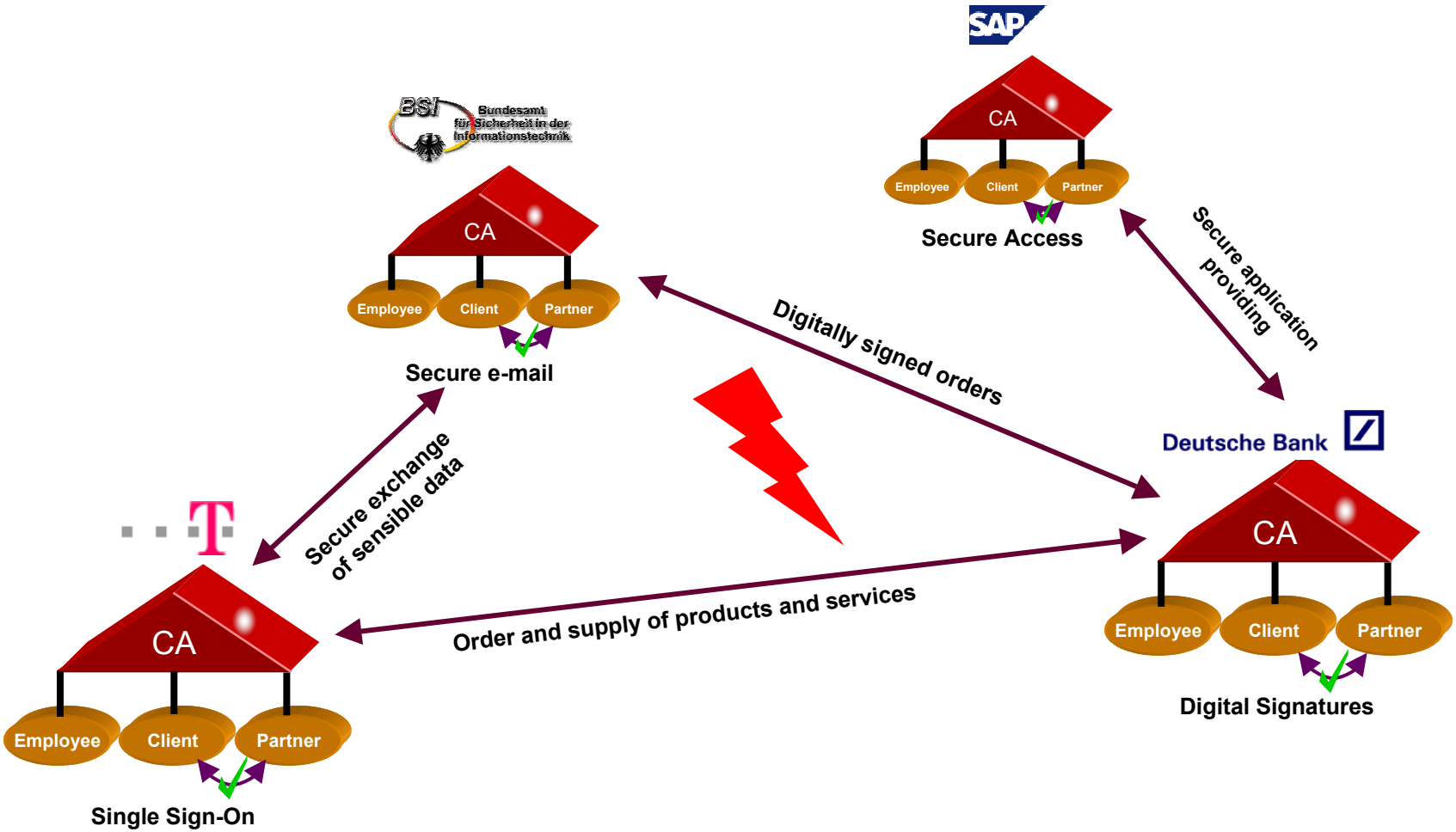
Making PKI a Reality: The European Bridge-CA and ISIS-MTT

