

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



Arno Fiedler
Projectmanager ISIS-MTT

Agenda

- The starting point

- The concept

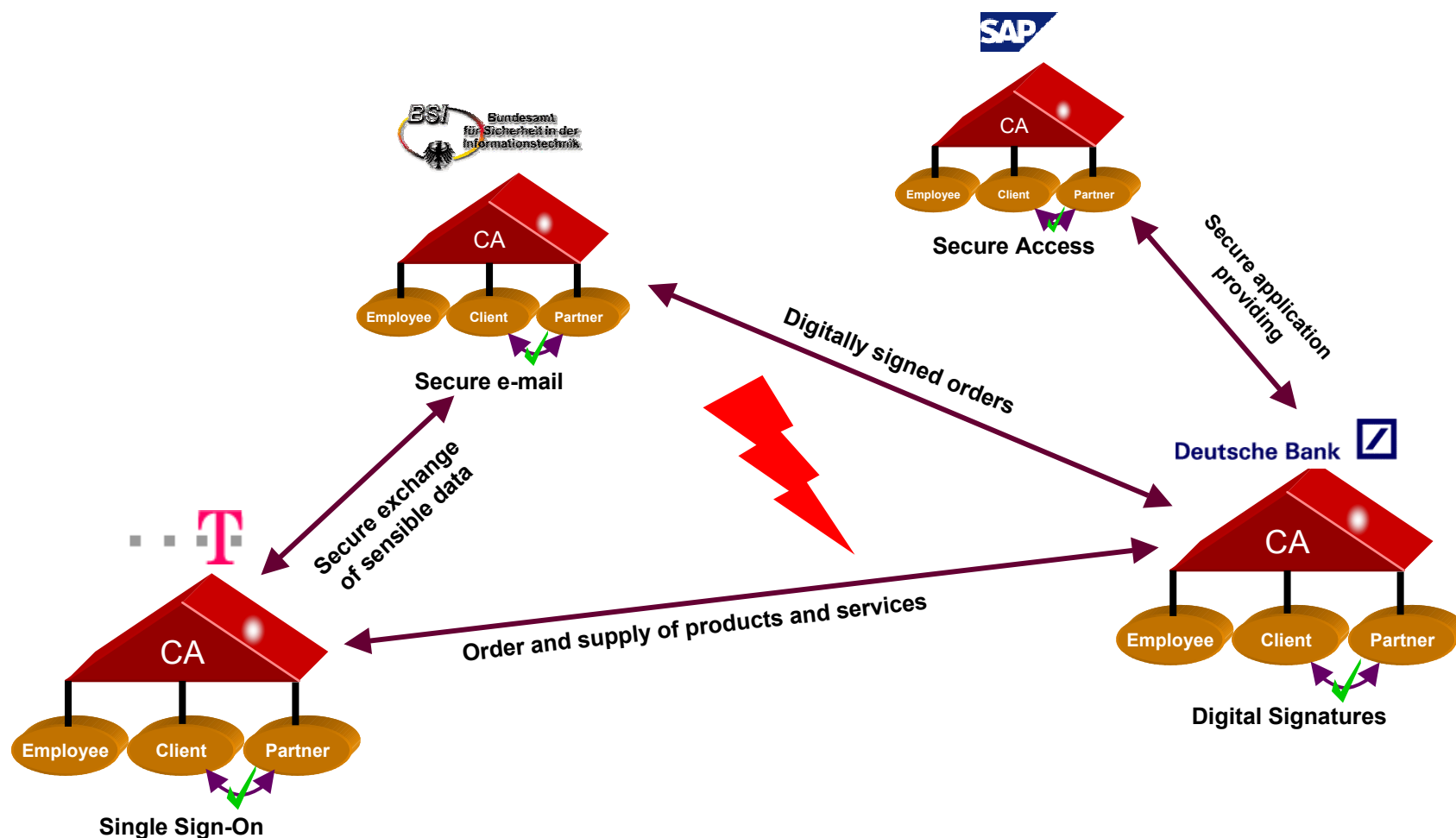
- The experience

- The comprehensive strategy

- ISIS/MTT

- The contact

The starting point: PKI Islands



The starting point

- Many organizations built up their own PKI (islands) or simply wait
- These PKI islands are not sufficiently linked
- There is a lack in interoperability

But the benefit of an infrastructure like a PKI increases (more than linear) with the number of users.

