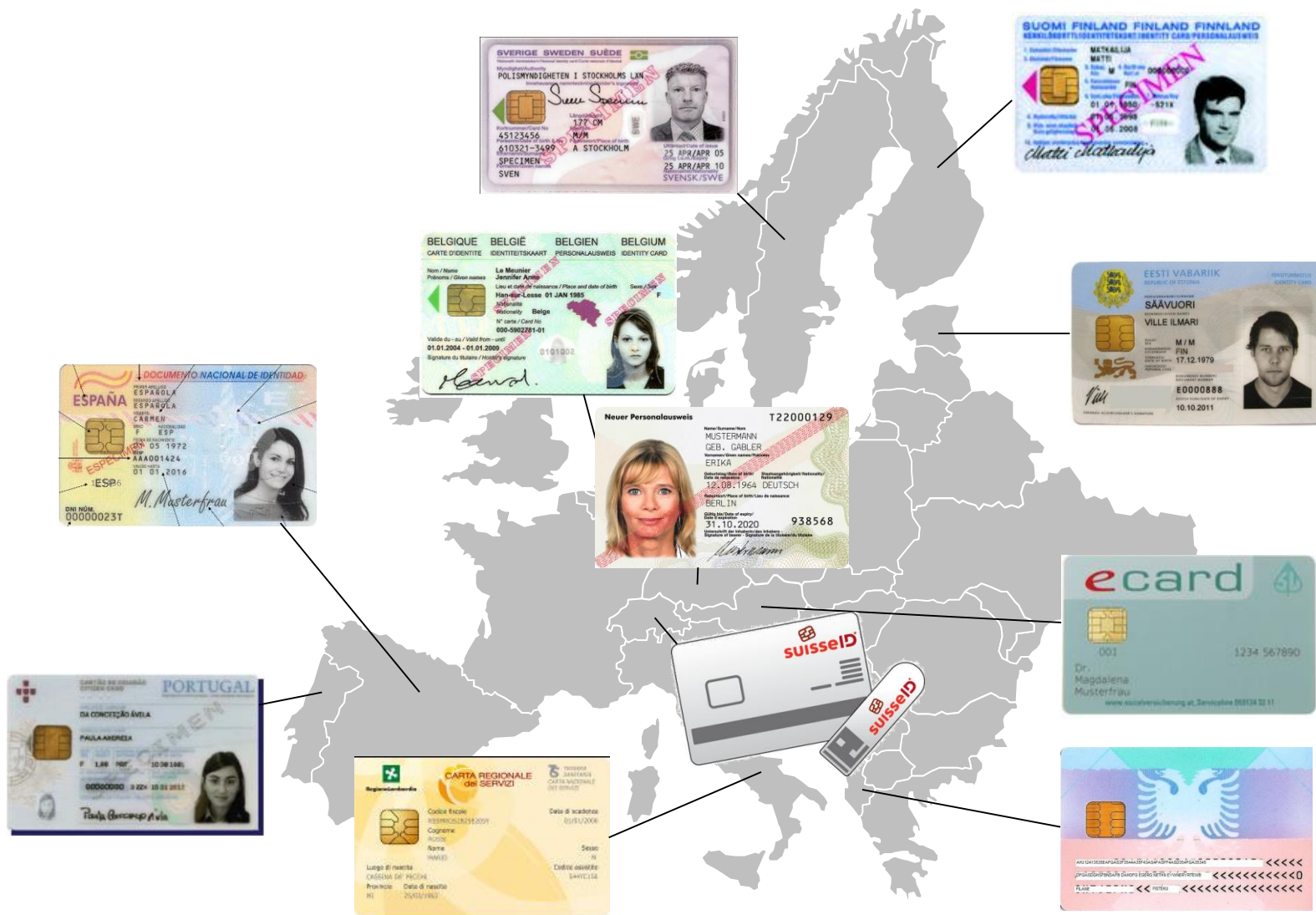


Open eIDAS

Offene Initiativen für Authentisierung und Signatur

Dr. Detlef Hühnlein, ecsec GmbH

- **Einleitung**
- Offene Initiativen
- Zusammenfassung



	Austria	http://www.signatur.rtr.at/currenttsl.xml
1	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH	
	• office@a-trust.at • http://www.a-trust.at	

