



## **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 Standardisierungsdschungel“**

# Facetten der Signatur-Standardisierung

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



# Facetten der PKI Standardisierung

- 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**

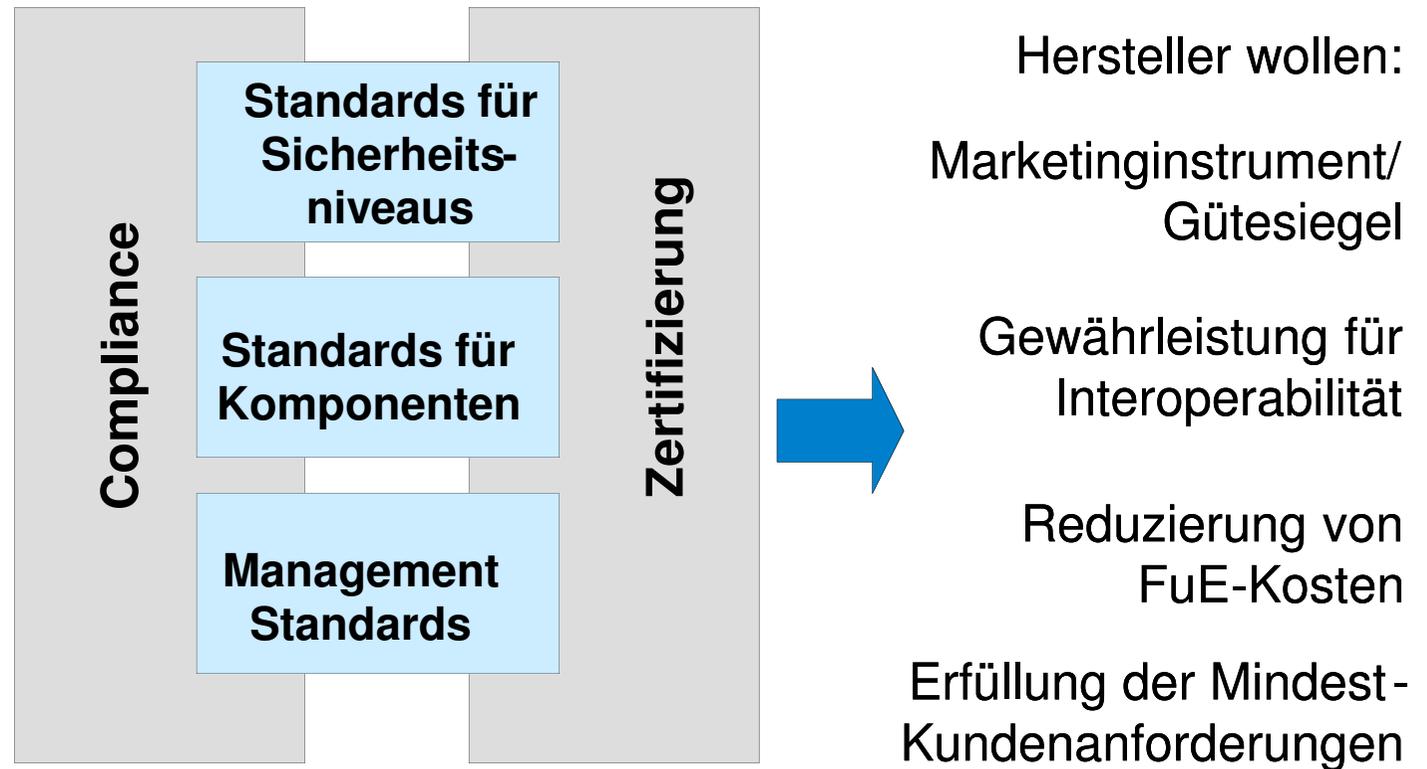
- RFC 5280 + PKI/X + PKCS#
- Common PKI
- ETSI XaDES + CaDES + PaDES
- LTANs
- Karten/HSM nach CEN
- S/MIME