Thus, one should link up the existing PKIs, but

- neither hierarchic (companies will not accept a superior CA)
- nor with a n:n cross certification (too much effort)

Agenda

- The starting point

- The concept

- The experience

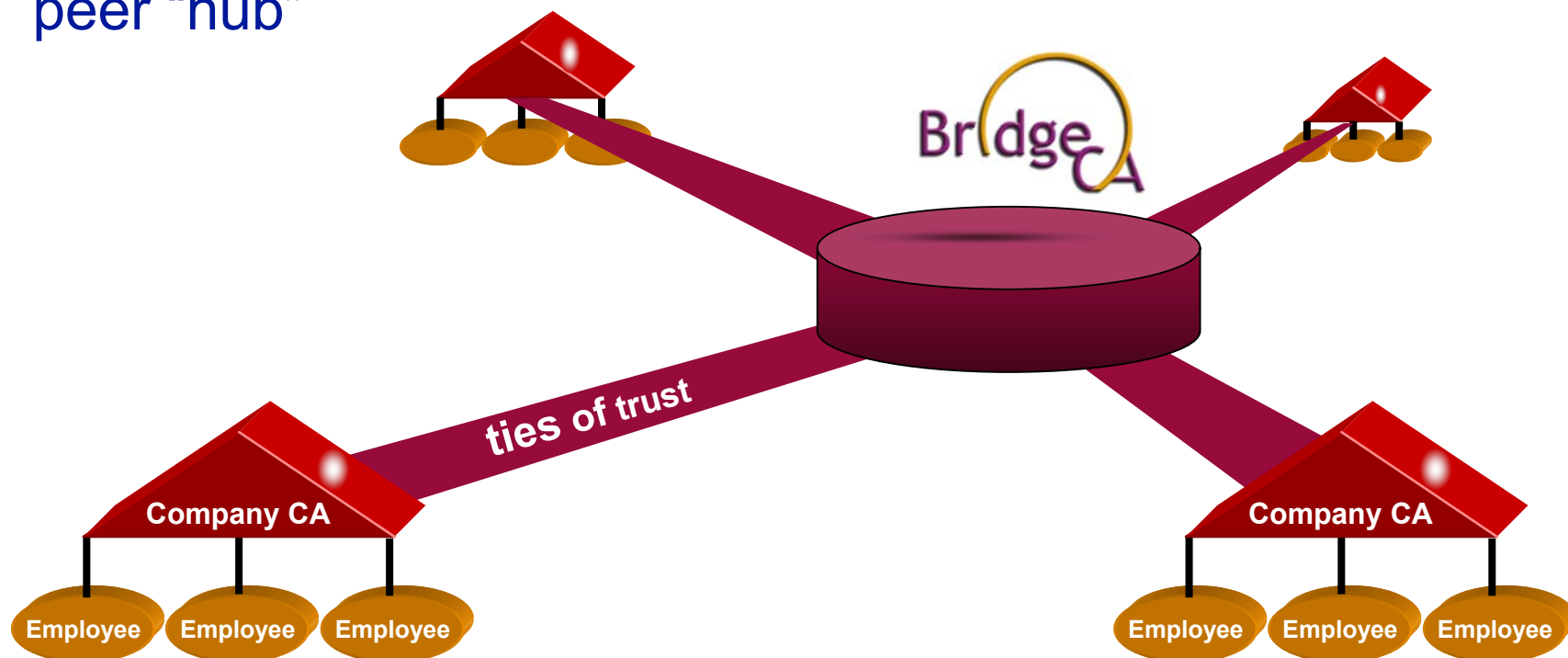
- The comprehensive strategy

- ISIS/MTT

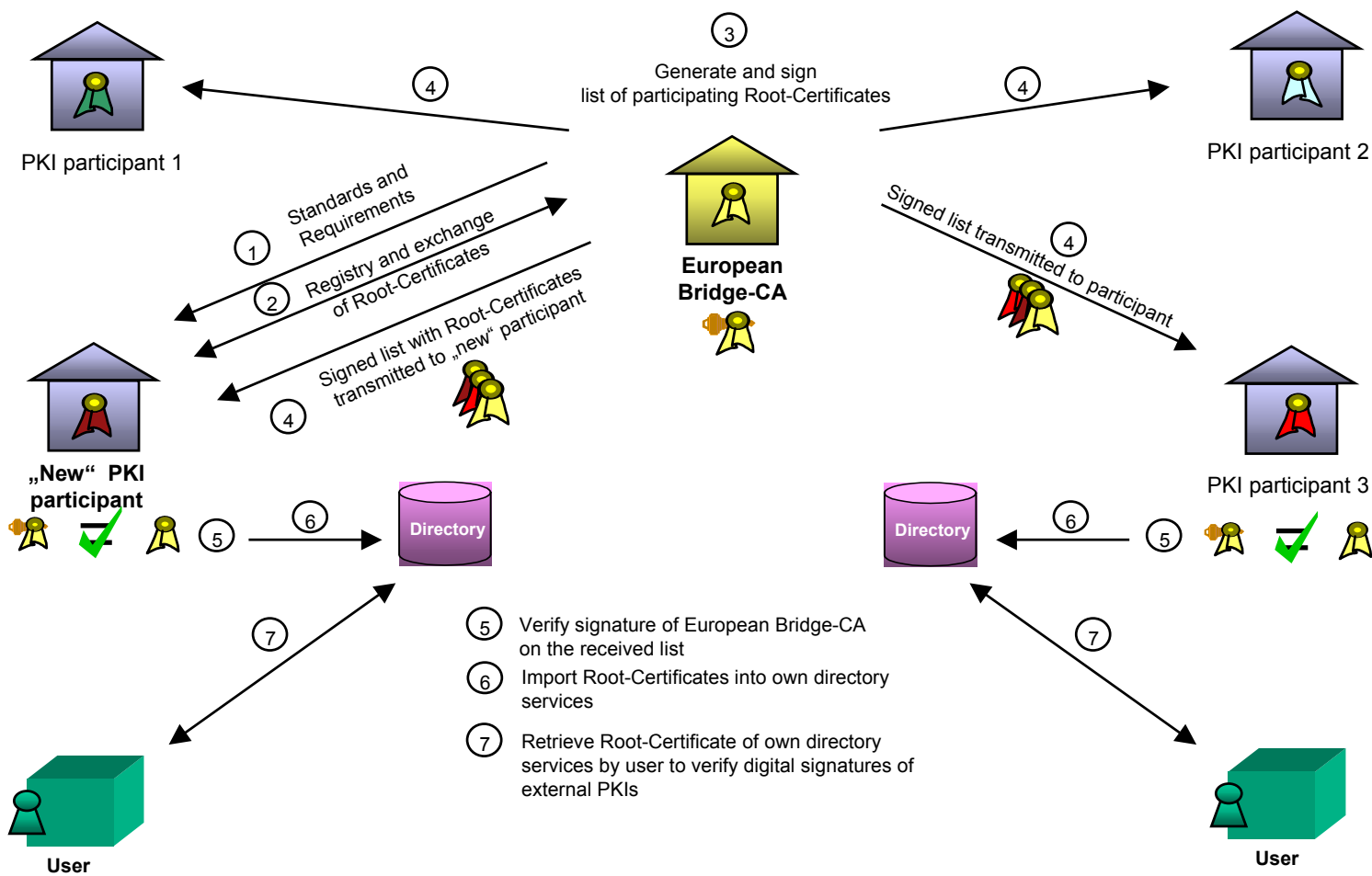
- The contact

The concept of the European Bridge-CA

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



Basic functionality



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 it 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

Agenda

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

Elements of interoperability of some participants

Organisation	E-Mail Client	S/MIME Solution (native e-mail client or with Plug-in)	CA-Products
BMW AG	Netscape Messenger 4.72	native	TC TrustCenter
Deutsche Bank AG *	Lotus Notes 4.5/4.6	Lotus MailProtect 1.3.4 a	TC TrustCenter (Produktion) SECUDE CA (Test, Development)
Deutsche Telekom AG	MS Outlook 98	SECUDE AuthentEmail (customized)	Cybertrust CA
Dresdner Bank AG	MS Outlook 2000	native	Netscape/Baltimore
Secartis AG	MS Outlook 98	G&D TrustedMail	GDTrust CA
Siemens AG	MS Outlook 98	SSE TrustedMime	Trusted CA
TC Trust Center GmbH	Netscape Messenger 4.76	native	TC TrustCenter
Cable & Wireless	MS Outlook 2000	Baltimore SecureMail	Baltimore

Interoperability demonstrated via exchange of signed and signed/encrypted S/MIME messages.