⋮

	Germany	http://www.nrca-ds.de/st/TSL_DE.XML.tsr.zip
21	D-TRUST GmbH	
	• http://www.d-trust.net • info@d-trust.net	

⋮

	Spain	https://sede.mityc.gob.es/prestadores/tsl/tsl.xml
133	Banco Santander, S.A	
	• certificacion.universitaria@gruposantander.com	

⋮

155	SIGNE, S.A. (SIGNE Autoridad de Certificación)	
	• www.signe.es/signa-ac • signe-ac@signe.es	

≈ 150 CSPs



<https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers>

- I. Allgemeine Bestimmungen (Artikel 1-5)
- II. Elektronische Identifizierung (Artikel 6-12)
- III. Vertrauensdienste
 - 1. Allgemeine Bestimmungen (Artikel 13-16)
 - 2. Aufsicht (Artikel 17-19)
 - 3. Qualifizierte Vertrauensdienste (Artikel 20-24)
 - 4. Elektronische Signaturen (Artikel 25-34)
 - 5. Elektronische Siegel (Artikel 35-40)
 - 6. Elektronische Zeitstempel (Artikel 41-42)
 - 7. Dienste für die Zustellung elektronischer Einschreiben (Artikel 43-44)
 - 8. Website-Authentifizierung (Artikel 45)
- IV. Elektronische Dokumente (Artikel 46)
- V. Befugnisübertragungen und Durchführungsbestimmungen (Artikel 47-48)
- VI. Schlussbestimmungen (Artikel 49-52)

I. Allgemeine Bestimmungen (Artikel 1-5)

II. Elektronische Identifizierung (Artikel 6-12)

eIDAS

III. Vertrauensdienste

1. Allgemeine Bestimmungen (Artikel 13-16)

2. Aufsicht (Artikel 17-19)

3. Qualifizierte Vertrauensdienste (Artikel 20-24)

4. Elektronische Signaturen (Artikel 25-34)

5. Elektronische Siegel (Artikel 35-40)

6. Elektronische Zeitstempel (Artikel 41-42)

7. Dienste für die Zustellung elektronischer Einschreiben (Artikel 43-44)

8. Website-Authentifizierung (Artikel 45)

eIDAS

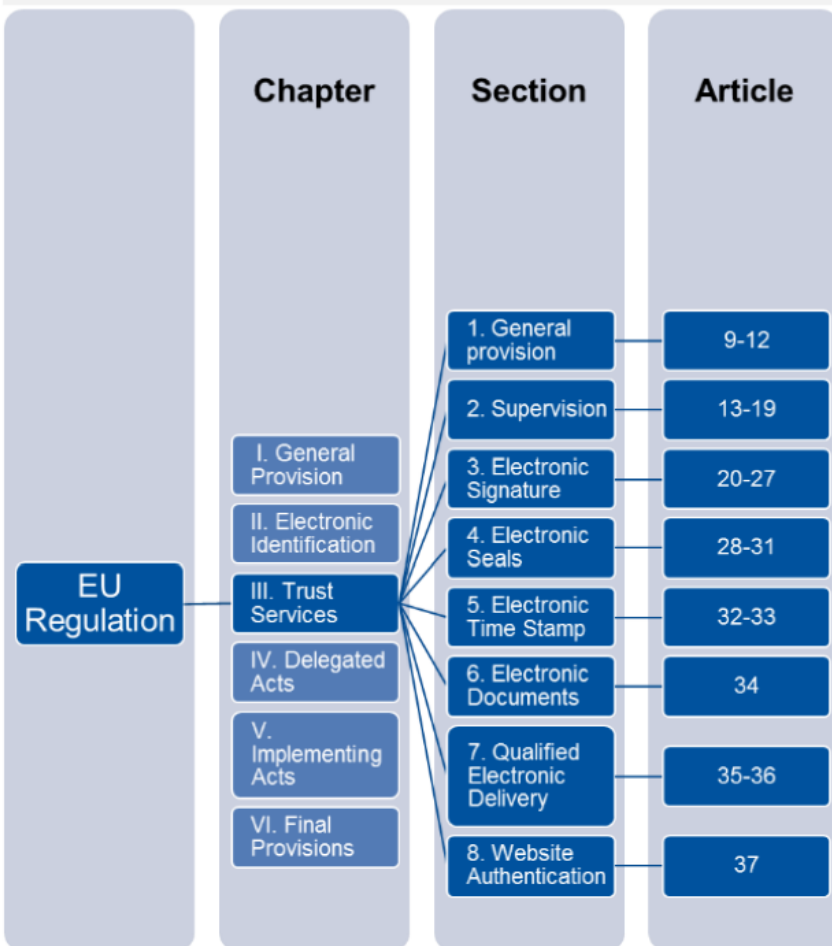
IV. Elektronische Dokumente (Artikel 46)

