SIEMENS

TeleTrusT
Pioneers in IT security.

TeleTrusT European Bridge CA – Status and Outlook

TeleTrusT Workshop, Saarbrücken, 2010-06-11

Dr. Guido von der Heidt, Siemens AG

Secure (E-Mail) Communication across Organizations – The Obstacles

- Existence and Use of Public Key Infrastructures (PKI)
  - ➔ Disposability and/or provision of digital certificates
- Interoperability
  - ➔ Interoperability of secure communication systems and PKI solutions
- Trust
  - ➔ Acceptance of security policies and operational practices
- Infrastructure
  - ➔ Access to and validation of digital certificates
- Know-How
  - ➔ Know-how and support to establish secure communications between partners

Secure (E-Mail) Communication across Organizations – Where the European Bridge CA comes in

- Existence and Use of Public Key Infrastructures (PKI)
  - ➔ Private PKIs of large enterprises and organizations, public PKIs and certificate services of Trust Centers

- Interoperability
  - ➔ Secure e-mail (S/MIME) and PKI standards (PKIX)
- Trust
  - ➔ Often no trust between organizations established; still no simple standard processes available
- Infrastructure
  - ➔ Public infrastructures for accessing and validating digital certificates still not developed
- Know-How
  - ➔ (Small and medium) Organizations often lack know-how in setting up secure communication with partners

Members of the European Bridge CA (EBCA)

Member PKIs

- Deutsche Bank
- German “PKI-1 der Verwaltung” represented by BSI
- Microsoft Deutschland
- Siemens
- Deutsche Bundesbank
- Landesbetrieb für Statistik und Kommunikationstechnologie Niedersachsen
- Signaturbündnis Niedersachsen
- Regulierungsbehörde Österreich (RTR)

Trust Centers

- TC Trust Center
- D-Trust

Associated Partners

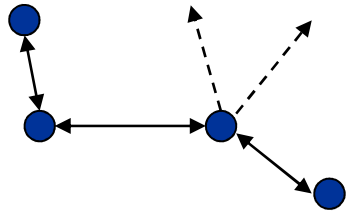
- Deutsche Telekom
- Daimler
- SAP

Trust – Trust Models

Trust

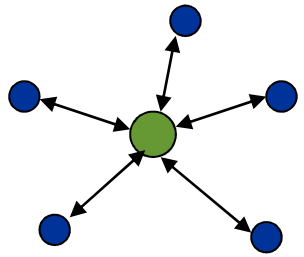
- Acceptance of Certificate Policies (CPs) and Certificate Practice Statements (CPS) of PKIs
- Ensuring root certificate validation across different IT infrastructures

Bilateral Trust



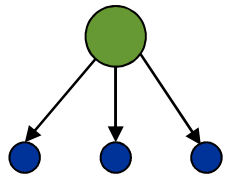
- Mutual agreements; manual exchange of root certificates
- Becomes quickly unwieldy with the number of partners

Bridge CA Models



- Trust community with Bridge CA as trust hub which establishes indirect trust between member PKIs
- Bridge CA defines policy requirements for member PKIs
- Managing “Certificate Trust Lists” of member root certificates
- Cross-certification of member PKIs with Bridge-CA

Hierarchical PKIs



- Members PKIs sub-ordinated to a common Root CA or
- Members have to comply with CP of the Root
- Simple certificate validation through distribution of only one Root CA

Trust – Trust Model of the European Bridge CA (1)

Policy Conformance – “Seal of Quality”

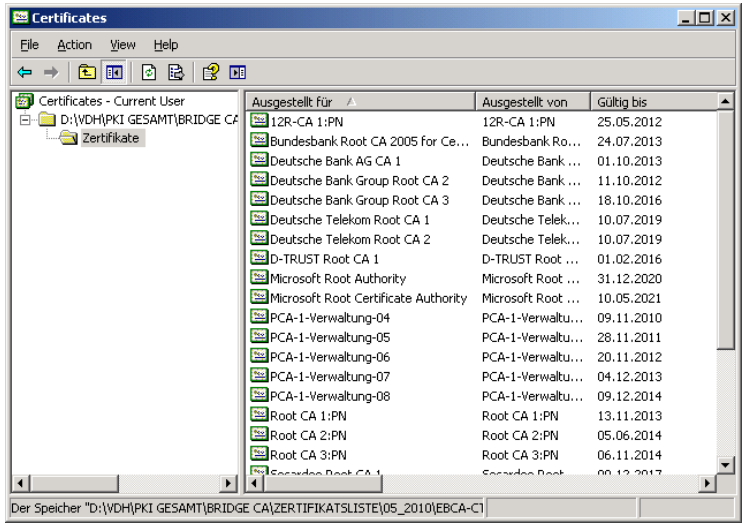
- Member PKIs must comply with the EBCA Certificate Policy
  - Based on the standard RFC 3647
  - Defines a minimum security standard which must be met by the PKIs of the EBCA members, i.e. for PKI operations, PKI processes and the security of the underlying system infrastructure.
- Thus, members and other organizations can trust EBCA members and rely on the security of their PKI systems.

