



your connection to the network of trust



ISIS-MTT and European Bridge-CA

Changes since 2005

P. Steiert



Short description: ISIS-MTT

- ISIS-MTT is a profile of the existing RFC 3280.
- Main focus was to ensure interoperability regarding a complete Public-Key Infrastructure.
 - Profile and requirements about Certificates, Services, other Standards, e.g. S/MIME, LDAP, OCSP, etc.
- Output:
 - 2 Profiles: 1 for international conformity, 1 for national conformity
 - 1 Testbed-CD to prove interoperability of PKI components
 - 2 implementations:
 - installable version,
 - bootable cd version

ISIS-MTT changes since 2005:

- Minor bugfixes in the specification
- Extending the specification with an XML-part
- Minor bugfixes in the Testbed software
- Extending the Testbed with an XML-part

- Online Testbed available (german language)
 - Test certificates against the ISIS-MTT profile online
URL: <http://zertifikatstest.teletrust.de/OAZ/>

Short description: EB-CA

- The European Bridge-CA is a service to enable and manage cross organizational trust relations.
 - Bilateral trust-relations are difficult to handle. So a more centralistic model is much more efficient.
- The idea is to integrate existing PKI-islands to a network of trust.
- This requires:
 - A common understanding for a policy.
 - A service to collect, evaluate and distribute compliant CA certificates in a identity and integrity saving way.
 - A set of services which ease the usage of the service.

EB-CA work in progress:

- Mid 2005:
 - Switch the EB-CA Policy from the proprietary format to a common international format.
 - RFC 3647 compliant format. (First step: German language only)
- Beginning 2006 translation of the new EB-CA policy into english. This will finish in July/August 2006.
- Extending the EB-CA in regard of:
Better usability by non-security experts:
 - Probably alternative solutions (e.g: cross-certification...) should be published to ease usage for end users not capable to understand PKI mechanisms.
 - Integration of the EB-CA into the root-keystore of different applications (e.g. Browsers, Viewers, etc.)

EB-CA work in progress:

- Directory service:
 - Centralized directory service to work as a „proxy“ fetching e-mail-certificates.
 - Currently heavy load
 - Load must be balanced more
 - Multiple distribution points must exist in future (fail-over)
 - Different Service Level Agreements are required. (e.g.: for free access, company access, etc.)

- Usage of organization certificates:
 - In the past the focus was rather only on person-based end-entity certificates. Organization related end-entity certificates are not covered by the policy
 - this is currently changed.

EB-CA work in progress:

- Cooperation with other organizations:
- Unizeto (PL) and ANK (RU):
 - These cooperation focuses on the usability of trans-national usage of PKI-services.
 - Benefit of PKI depends on the usability not to stop on a specific country border. The higher the benefit, the more people use this technique.
 - Discussion and evaluation of policy and services. The current parts are designed to be as interoperable for most countries as possible. But we have seen that we have to discuss parts with other countries as well to ensure higher acceptance.
- The OpenGroup in the field of Policy Assurance:
 - This work tries to omit the currently very often required policy check and possible policy mapping. This only takes time and increases costs.
 - Rethinking required for the future:
 - A new member for a Bridge-CA can get a kind of quality seal for specific purpose (like ISO-9001 for instance)
 - Others can check this seal and find out that this security level is adequate to realize some business processes.
 - Reduction of auditing and validation costs regarding to Policies.



your connection to the network of trust

Questions ? Need help ? Ideas ?

Feel free to contact us.

Peter Steiert
TeleTrusT e.V.
email: peter.steiert@teletrust.de

Telefon: +49 361 3460531
Telefon: +49-172-2764341
Telefax: +49 361 3453957

Helmut Reimer
TeleTrusT e.V.
email: helmut.reimer@teletrust.de
Chamissostraße 11
D-99096 Erfurt
Telefon: +49 361 3460531
Telefax: +49 361 3453957