V. Befugnisübertragungen und Durchführungsbestimmungen
(Artikel 47-48)

VI. Schlussbestimmungen (Artikel 49-52)

- eID-Mechanismen im Verantwortungsbereich der Mitgliedstaaten können notifiziert (Art. 9) und dadurch gegenseitig anerkannt werden (Art. 6)
- eID-Sicherheitsniveaus „niedrig“, „substanziell“ und „hoch“ (Art. 8) (Durchführungsrechtsakte (DRA) bis zum 18.09.2015)
- Der notifizierende Mitgliedstaat stellt Verfügbarkeit eines grenzüberschreitenden Authentifizierungsdienstes sicher (Art. 7).
„Die grenzüberschreitende Authentifizierung sollte gebührenfrei sein, wenn sie in Bezug auf einen Online-Dienst erfolgt, der von einer öffentlichen Stelle erbracht wird.“
- Umgehende Meldung von Sicherheitsverletzungen, Behebung spätestens nach 3 Monaten (Art. 10)
- Der notifizierende Mitgliedstaat haftet für etwaige Schäden (Art. 11)
- Es wird ein eID-Interoperabilitätsrahmen geschaffen in dem die Mitgliedstaaten zusammenarbeiten (DRA bis 18.09.2015 bzw. 18.03.2015)