Arno Fiedler
Projectmanager ISIS-MTT

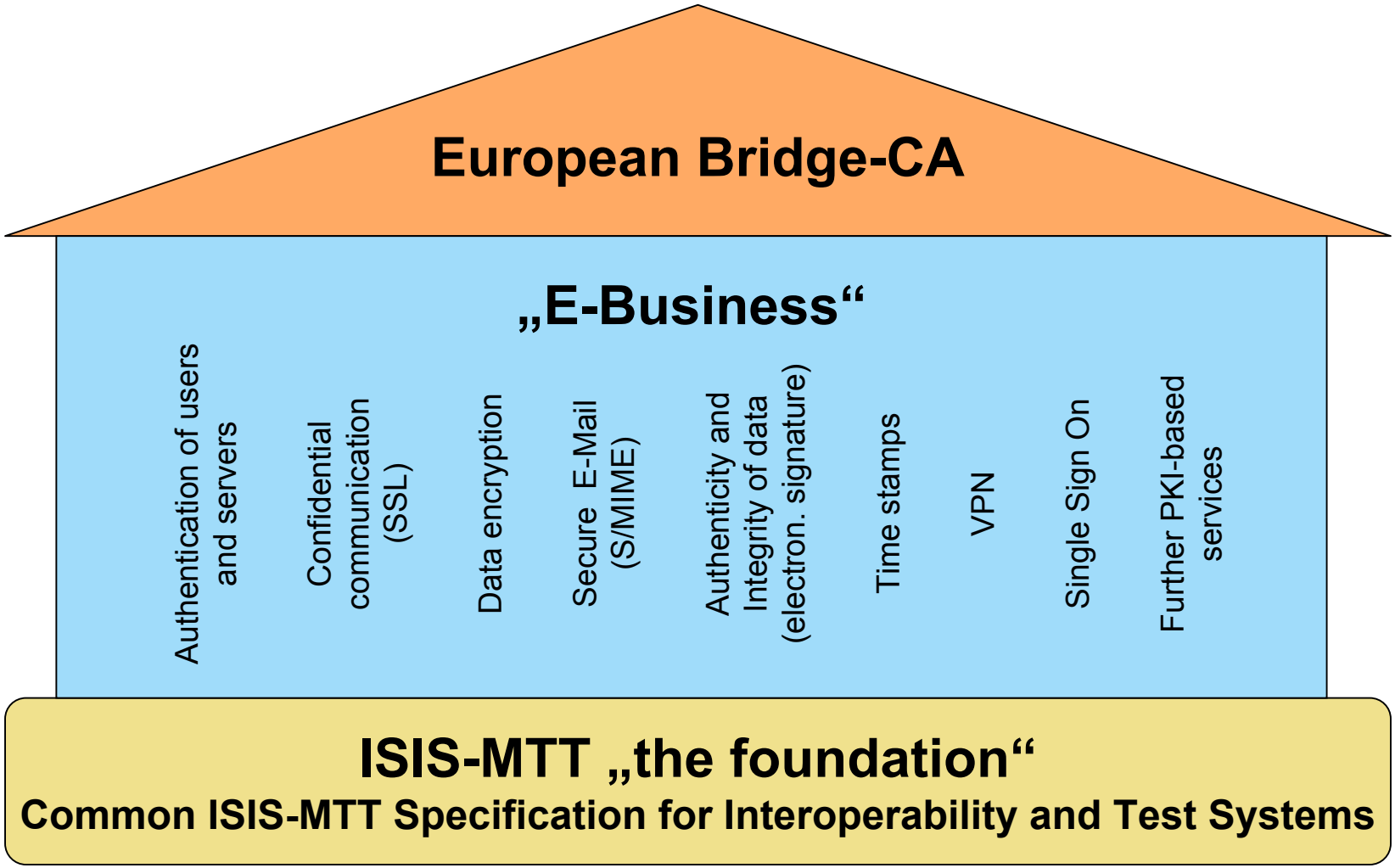
Agenda

- The starting point
- The concept
- The experience
- The comprehensive strategy
- ISIS/MTT
- The contact