* From 12/2002 on S/MIME is available for all Deutsche Bank employees using an S/MIME gateway and an internal PKI.

Agenda

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

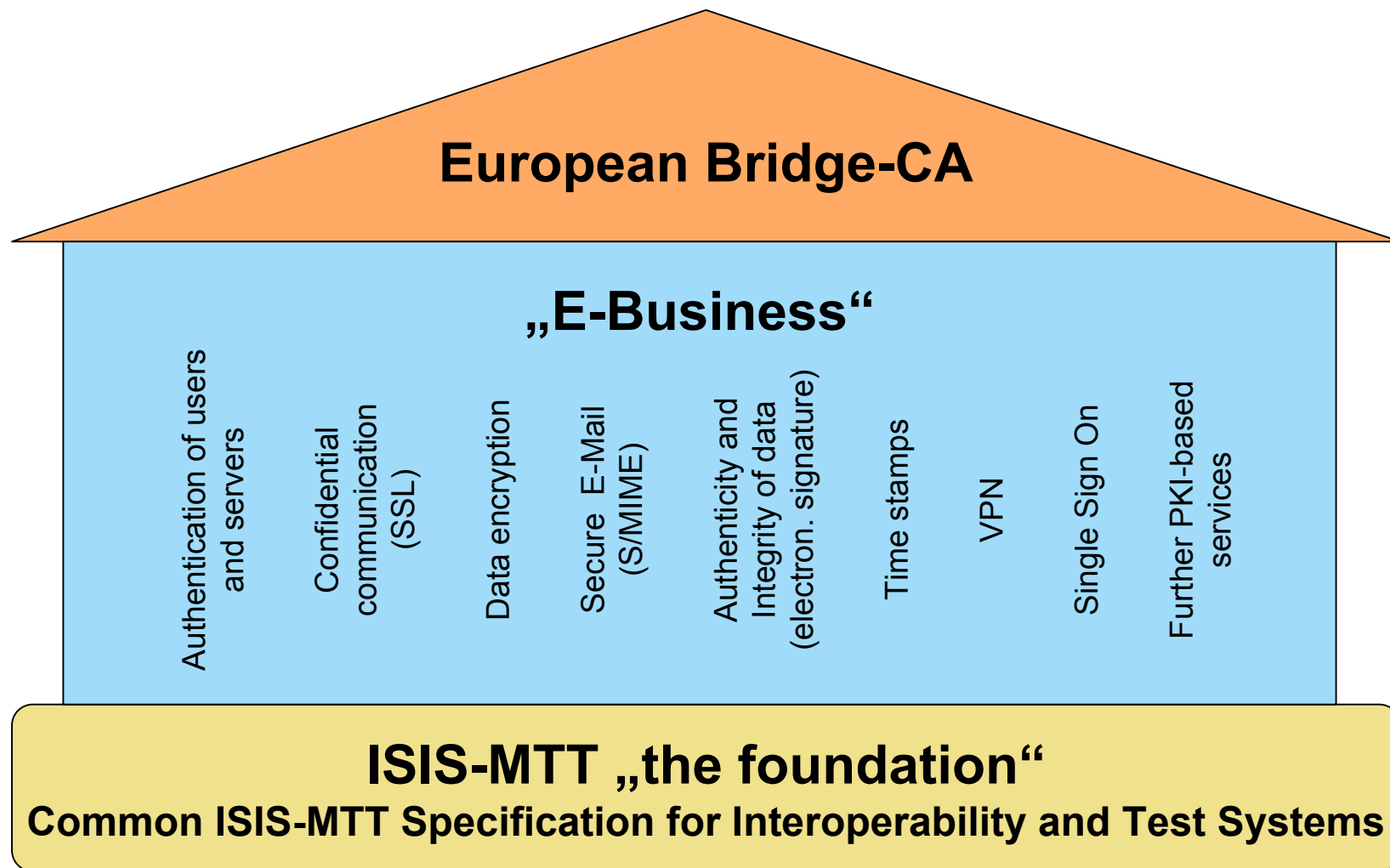
The comprehensive strategy

The Bridge-CA initiative should be part of

- the security strategy of each organization
(and linked with, other security measures)
- a public-private partnership
- a larger security framework

The Bridge-CA is not a stand-alone solution. In order to be effective, it is linked with other security measures.