Legal Framework

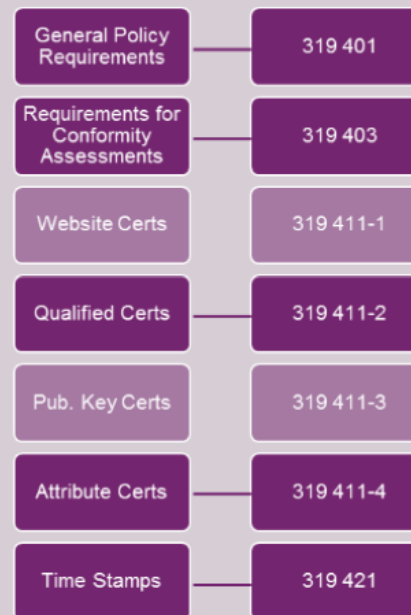


Implementing Acts

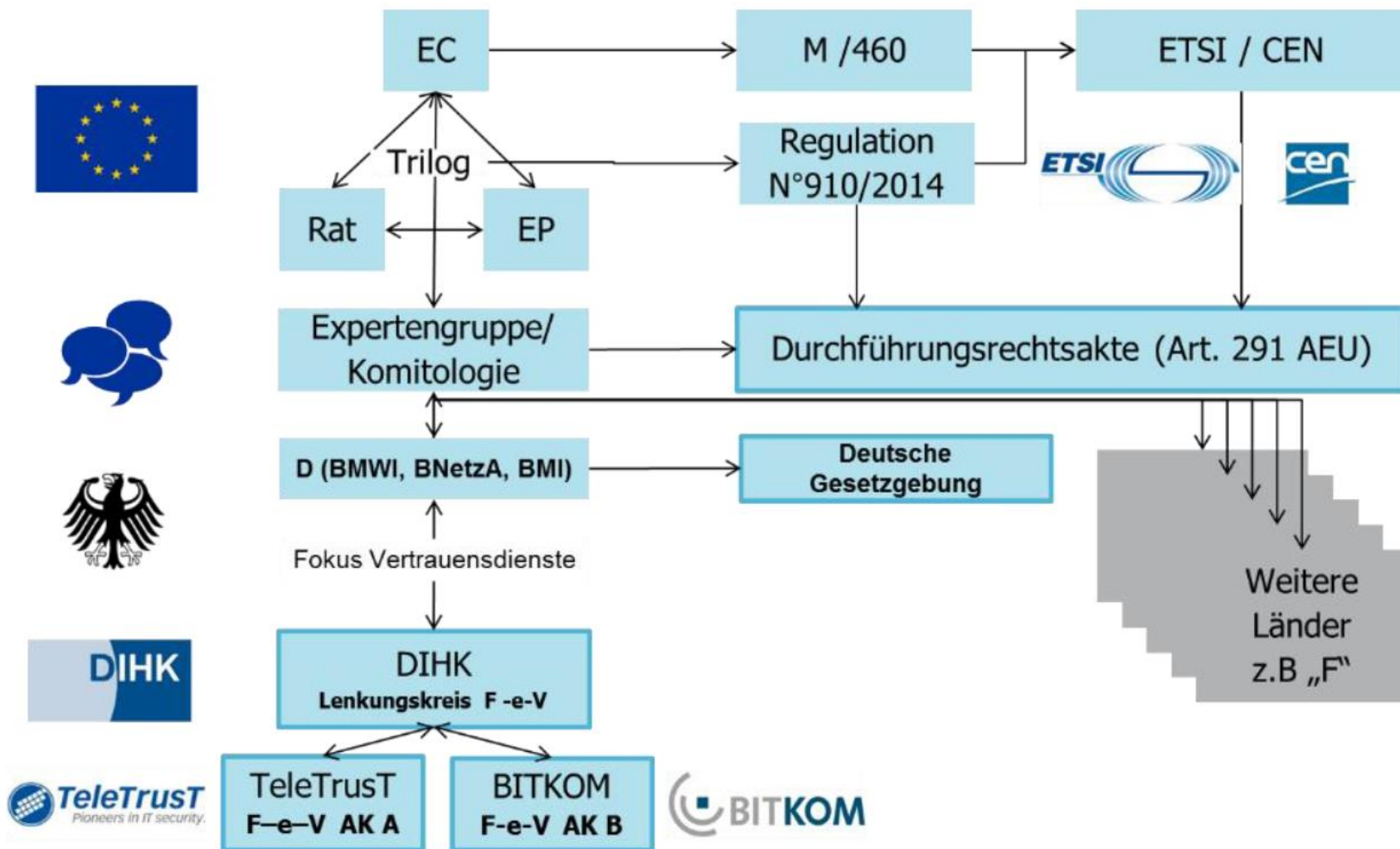
Art. 13(6)
 Art. 15(6)
 Art. 16(6)
 Art. 17(5)
 Art. 18(6)
 Art. 18a(3)
 Art. 19(5)
 Art. 20(7)
 Art. 21(5)
 Art. 22(2)
 Art. 23(2a)
 Art. 24(3)
 Art. 25(3)
 Art. 26(2)
 Art. 27(3)
 Art. 28(7)
 Art. 29(5)
 Art. 30(1,2,3)
 Art. 31(1)
 Art. 34(4)
 Art. 36(2)
 Art. 37(4)