The starting point: PKI Islands

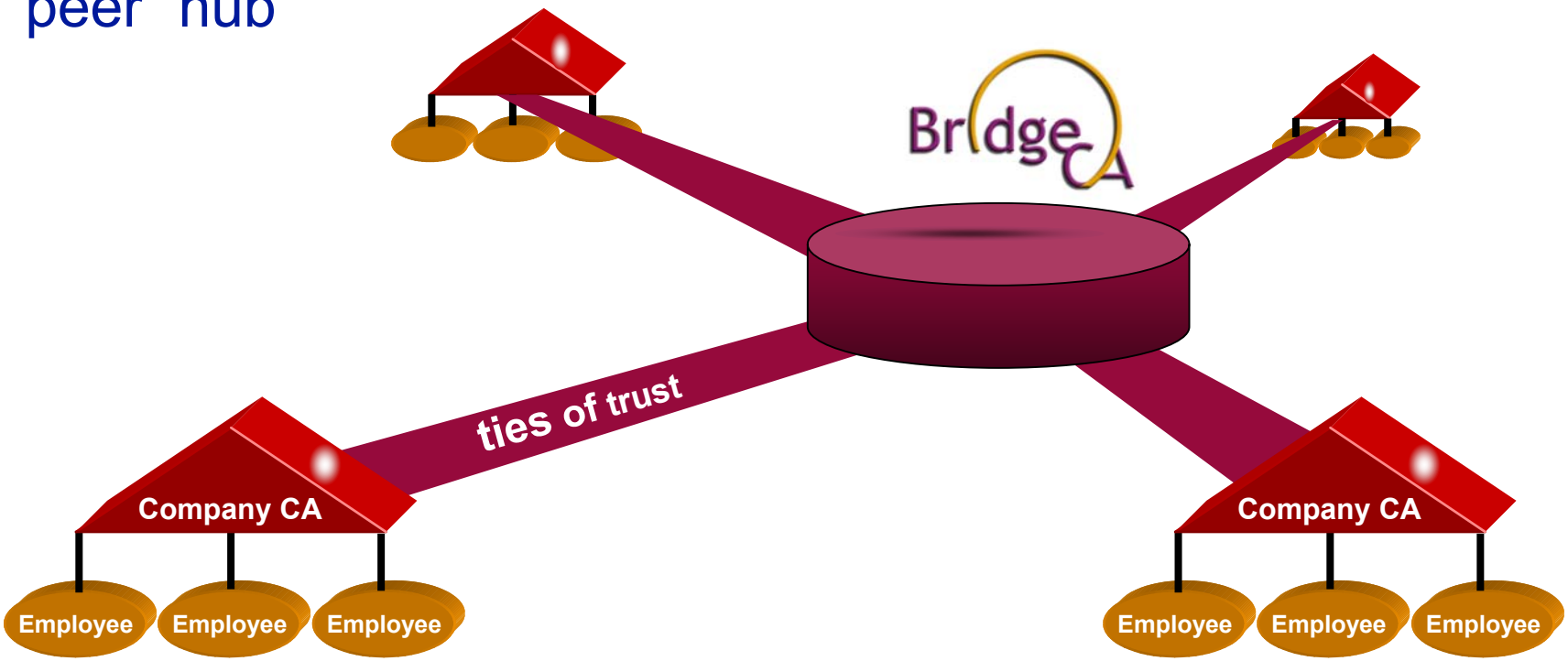


European Bridge-CA in the ISIS-MTT framework



The concept of the European Bridge-CA

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



The European Bridge-CA approach is

- **pragmatic**, because it allows the companies to stay in full control of their data and saves already made investments
- **cost efficient**, because existing PKI islands can be linked and uneconomical administration (n:n cross certification) can be avoided
- **forward-looking**, because it is based on well-established standards
- **secure**, because an adequate level of security is guaranteed

The strength of the bridge CA approach is that is provides interoperability of PKIs and a progress in security with minimal effort.

Philosophy of the European Bridge-CA

Include as many major companies and public authorities as possible (launched at CeBit 2000, learn from others)

