TeleTrusT – IT Security Association Germany

TeleTrusT EBCA
European Bridge Certificate Authority

Overview
TeleTrusT – IT Security Association Germany

Introduction to TeleTrusT EBCA

- Since 2001
- Consolidation of individual, equal PKIs in a PKI network of trust
  - simple, secure email communication & data exchange via Internet
    - with signature, encryption and verification
- Network of
  - Enterprises
  - Institutions
  - public authorities
- Requirements
  - individual Public Key Infrastructure (PKI) with X.509 certificates
  - S/MIME emails
  - Policy
  - Interoperability test
- Only one contract partner is necessary (the EBCA), which services are available for all members
Selection of associated participants

- BSI
- Deutsche Bank
- Deutsche Bundesbank
- Fiducia & GAD IT
- E.ON Business Services
- Unify
- Siemens
Why Bridge CA? Starting situation

PKI islands

Advantages and disadvantages

+ secure in-house communication between staff, partners and clients

— insecure communication between various enterprises and public authorities
Why Bridge CA? Development

Individual PKI network

Network of trust, disadvantages

- Complex and uneconomic administration
- Missing common standards
- Multiple (n:n) contractual stipulations as well as deviating contracts and agreements
Why European Bridge CA? That’s why!

**Mediator for equal-ranking PKIs**

+ only one contract partner (1:n-relation)
+ common Minimum Policy
+ appointed and implemented international standards
+ individual PKIs are the company’s responsibility
+ Made-to-measure chain of trust
+ Directory/Validation service
Distribution of certificates via the EBCA

1. Certificate Trust List for the distribution of Root-/CA-certificates

2. Bridge LDAP Directory Service for the distribution of user certificates
How can I join the EBCA?

Registration process
1. Registration, verification
2. Interoperability test
3. Registration, distribution of the Root Certificate
4. Signed Certificate Trust List (CTL)
5. User certificates
6. Signed, encrypted email
Benefits for participants

- **Investment protection**: existing PKI can be utilized beyond corporate boundaries
- **Flexibility**: Software as well as hardware-based certificates are valid
- **Exchange of experience**: Exchange of knowledge between participants in various boards
- **Network effect**: Benefits increase with the number of participants
- **Innovations**: Utilization and development of standards for cross-organization secure communication
Are you interested?  
Contact us!

Your contact with TeleTrusT – IT Security Association Germany

Marieke Petersohn  
Martin Fuhrmann  
Project Coordinators  
Chausseestrasse 17  
10115 Berlin  
GERMANY

info@ebca.de  
Phone: +49 30 4005 4308  
Fax: +49 30 4005 4311  
http://www.teletrust.de/en/
EBCA Reference architecture (Email)

Participant X
- Client PCs
- PKI System
- Certificate directory
- LDAP Proxy

Participant Y
- Client PCs
- PKI System
- Certificate directory
- LDAP Proxy

Participant Z
- PKI System
- Certificate directory
- Email Gateway

EBCA participants can issue user certificates directly on the EBCA Directory Service (instead of operating their own directory service).

Internet
- Automated download via LDAP or manually via HTTP

Manual download via HTTP or automated via LDAP (or HTTP)

"Third parties" (Other organizations, individual user)
- Certificate download from EBCA Directory Service
- Certificate provisioning with EBCA Directory Service

LDAP Proxy

TeleTrusT EBCA
European Bridge Certificate Authority

Directory Service