

Trust and Mutual Recognition What should we do?

Helmut Reimer
TeleTrust
www.teletrust.de

IT-Security Workshop, Tokyo, 27th October 2004

TeleTrust - General

- Promoting the trustworthiness of information and communication technology
- founded in 1989 in Germany
- Focus on Applied Cryptography & Biometrics
- 90+ members: major user sectors, research organisations, developers and manufacturers of security products, government agencies, and test institutes.
- non-profit, political independent

More than 10 Years Experience

View on implementation of PKI-Solutions:

- The standards (ISO, ETSI, CEN, IETF, PKCS etc.) gives orientations, but no concepts for interoperability.
- The Implementations follows often the (different) legal requirements more than practical considerations.

but

- For a long time we will have paper & electronic documents in parallel.
- Therefore we have to accompany the transformation and not to expect the jump.
- The ,take-off‘ of signatures in PKI-applications needs the business case, also for CSPs.

Interoperability: Different aspects

- **From the view of a relying party:** Has to accept qualified certificates issued from different providers.
- **From the view of a signing party:** The interpretation of the signature should be possible with standard tools.
- **From the view of a business process:** Certificates of different PKI-applications should be interoperable.

Transformation - some remarks

- The gap is too wide between the high-end, one-purpose signature vision and real-used PKI applications.
- The benefit from signature applications in open environments is uncertain up to now.
- Applications in closed user groups and also in enterprise & governmental PKI's can help to find out the 'best practices'.
- Trust establishing needs a step-by-step turn over strategy.

TeleTrust Proposals

- ISIS-MTT: Profiled PKI standards
- European Bridge-CA (EB-CA): Trust establishment between PKI islands

European Bridge-CA

Applications

Authenticaitaion of users
and servers

confidential
communication
(TLS/SSL)

file encryption

encrypted Email
(S/MIME)

data authenticity and -
integrity
(digital signature)

time stamping

VPN

Single Sign On

Non Repudiation
(digital signature)

ISIS-MTT „the foundation“

Common ISIS-MTT Specification for Interoperability and Test Systems





ISIS-MTT: Objectives of the project:

- **Synthesis** of already available specifications towards a unified and open standard.
- This standard should take into account the current technical and legal requirements and should receive **active** support by the **market players**.
- Development of a test specification and a test bench, which allows the applications developers to prove their ISIS-MTT-interoperability
- Investment protection for users because of exchangeability of single components.





Actions in progress 2004

- Deployment of a usable test bench for realistic test of applications and services.
- Awarding of a “Quality Seal” for applications with proven interoperability.
- Further contribution from the specification to the international standardization.
- Strengthening of public relations and project management.
- Development of a XML-Profile based on W3C and ETSI
- Development of an Authentication-Profile (MS, SUN, Linux-OSS, SAP)



Mission of the European Bridge-CA is ...

- ... to promote the acceptance of secure eCommerce solutions with digital signatures and certificates
- ... to establish a worldwide bridge of trust and interoperability between the different spot solutions of the participants
- ... to offer a pragmatic way for a solid, cost-effective and forward-looking solution

Trust based networking of security infrastructures

⇒ **supplies with an added value (network effect)**

⇒ **helps in the investment protection of existing solutions!**



Basic Requirements

- Interoperability of Services and Applications
- Stability of the Policies on a comparable level
- Acceptance with the business process holders and with the users