- Private companies




- Public authorities

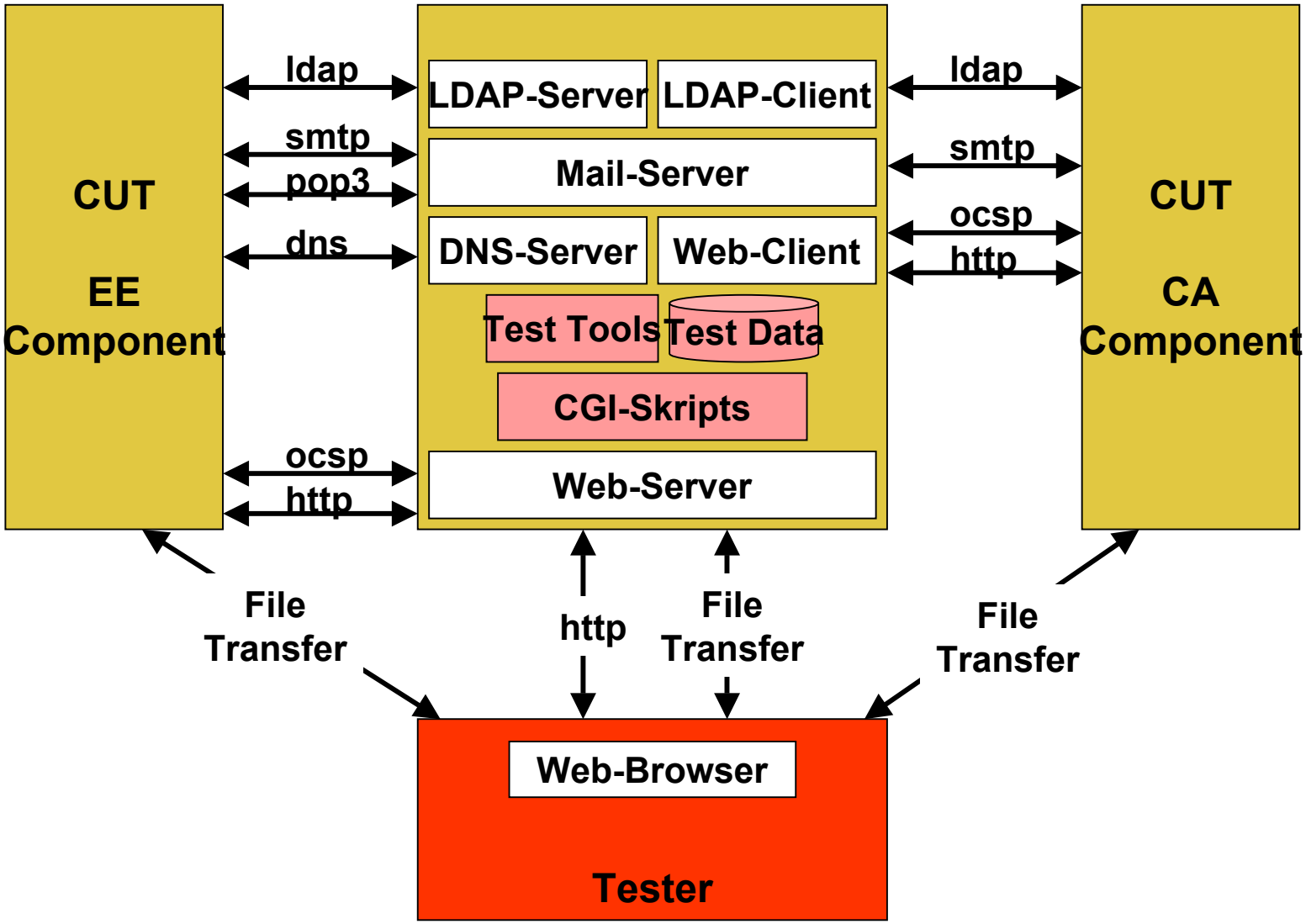
The more participants the European Bridge-CA has, the more benefit it can provide to its members.

