



Informationstag 'Elektronische Signatur'

**Gemeinsame Veranstaltung
von TeleTrust und VOI**

Berlin, 24.09.2010

**Dipl. Wirtsch.-Ing. Arno Fiedler
Nimbus Technologieberatung GmbH**

**„Viele Standards sind der Signaturen Tod: Blicke durch
den Standardisierungsschlingel“**

- Signatur-Standardisierung betrifft immer mindestens drei Ebenen:
 - Herausgeber
 - Akteur/Inhaber
 - Vertrauende Instanz
- Signatur-Standardisierung unterscheidet sich grundsätzlich zwischen
 - Austauschdaten,
 - Bestandsdaten und
 - Archivdatenverwaltung.

- Offizielle Normungsgremien:
 - International: ISO, ITU...
 - Europäisch: ETSI ESI, CEN ESIGN,
 - National: DIN, DKE.....(und BSI Richtlinien?)

- Branchenspezifisch:
 - Banken: ZKA, IDENTRUS, EMV, PCI
 - EVU: VEDIS
 - E-Government: IDA - BC, OSCI, SAGA....

- Funktionsbezogen:
 - Signatur zur Authentifizierung: SSL, S/MIME, COMMON-PKi
 - Signatur mit Qual. Zertifikat zum Non-Repudation: COMMON-PKi
 - Verschlüsselung: SSL, Kerberos, COMMON-PKi
- Marktbezogen:
 - Marktdominierende Unternehmen: W3C, OASIS Global Plattform, PKI/X, PKCS#ff...Liberty,
 - Wirtschaftsorganisationen und Public-Private-Partnership: Signaturbündnis, COMMON-PKi
 - Nutzerorganisationen

Push- und Pull für PKI-Standards:

Nur wenige Beispiele:

Standards für Sicherheits niveaus

- WebTrust
- ETSI TS 102 042 + 101 456
- SigVo Sicherheitskonzept
- EBCA Policy nach RFC