Root Certificate Validation

a) Certificate Trust List

- Distribution of a “Certificate Trust List (CTL)” containing the root certificates of the member PKIs
  - Digitally signed PKCS#7 file
  - Members and/or partner organizations need to validate the CTL and to distribute the root certificates within their IT infrastructure.

➔ Solution is not suitable for end-users

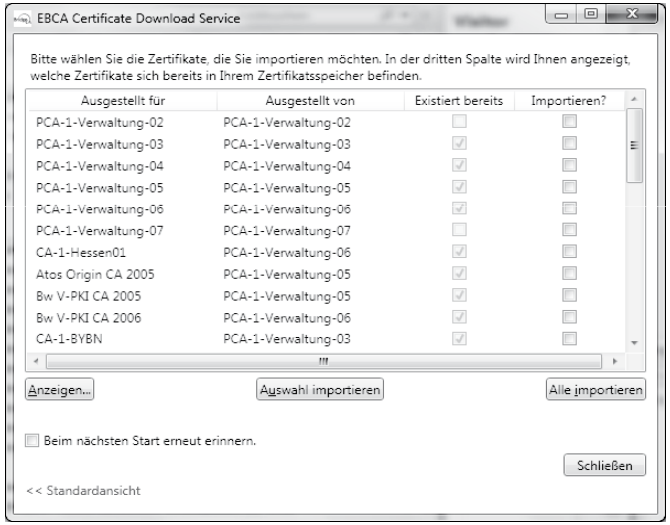


EBCA Certificate Trust List in PKCS#7 format

Trust – Trust Model of the European Bridge CA (2)

b) Certificate Download Service (CDS) – C*urrently being released*

- Provision of the EBCA CTL integrated with client SW tools which manage the validation of the CTL and the import of the root certificates in the respective client systems.
  - Addon for Mozilla Firefox / Thunderbird
  - Plugin for Microsoft Outlook
  - Joint development of BSI, EBCA and FH Gelsenkirchen
  - ➔ Simple solution for end-users as “update service”
  - ➔ Not suitable for large organizations since automated updates from Internet are usually not allowed