**Management  
Standards**

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



## Herstellermotivation



# Push- und Pull für Standards:

## Kundenmotivation

## Herstellermotivation

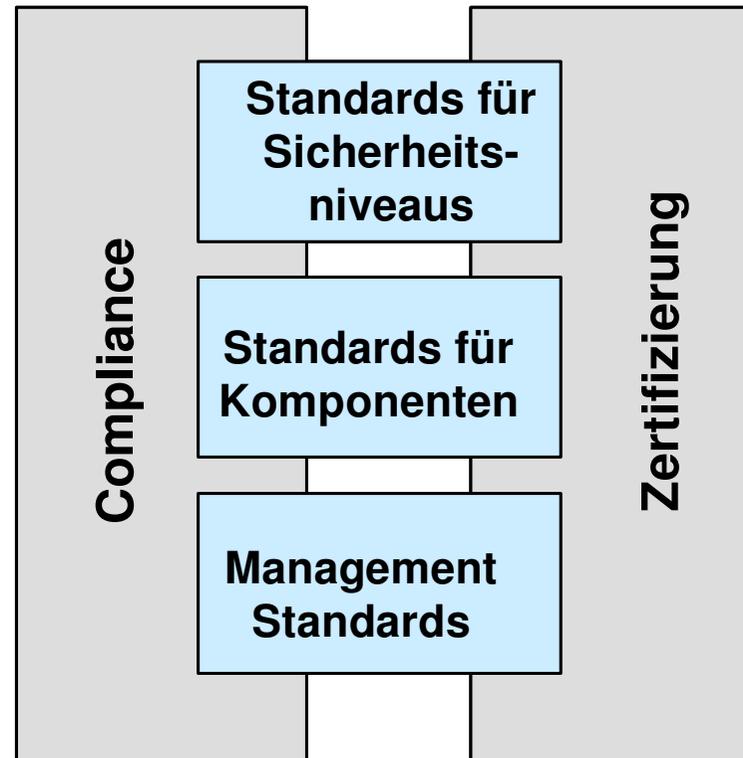
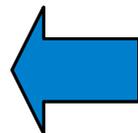
Kunden wollen:

Maßstab für  
Gleichwertigkeit

zuverlässige  
Interoperabilität

Kostenreduzierungen

garantierte  
Sicherheitsniveaus



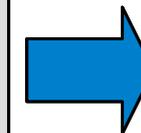
Hersteller wollen:

Marketinginstrument/  
Gütesiegel

Gewährleistung für  
Interoperabilität

Reduzierung von  
FuE-Kosten

Erfüllung der Mindest-  
Kundenanforderungen



# Facetten der eID-Standardisierung

- Standardisierung findet lokal, national (TR eID, eCARD, OSCl), 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.