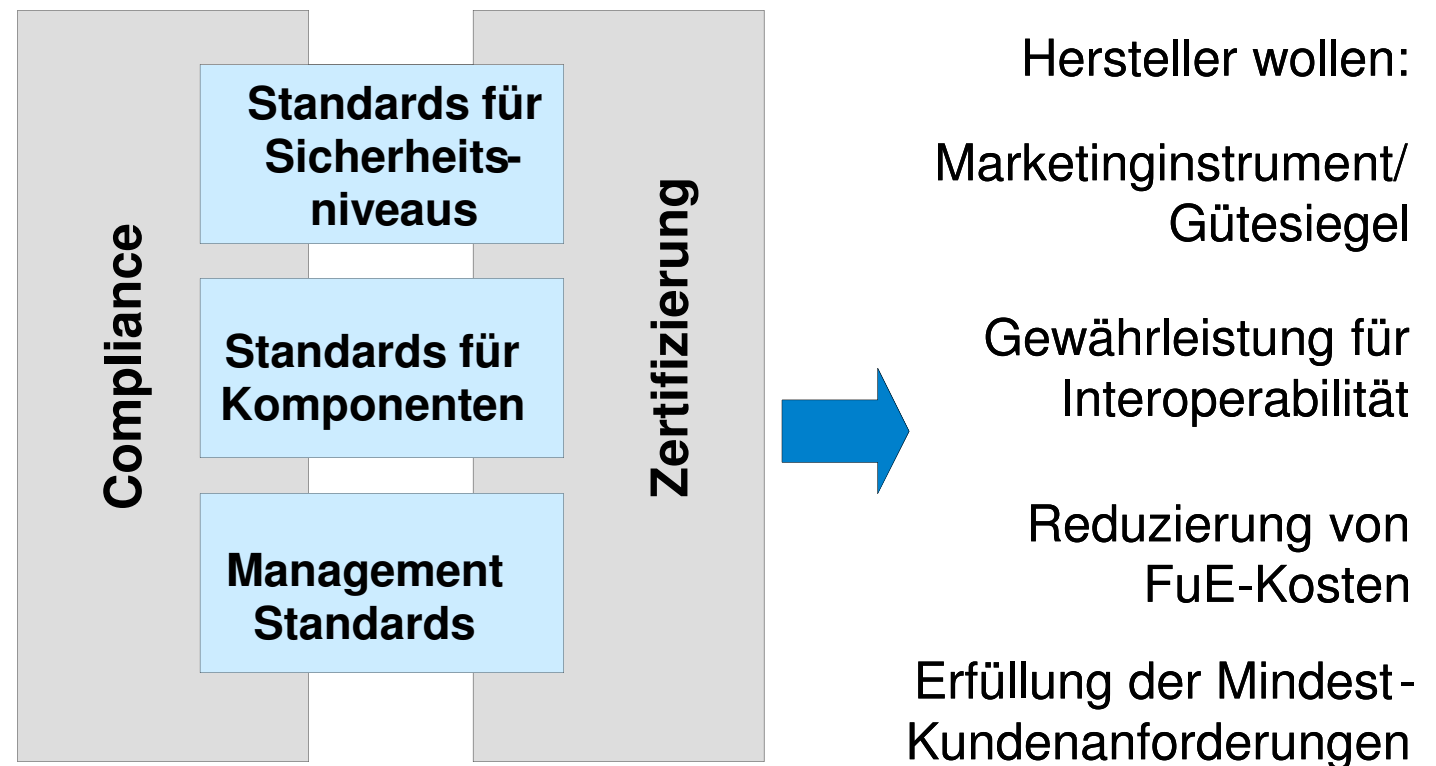
Standards für Komponenten

- RFC 5280 + PKI/X + PKCS#
- Common PKI
- ETSI XaDES + CaDES + PaDES
- LTANs
- Karten/HSM nach CEN
- S/MIME

Management Standards

- ISO 27001
- PCI
- BSI Grundschrift BS 100-X

Herstellermotivation



Push- und Pull für Standards:

Kundenmotivation

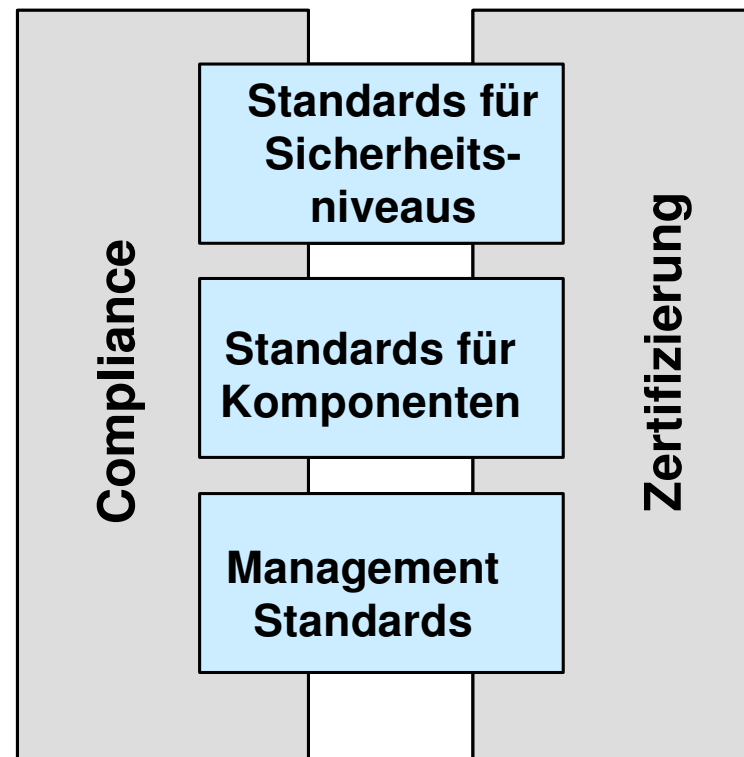
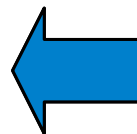
Kunden wollen:

Maßstab für
Gleichwertigkeit

zuverlässige
Interoperabilität

Kostenreduzierungen

garantierte
Sicherheitsniveaus



Herstellermotivation

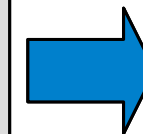
Hersteller wollen:

Marketinginstrument/
Gütesiegel

Gewährleistung für
Interoperabilität

Reduzierung von
FuE-Kosten

Erfüllung der Mindest-
Kundenanforderungen



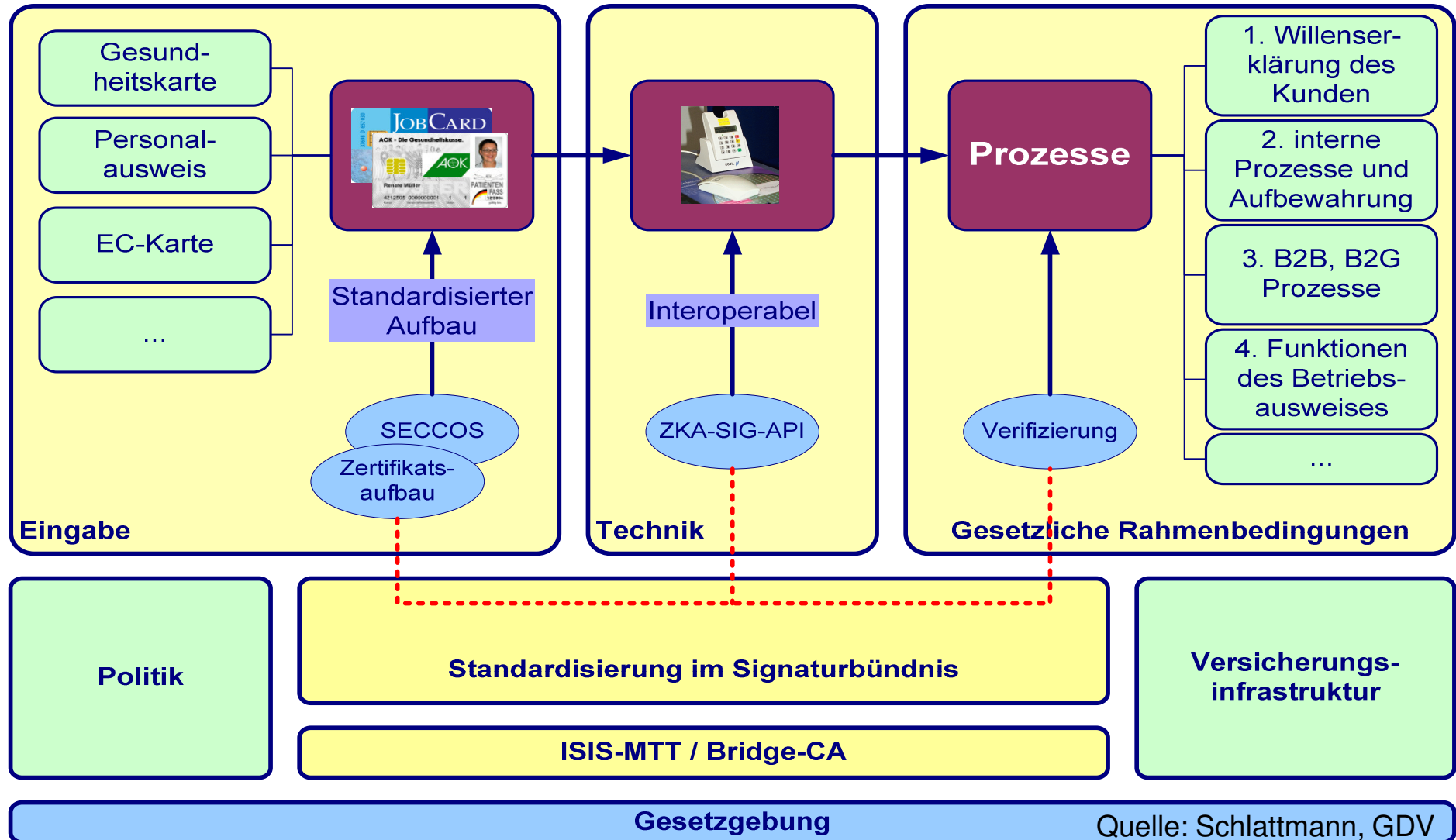
Facetten der eID-Standardisierung

- Standardisierung findet lokal, national (TR eID, eCARD, OSCI), europäisch (CEN versus ETSI) und international statt, seltener global (ISO, ITU, ICAO, OASIS).
- Standardisierung erfolgt durch offizielle Gremien in großer Menge,
- durch Inoffizielle Allianzen mit Erfolg (RFC's, CAB/Forum, Liberty, CardSpace, pdf...)
- Es gibt für fast alles mindestens einen Standard!
- Die Entwicklung „neuer“ Standards ist selten sinnvoll!
- Wichtiger ist die Profilierung und die konstante Anwendung der Standards.