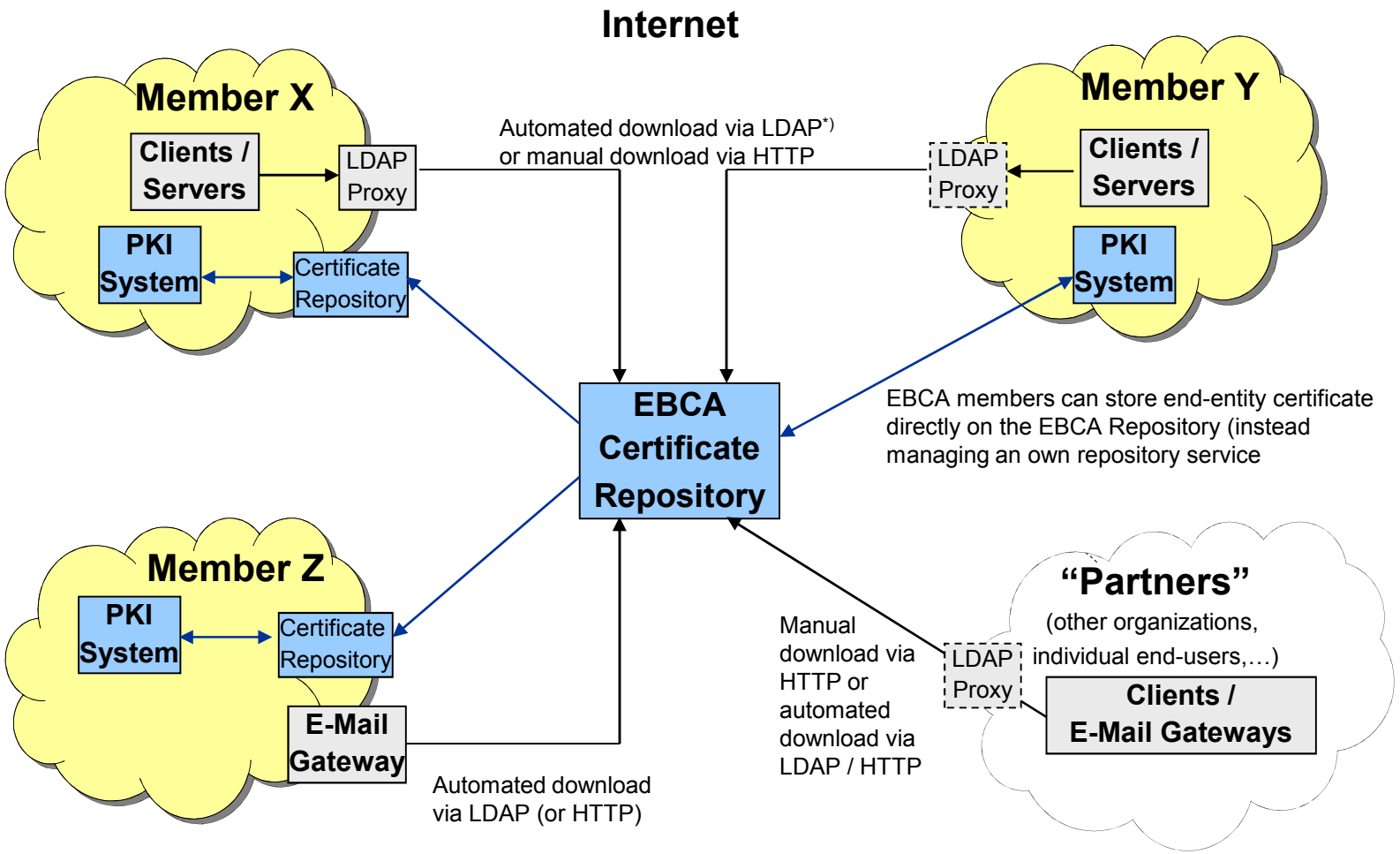


Certificate Download Service Addon for Mozilla

c) Cross-Certification – *For future discussion*

- The EBCA <u>does not provide</u> cross-certification services as other Bridge-CAs (e.g. US 4 Bridges Forum)
- In bilateral scenarios all end-entity chain up to each member root. This causes chain validation problems due to multiple validation paths and path lengths.
- EBCA investigated a root-signing model in which member CAs are unilaterally cross-signed by common EBCA root integrated in current browsers and operating systems. However, this model was currently not realizable due to cost and legal reasons.

Infrastructure – A public Infrastructure for Access and Validation of Certificates provided by the EBCA



*) Lightweight Directory Access Protocol.

Infrastructure – Offerings of the EBCA and Issues

EBCA Offerings

- Public Certificate Directory service providing access to end-entity certificates of member PKIs via LDAP or HTTP.
  - Partners need only to configure the EBCA Certificate Directory as single certificate source.
- EBCA members
  - can connect own external Certificate Repositories to the EBCA Repository or
  - store their end-entity certificates directly on the EBCA Certificate Repository.
- The “Certificate Store” function of the EBCA Certificates Repository provides a simple and affordable solution for organizations not having an own external directory service.

(Technical) Issues

- In many cases organizations do not allow LDAP access to the Internet form their Intranets. Thus, LDAP proxy solutions are to be set-up in order to allow automated certificate download from client or server systems.
- Validation of external Certificate Revocation Lists (CRLs) from partners might also require proxy solutions.
- Not all EBCA members publish their end-entity certificates externally (by policy reasons).

Infrastructure – The EBCA Certificate Repository
Web-Interface for manual Certificate Download

Know-How – Offerings of the EBCA

- Organizations often lack of know-how in setting up secure communication with partners
  - Meaning and establishing of trust
  - Management of root certificates
  - Provision of own certificates and access to the partner's certificates
  - Set-up and configuration of the IT infrastructure to support secure communication with partners
  - ➔ Insufficient know-how on solutions provided by he European Bridge CA (and other Trust Communities)
- The EBCA Board and the EBCA Technical Work Group provide platforms for information exchange and best practice sharing
  - The Board consists of the full members of the EBCA
  - The Technical Work Group is open for all Teletrust members and guests
- EBCA documentation – *currently being updated*
  - Web-site
  - Flyer
  - Process documentation

Outlook and Objectives

- Start operation of Certificate Download Service
- Update of EBCA documentation
  - Update of web-site and flyer
  - Development of user guide(s)
- Increase usage of EBCA offerings
  - Motivate members to publish their end-entity certificates (in EBCA Certificate Repository)
- Increase of marketing activities
- **Gain new members for the EBCA**
  - ➔ Prerequisite for widening of activities
- Identify further needs and fields of activity (e.g. authentication, digital signature schemes, Trust in federation scenarios,…)
- Continue discussion on cross-signing services

Outlook – New/Potential Members

New Member in 2010:

E.ON IS GmbH

Potential Members:

Siemens Enterprise Communications GmbH & Co. KG