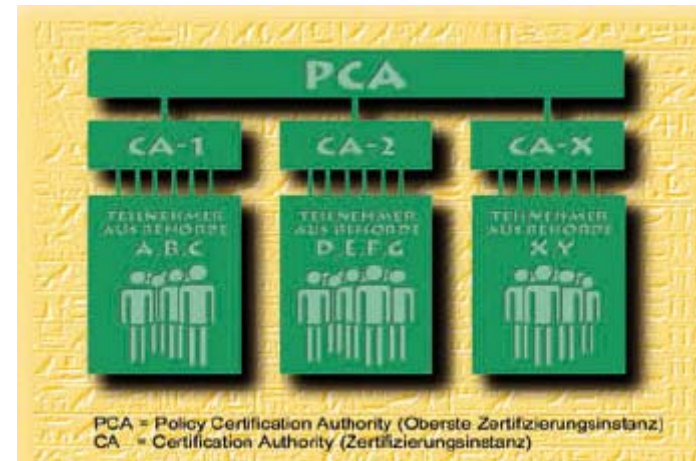
European Bridge-CA in the ISIS-MTT framework



Partnerships (established)

The Bridge-CA initiative uses experiences with

- ISIS/MTT (joint testing environment)
- international standardization efforts (Core part of ISIS/MTT)
- Sphinx project of BSI (interoperability of S/MIME mailers)



... and of course we would very much appreciate if more companies join the European Bridge-CA

... any new partnership that could be established, is appreciated: for example with the EU project IDA, the Japanese Bridge-CA or Boeing

The European Bridge-CA, 2002/10/02 · page 16

Agenda

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

TeleTrust Project - ISIS-MTT

Common ISIS-MTT Specification for Interoperability and Test Systems

Joint project of more than 40 leading companies and organizations to create a widely accepted synthesis of existing international standards for electronic signatures, encryption and authentication.

The aim is to ensure the unrestricted interoperability between applications including those with different security requirements.

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 application developers to prove their ISIS-MTT interoperability.
- Investment protection for users because of exchange-ability of single components.

ISIS-MTT document structure:

- Part 1: Certificate and CRL Profiles,
- Part 2: PKI Management,
- Part 3: Message Formats,
- Part 4: Operational Protocols,
- Part 5: Certificate Path Validation,
- Part 6: Cryptographic Algorithms,
- Part 7: Cryptographic Token Interface,

- Profile: SigG-conforming Systems and Applications
- Profile: Optional Enhancements to the SigG-Profile.