More information: www.teletrust.de / www.bridge-ca.org

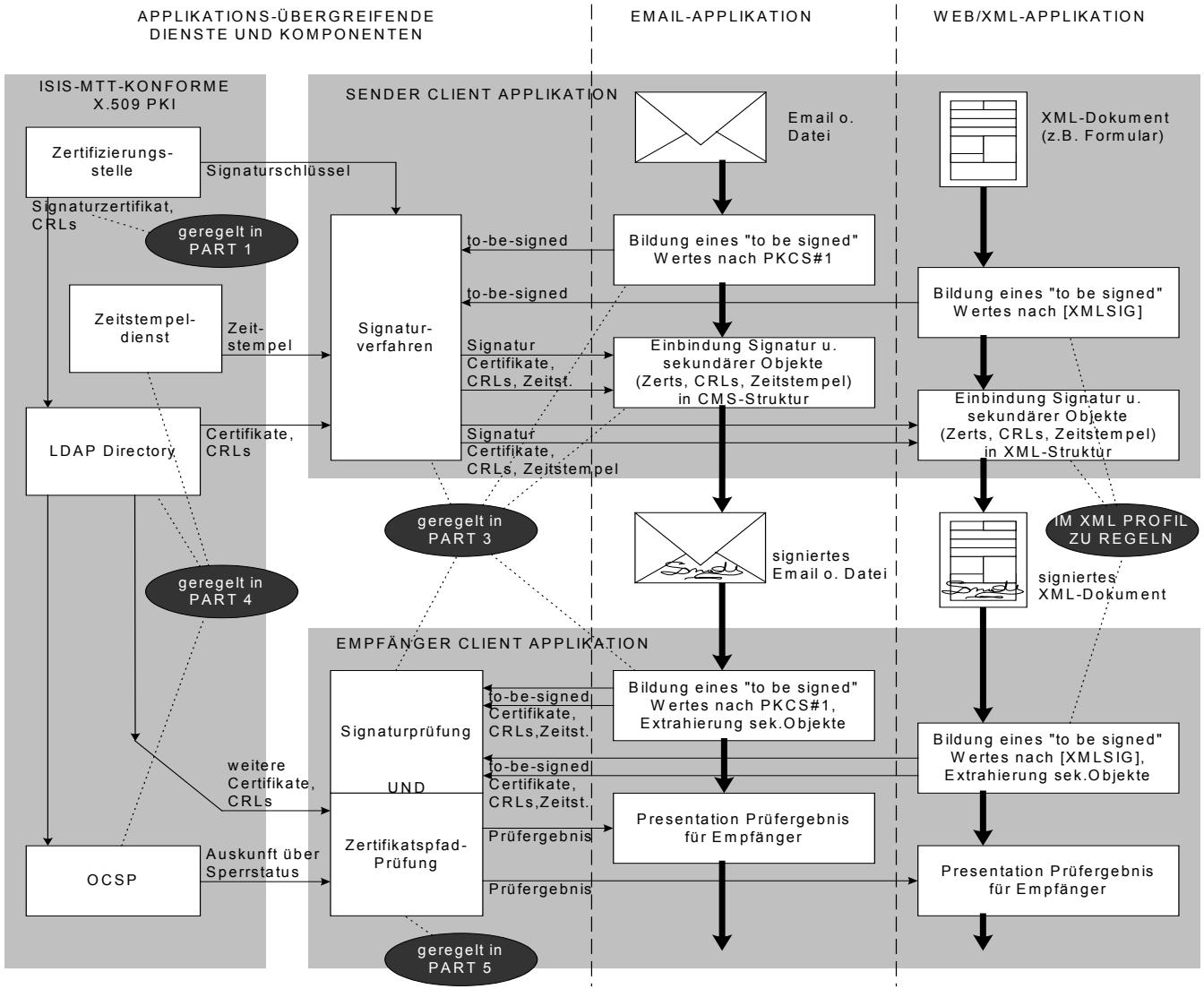
ISIS-MTT- behind the cover

#	Object	Content of the ISIS-MTT-Core-Profile
1	Certificate Profile	**Standard X.509 V3; Qualified Certs According ETSI QCP (RFC 3039) Attributes allowed in Key Certificates**
1.3	Attribut Certificate	**Standard X.509 V2**
1.4	CRL	**Standard CRL (including Delta CRL)**
2	PKI Management	**Simple PKI-Management as in CMC**
3	S/MIME	**Subset of S/MIME for mail**
4.2	LDAP	**Standard LDAP V.3, no restrictions to DIT**
4.3	OCSP	**Standard OCSP Optional extension for positive statement**
4.4	TSP	**Standard TSP, no profiling yet**
5	Cert.Path Validation	**Standard PKIX procedures**
6	Algorithms etc	**Look at: www.teletrust.de**
7	PKCS#11	**Profile**

Testbed Prototype Platform



Concept for XML-Integration



Core theses for ISIS-MTT

- ISIS-MTT is a free-of-charge offer of PKI integration to all applications developers.
- ISIS-MTT is internationally aligned, existing standards are used an extended
- ISIS-MTT defines a complete security architecture: encryption, authentication and signing.
- ISIS-MTT provides different security levels;
  legal binding according to German signature law is just an option.
- ISIS-MTT interoperability criteria are publicly defined and provable through a test bed.

Contact

Bernhard Esslinger
Head of Information Security
Corporate IT Office
Deutsche Bank AG
e-mail: bernhard.esslinger@db.com

Arno Fiedler
Projectmanager ISIS-MTT
e-mail: arno.fiedler@teletrust.de

Bernd Kowalski
Head of Certification
Dep.Federal Office
for Information Security – BSI
e-mail: bernd.kowalski@bsi.bund.de