Facetten der Signatur-Standardisierung

- Standards setzen hilft nur, wenn man diese auch durchsetzen kann!
- Standardisierung DARF NICHT Selbstzweck sein, (auch wenn reisen bildet)
- Wer finanziert, bestimmt die (hoffentlich offenen) „Standards“.
- Standardisierung ohne Konformität und Testung ist nicht sinnvoll.

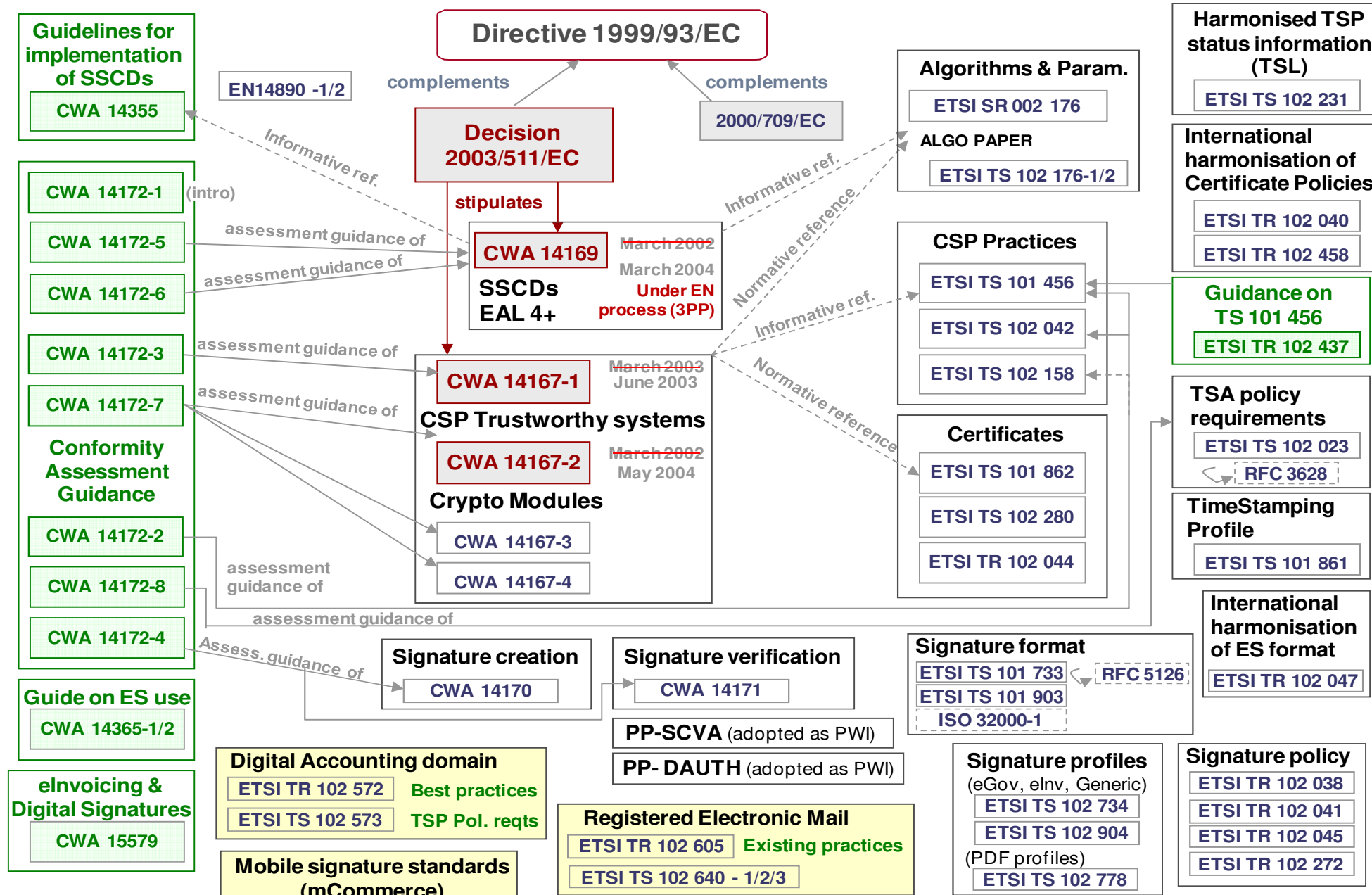
éCard-Strategie (geträumt in 2005)