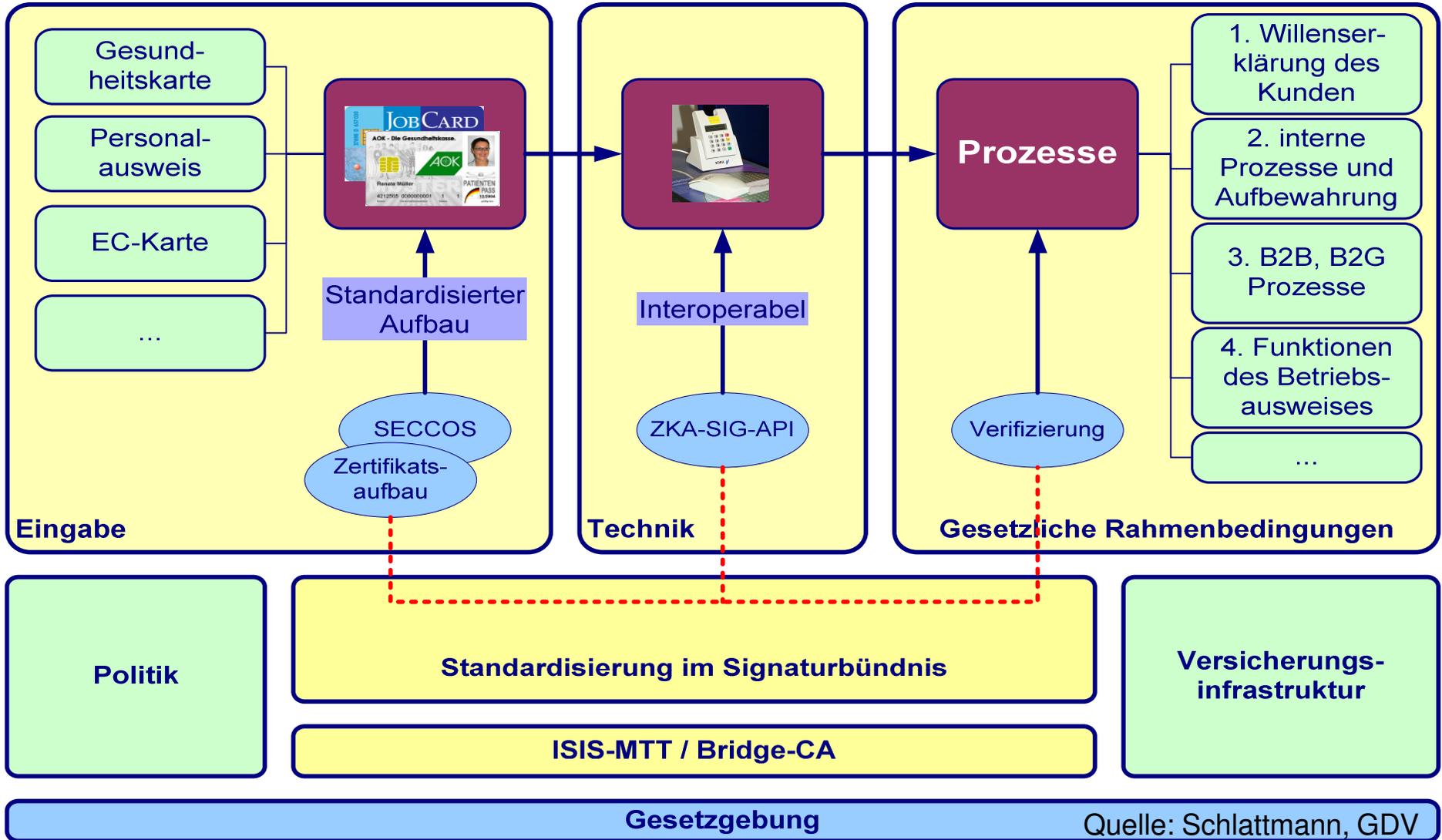


# Facetten der Signatur-Standardisierung

- 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 )