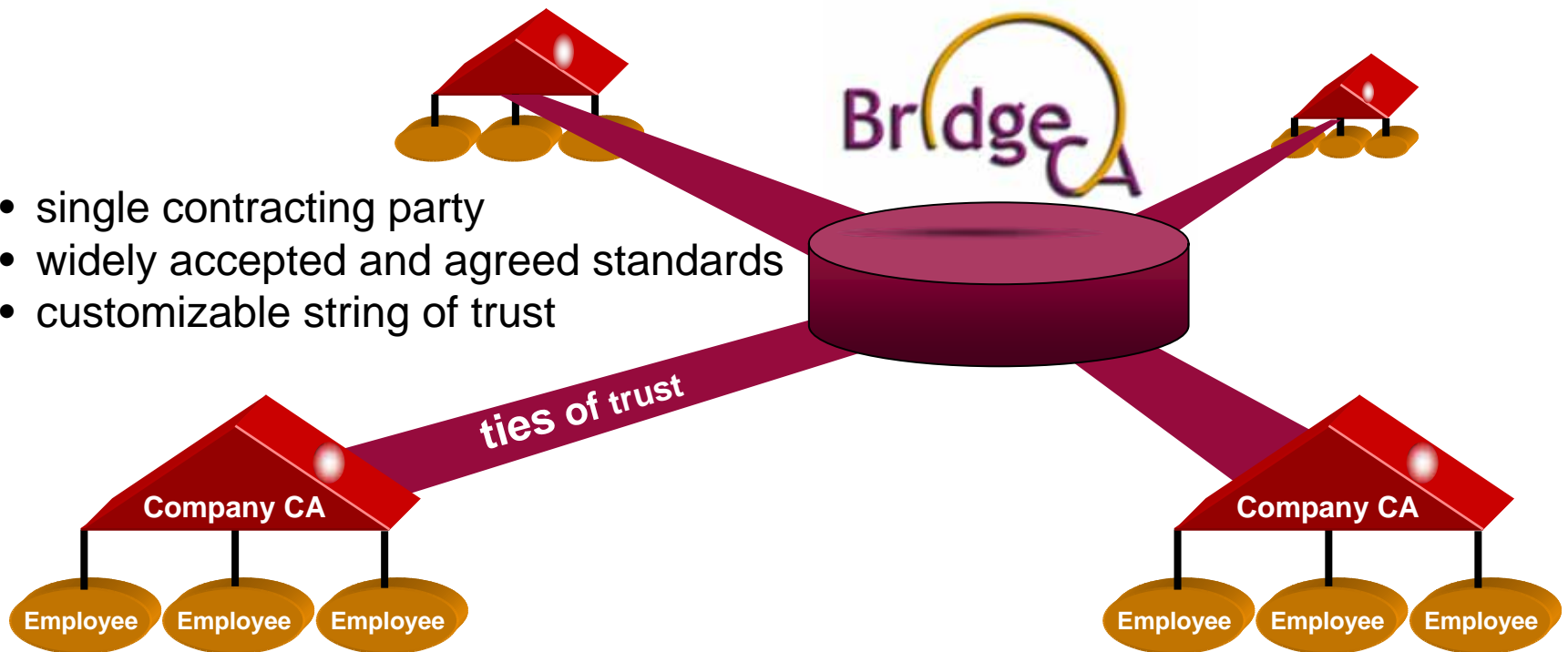
Additional success factors:

- The EB CA is a Network of PKI Operators
- Certification Services and the application of certificates are optimized together



The European Bridge-CA is a non-hierarchical, 1:n peer-to-peer “hub”

- single contracting party
- widely accepted and agreed standards
- customizable string of trust





Lessons learned

- Try to understand the needs of the different markets, but take care about „specific requirements“ which are proprietary.
- Don´t discuss the legal aspects too much, you can´t find a 100 percent solution! (not even 85 %, also in „real life“)
- Public-Private-Partnership is not the easiest, but the most effective way of Teamwork.
- Trust establishing needs a step-by-step turn over strategy
- The ‚take-off‘ of signatures (and Identity Management) in PKI-applications needs the business case.





Currently participating & interested parties



Deutsche Telekom



Daimler Chrysler

Austria Telekom Control



T-Online



SAP



Siemens



D-Trust



Giesecke & Devrient



Utimaco



TC TrustCenter



Secude



German Savings Bank Organization

Microsoft Germany



Deutsche Bank

Deutsche Bundesbank



German Information Security Agency (GISA) for the eGov Infrastructure

Allianz Versicherung





Contacts for the project

www.bridge-ca.org

www.isis-mtt.org

- **TeleTrust: www.teletrust.de**
Mr. Prof. Helmut Reimer, TeleTrust e.V.
Managing Director; Helmut.Reimer@teletrust.de
- **ISIS-MTT Project management and public relations:**
Mr. Fiedler, Nimbus Network; Arno.Fiedler@teletrust.de
- **European Bridge-CA Project management:**
Mr. Steiert, TeleTrust e. V.; info@bridge-ca.org