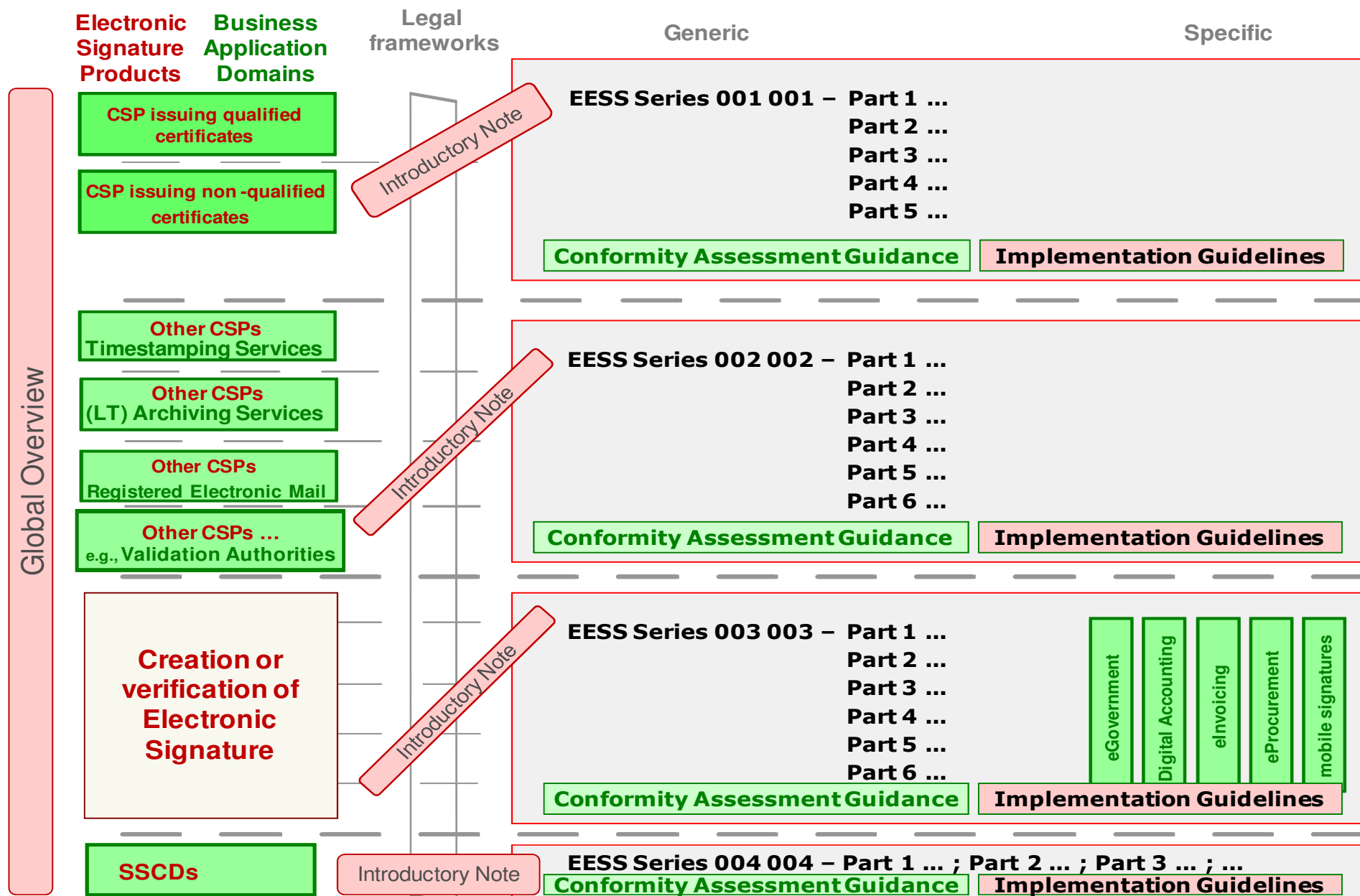
EU-Mandate 460:

Vieles neu, einiges besser:

EU eSignature standardisation work overview



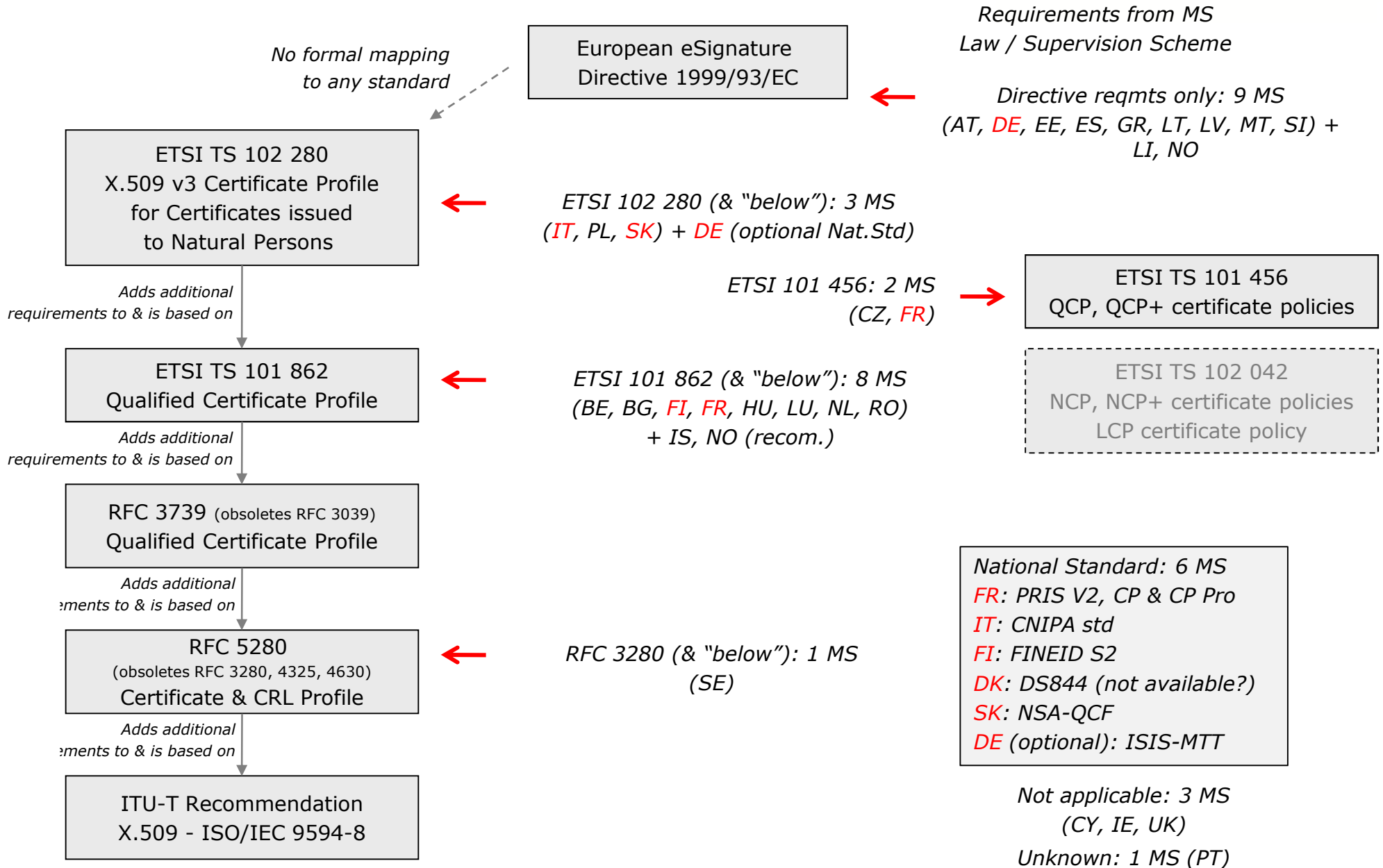
TeleTrust
Pioneers in IT security.



