client certificates
- Server / machine certificates
- Generic CA & RA for personal bulk / mass S/MIME & client and server / machine certificates operated by DFN-PCA for members that have no specific CA of their own (conditions are discussed at present)

Thanks

Thanks for your attention!

If you want to use this opportunity to enroll and identify yourself personally for a certificate, please contact me in the lobby during the workshop.

dfnpca@dfn-pca.de

www.dfn-pca.de