Technical Framework

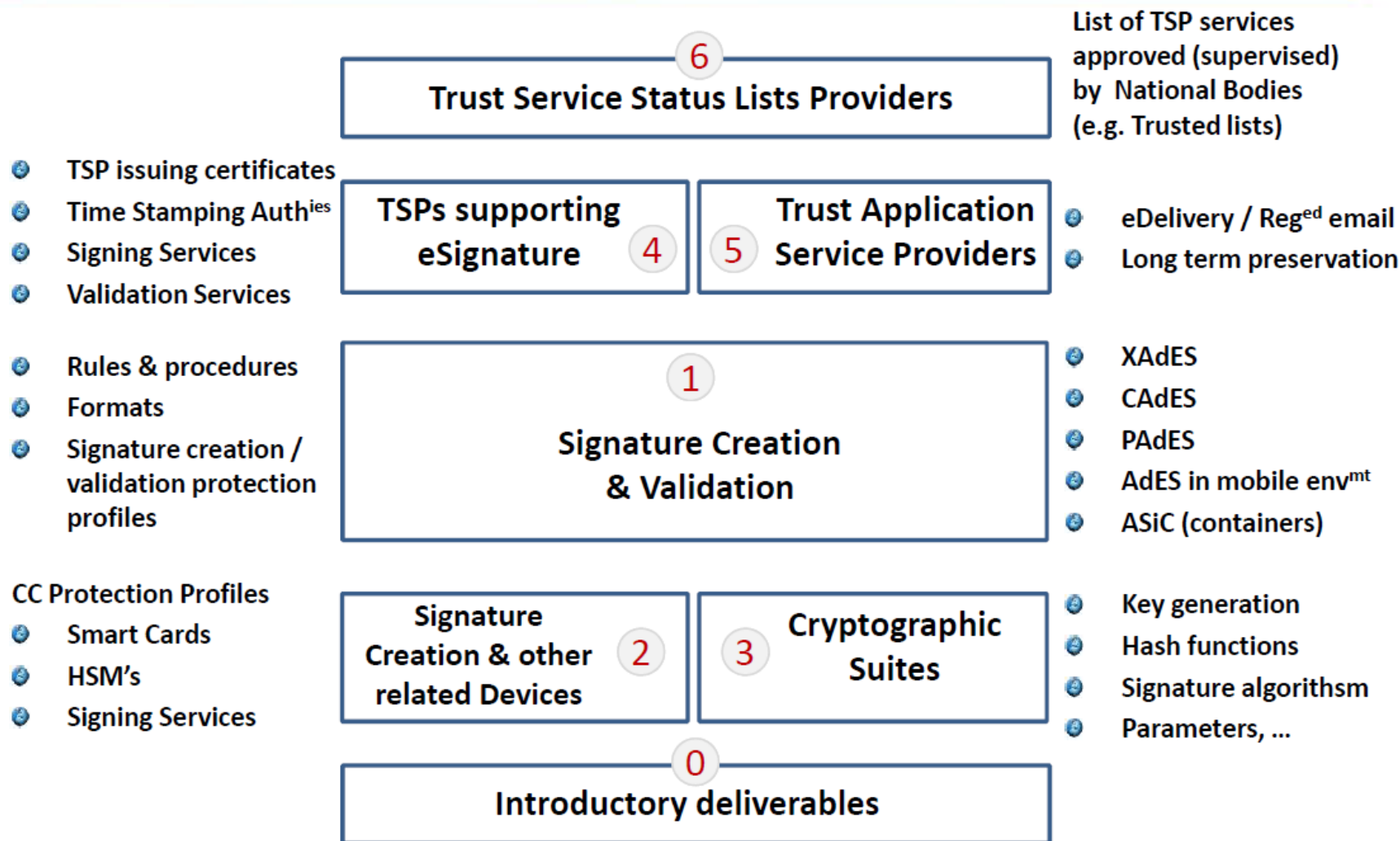
ETSI Conformity Assessment Framework

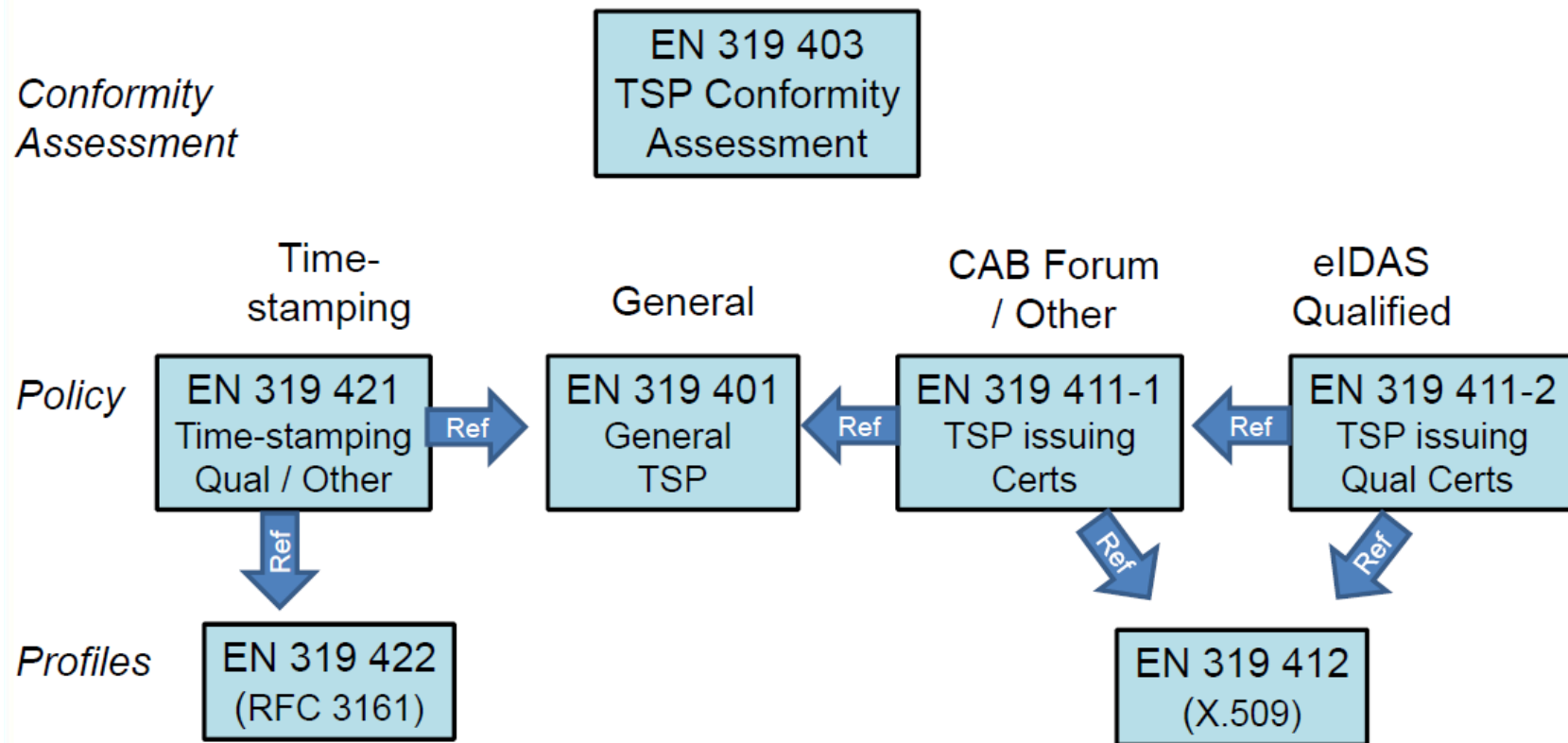


Artikel	T	Regelungsgegenstand des Rechtsaktes
17 (8)	K	Form und Verfahren für die jährliche Berichterstattung der Aufsichtsstellen an EU Komm.
19 (4) a)	K	Sicherheitsmaßnahmen für Vertrauensdiensteanbieter
19 (4) b)	K	Form und Verfahren für die Meldung von Sicherheitsvorfällen
20 (4) a)	K	Akkreditierung von Prüfstellen für die Prüfung von Vertrauensdiensteanbietern
20 (4) b)	K	Überprüfungsvorschriften
21 (4)	K	Form und Verfahren für Beginn der Erbringung qualifizierter Vertrauensdienste
22 (5)	M	Spezifikation und Form der Vertrauenslisten
23 (3)	M	Form des EU-Vertrauenssiegels
24 (5)	K	Anforderungen an vertrauenswürdige Systeme und Produkte
27 (5)	M	Formate für fortgeschrittene elektronische Signaturen
28 (6)	K	Anforderungen an qualifizierte Zertifikate für elektronische Signaturen
29 (2)	K	Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten
30 (3)	M	Sicherheitsbewertungsverfahren informationstechnischer Produkte
30 (4)	D	Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten
31 (3)	K	Liste zertifizierter Signaturerstellungseinheiten
32 (3)	K	Validierung qualifizierter elektronischer Signaturen
33 (2)	K	Anforderungen an qualifizierte Validierungsdienste
34 (2)	K	Anforderungen an qualifizierte Bewahrungsdienste
37 (5)	M	Formate oder Referenzverfahren für fortgeschrittene elektronische Siegel
38 (6)	K	Anforderungen an qualifizierte Zertifikate für elektronische Siegel
42 (2)	K	Anforderungen an qualifizierte elektronische Zeitstempel
44 (2)	K	Anforderungen an qualifizierte Dienste für die Zustellung elektronischer Einschreiben
45 (2)	K	Anforderungen an qualifizierte Zertifikate für die Website-Authentisierung