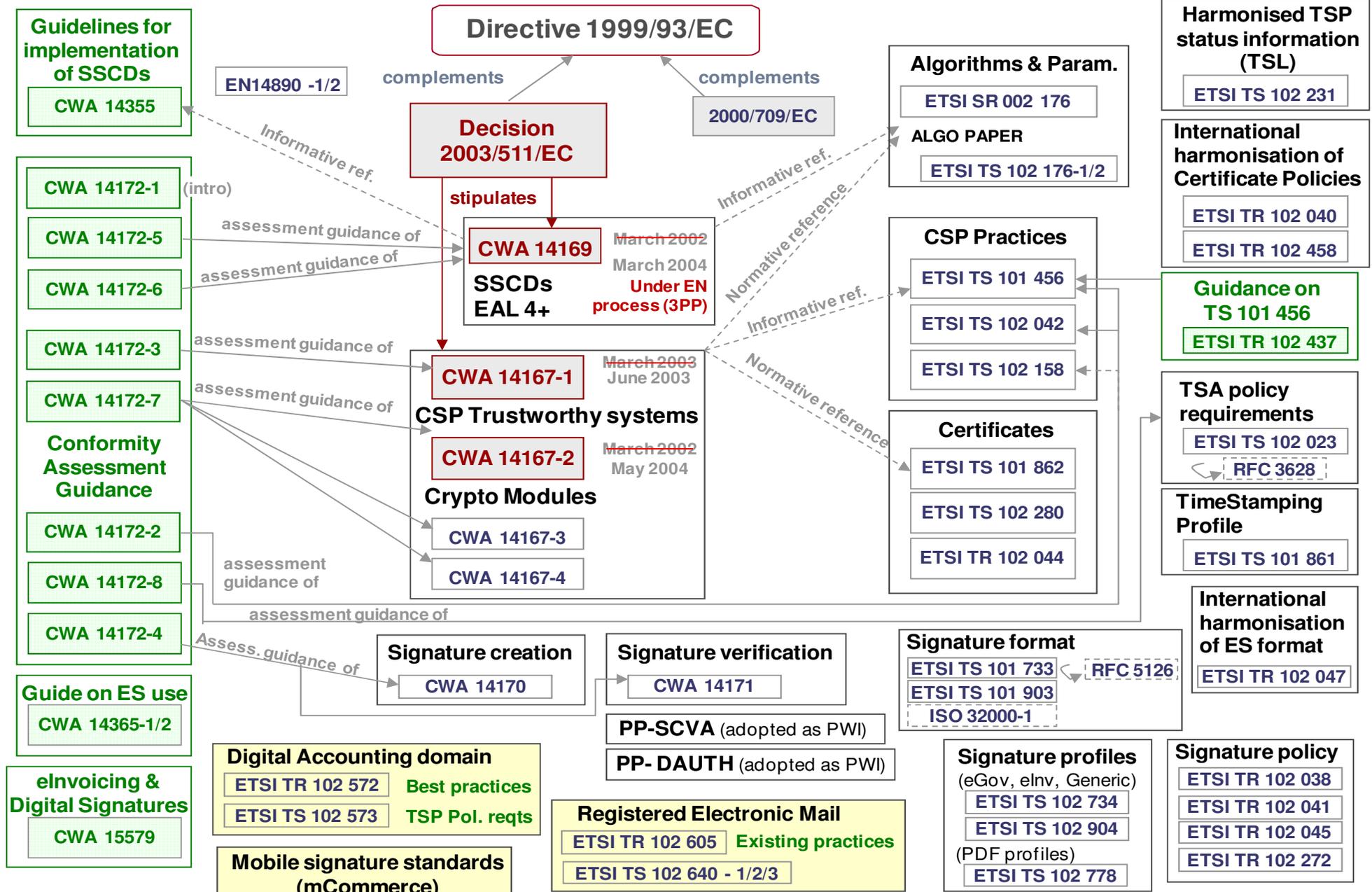


---

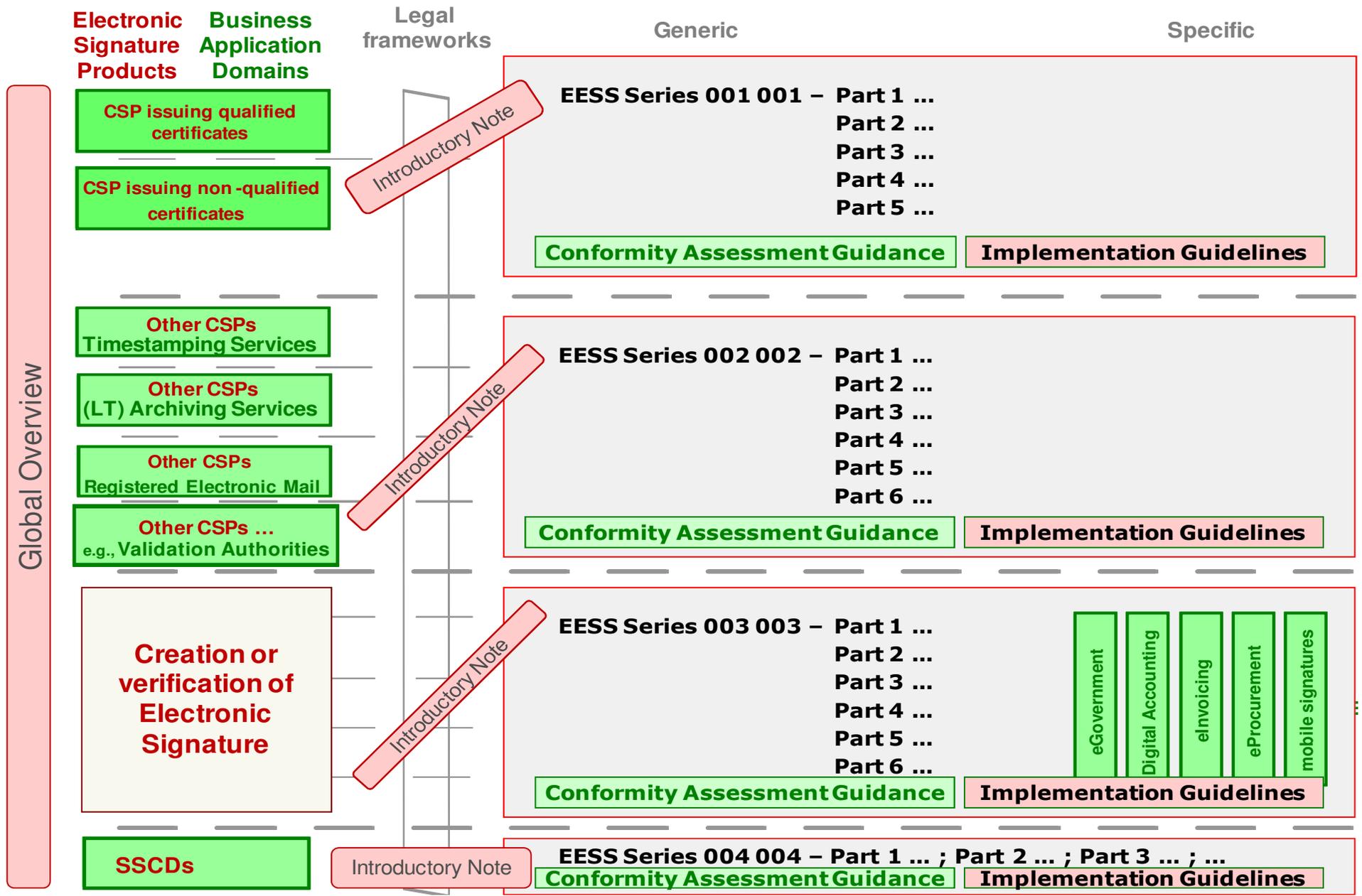
## EU-Mandate 460:

Vieles neu, einiges besser:

# EU eSignature standardisation work overview



# Rationalised architecture for EU eSig standards



- 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



Requirements from MS  
Law / Supervision Scheme

Directive reqmts only: 9 MS  
(AT, DE, EE, ES, GR, LT, LV, MT, SI) +  
LI, NO

European eSignature  
Directive 1999/93/EC

No formal mapping  
to any standard

ETSI TS 102 280  
X.509 v3 Certificate Profile  
for Certificates issued  
to Natural Persons

ETSI 102 280 (& "below"): 3 MS  
(IT, PL, SK) + DE (optional Nat.Std)

Adds additional  
requirements to & is based on

ETSI 101 456: 2 MS  
(CZ, FR)

ETSI TS 101 456  
QCP, QCP+ certificate policies

ETSI TS 101 862  
Qualified Certificate Profile

ETSI 101 862 (& "below"): 8 MS  
(BE, BG, FI, FR, HU, LU, NL, RO)  
+ IS, NO (recom.)

Adds additional  
requirements to & is based on

ETSI TS 102 042  
NCP, NCP+ certificate policies  
LCP certificate policy

RFC 3739 (obsoletes RFC 3039)  
Qualified Certificate Profile

Adds additional  
requirements to & is based on

RFC 5280  
(obsoletes RFC 3280, 4325, 4630)  
Certificate & CRL Profile

RFC 3280 (& "below"): 1 MS  
(SE)