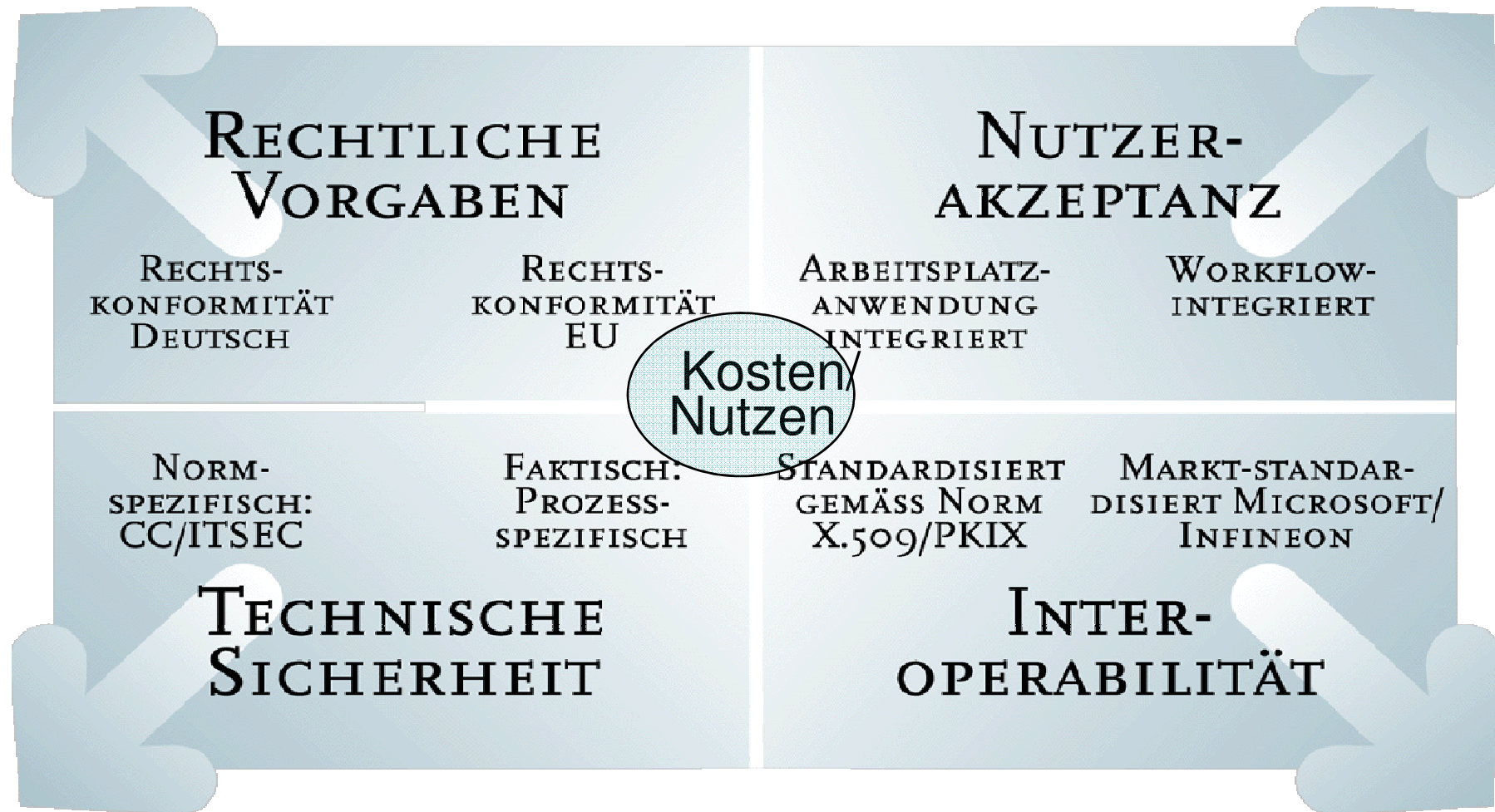
- CROBIES input on QC profile
 - Proposal for rationalisation of QC profile as part of Natural& Legal person certificate profile
 - Rationalisation of existing standards precedence to be solved through EESS series organisation
 - Mandating machine processable information on QC status and SSCD support
 - Signatories & Issuer identification consistent with STORK, and other related initiatives
 - Key usage combination issue

- CROBIES input on Trusted Lists – TSL ETSI TS 102 231
 - ETSI TS 102 231 v3.1.1 to be published rather soon,
 - Basis for Trusted List common template and format specifications as part of forthcoming Commission Decision
 - Minor updates expected on both from forthcoming Plug-Tests

(Qualified) Certificate Profile related standards



Spannungsfeld der Anforderungen



Murphy's Laws on Justice (Bureaucracy?):

*If the government hasn't taxed, licensed
or regulated it, isn't probably worth
anything.*



Noch Fragen ??

Dipl. Wirtsch.- Ing. Arno Fiedler
Nimbus Technologieberatung GmbH
Reichensteiner Weg 17
14195 Berlin

arno.fiedler@nimbus-network.de

Mobil: 0172-3053272