- Einleitung
- Offene Initiativen
 - ETSI/CEN M/460
 - Open Signature
 - Open eCard
 - SkIDentity
 - Common-eID
 - FutureID
- Zusammenfassung





© ETSI 2014. All rights reserved

Trust Service Providers Supporting Electronic Signatures

[EN 319 401](#) General Policy Requirements for Trust Service Providers

EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates

[319 411-1](#): General requirements

[319 411-2](#): Requirements for trust service providers issuing EU qualified certificates

EN 319 412 Certificate Profiles

[319 412-1](#): Overview and common data structures

[319 412-2](#): Certificate profile for certificates issued to natural persons

[319 412-3](#): Certificate profile for certificates issued to legal persons

[319 412-4](#): Certificate profile for web site certificates issued to organisations

[319 412-5](#): QCStatements

[EN 319 421](#) Policy and Security Requirements for Trust Service Providers issuing Electronic Time-
Stamps

[EN 319 422](#) Time-stamping protocol and electronic time-stamp profiles

- Einleitung
- Offene Initiativen
 - ETSI/CEN M/460
 - Open Signature
 - Open eCard
 - SkIDentity
 - Common-eID
 - FutureID
- Zusammenfassung



Press Release

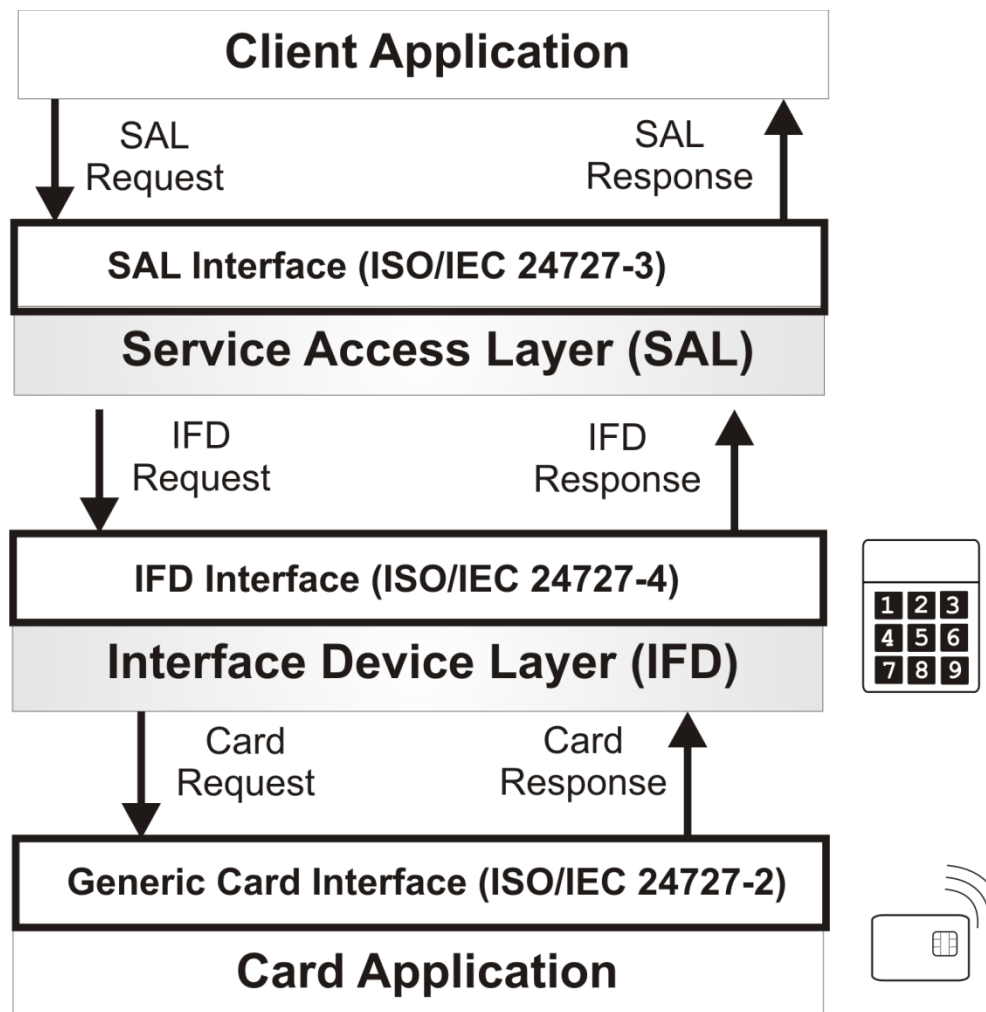
Open Signature Initiative to foster transparency and interoperability for electronic signatures