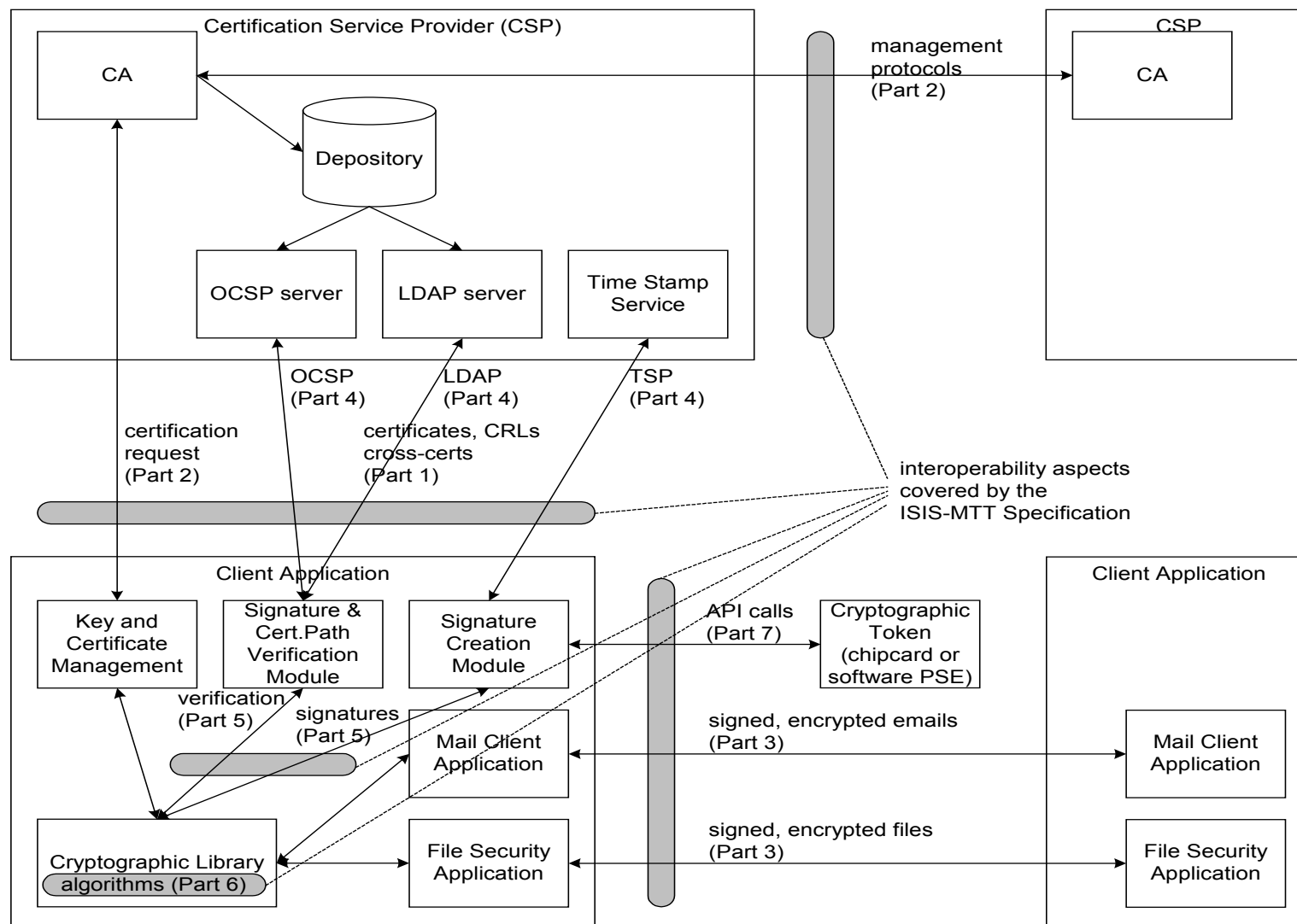
C
O
R
E
-
S
P
E
C

O
P
T
I
O
N

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

ISIS-MTT and the Infrastructure



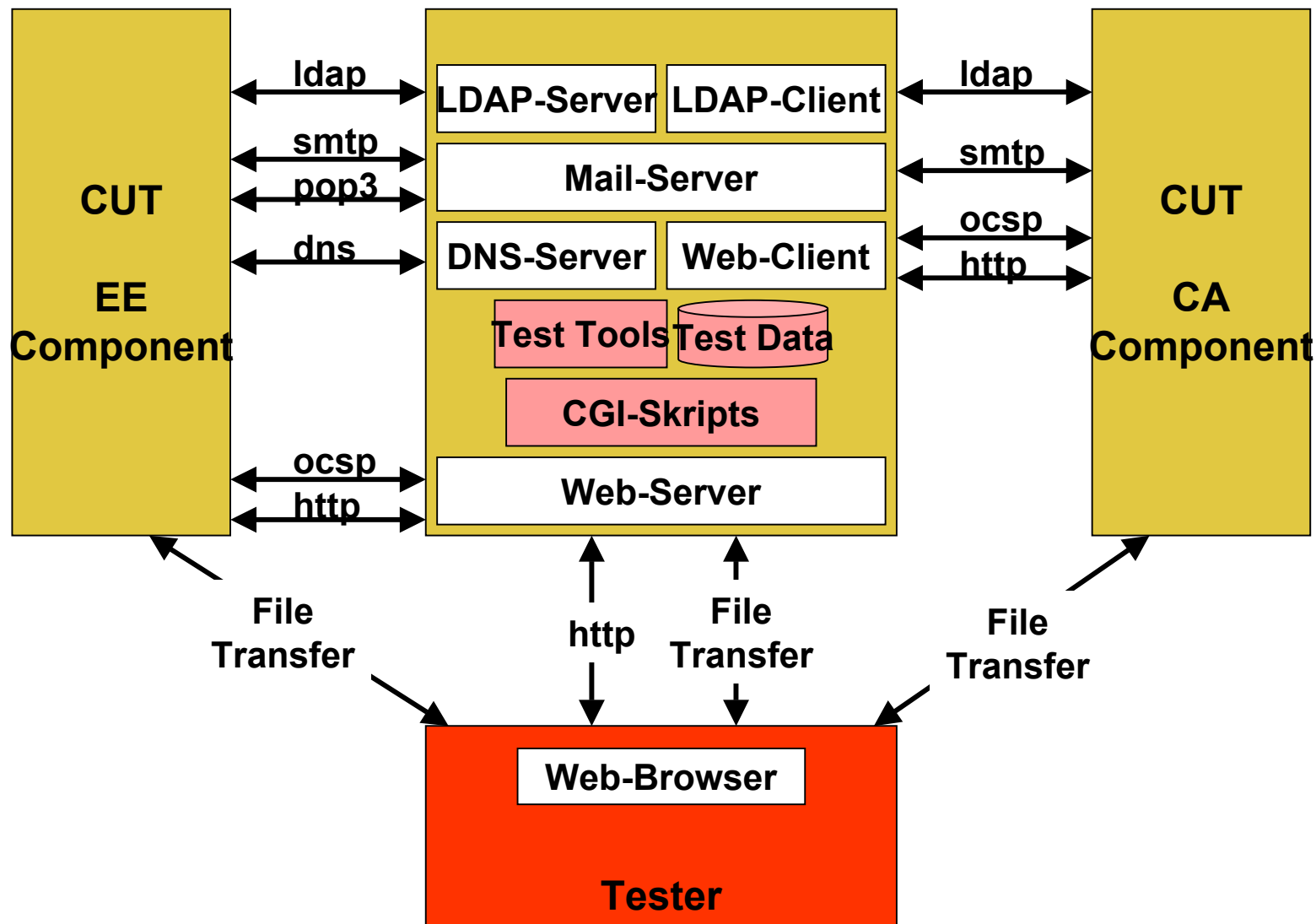
Actions in progress 2002

- Development of a usable test bed for realistic tests of applications and services.
- Award of a “Quality Seal” for applications with proven interoperability.
- Further development of ISIS-MTT specification.
- Further contribution of the specification to international standardization.
- Strengthening of public relations and project management.
- Development of an XML profile based on W3C and ETSI