Adds additional  
requirements to & is based on

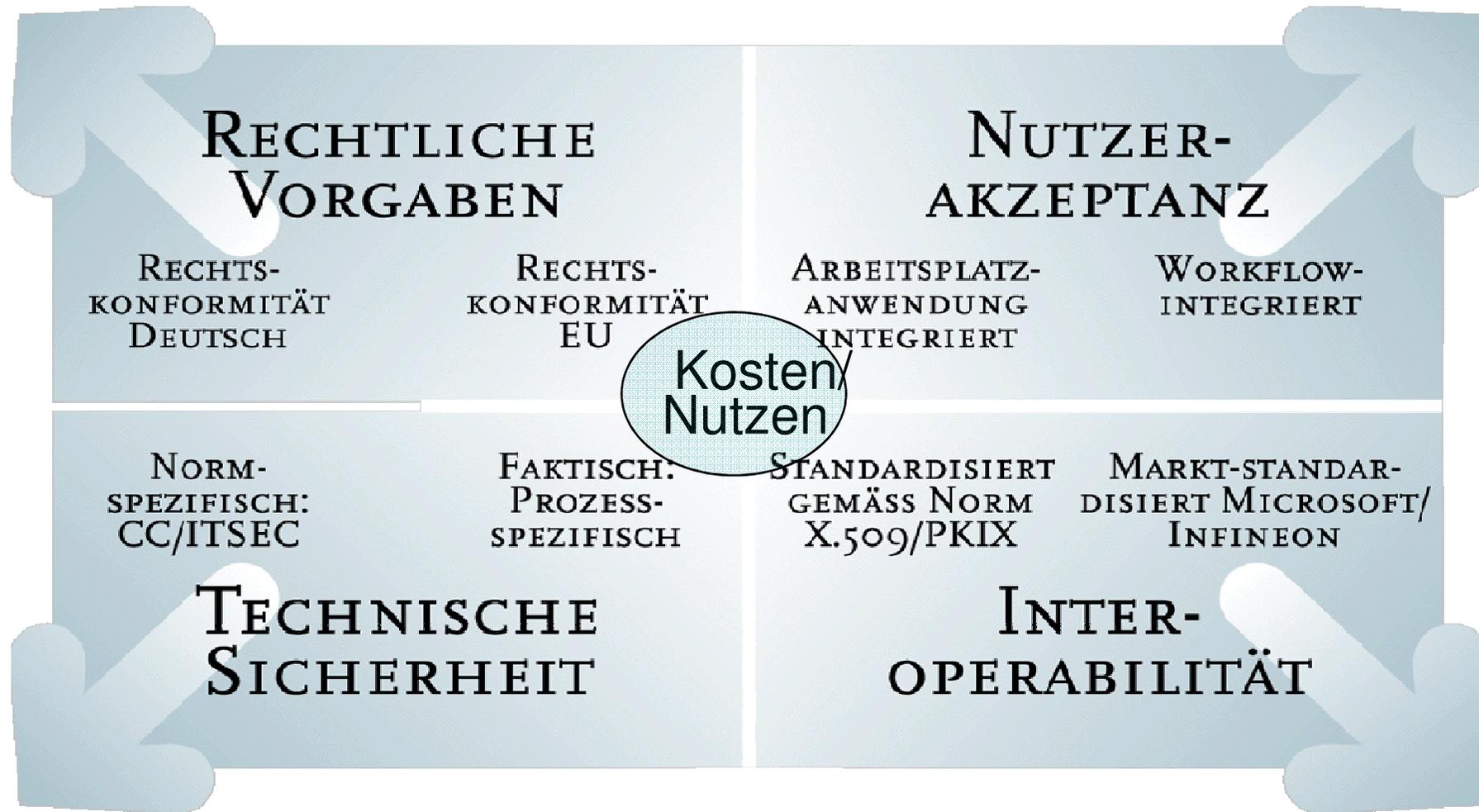
National Standard: 6 MS  
FR: PRIS V2, CP & CP Pro  
IT: CNIPA std  
FI: FINEID S2  
DK: DS844 (not available?)  
SK: NSA-QCF  
DE (optional): ISIS-MTT

ITU-T Recommendation  
X.509 - ISO/IEC 9594-8

Not applicable: 3 MS  
(CY, IE, UK)

Unknown: 1 MS (PT)

# 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](mailto:arno.fiedler@nimbus-network.de)

Mobil: 0172-3053272