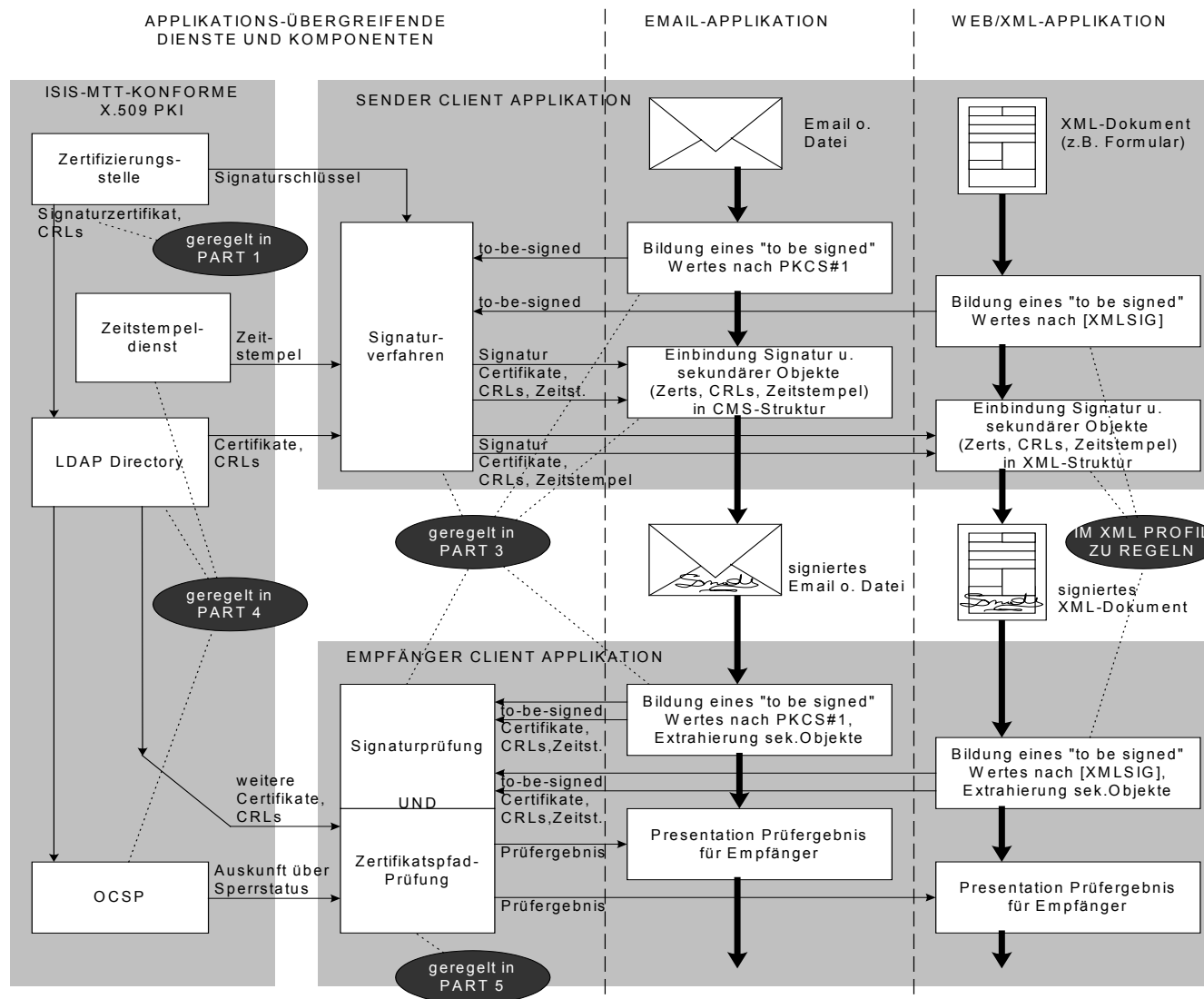
Benefits of the project

- Interoperability at application level increases acceptance of signature, encryption and authentication products in E-government and E-commerce.
- Interoperability is an investment incentive for applications developers and ensures portability of applications.
- Interoperability provides choice of services and products for the users and could possibly save costs (e.g. Media@Komm).

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 and 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.

Currently participating & interested parties



Deutsche Telekom



Deutsche Bank & Deutsche Bank 24



T-Online



Siemens



Giesecke & Devrient



TC TrustCenter



German Savings Bank Organization



German Information Security Agency (GISA)



Daimler Chrysler



Dresdner Bank 



BMW 



SAP 



D-Trust 



Utimaco 



Secude 

Internationally we are talking to:

IBM, Microsoft, and others

ISIS-MTT-Lessons learned

- 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.
- To get a commitment for a profile like ISIS-MTT is hard work, lobbying doesn't work via e-mail.
- Try to understand the needs of the different markets, but beware of „specific requirements“ which are proprietary.
- Keep the project interesting, the work is never completed.
(Test bed, XML....)

More information: www.teletrust.de (available in German and English)

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

Besonderheiten im SigG-Profil

Verifikation nach dem Kettenmodell

- nicht konform zu PKIX und EESSI
- z.Zt. Prüfung auf SigG-Konformität des Schalenmodells

OCSP-Positivauskünfte im Kontext SigG

- erzwungen durch Anforderungen des deutschen Gesetzgebers (SigG §15)

Proprietäre Inhalte in optional Enhancements SigG

- RetrievelfAllowed, CertInDirSince, DateOfCertGen