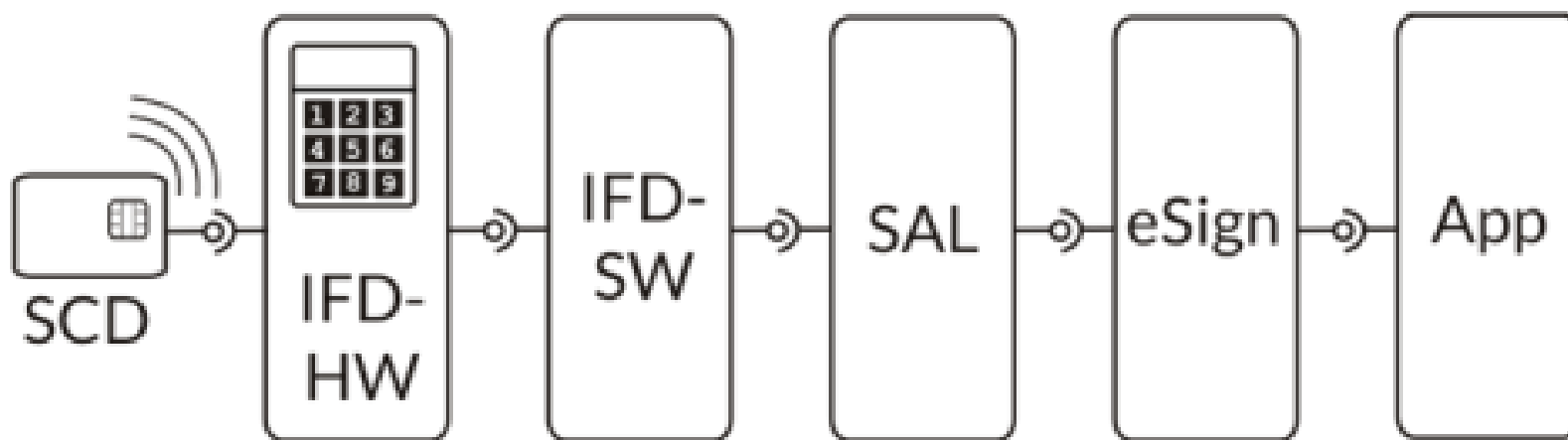
[Europe, September 3rd, 2013] Leading European institutions, associations, enterprises and projects join forces to launch the non-profit Open Signature Initiative (<http://opensignature.org>), which aims at improving transparency and interoperability with respect to electronic signature technology and related trust services.

<http://opensignature.org>

initiated by







Press Release



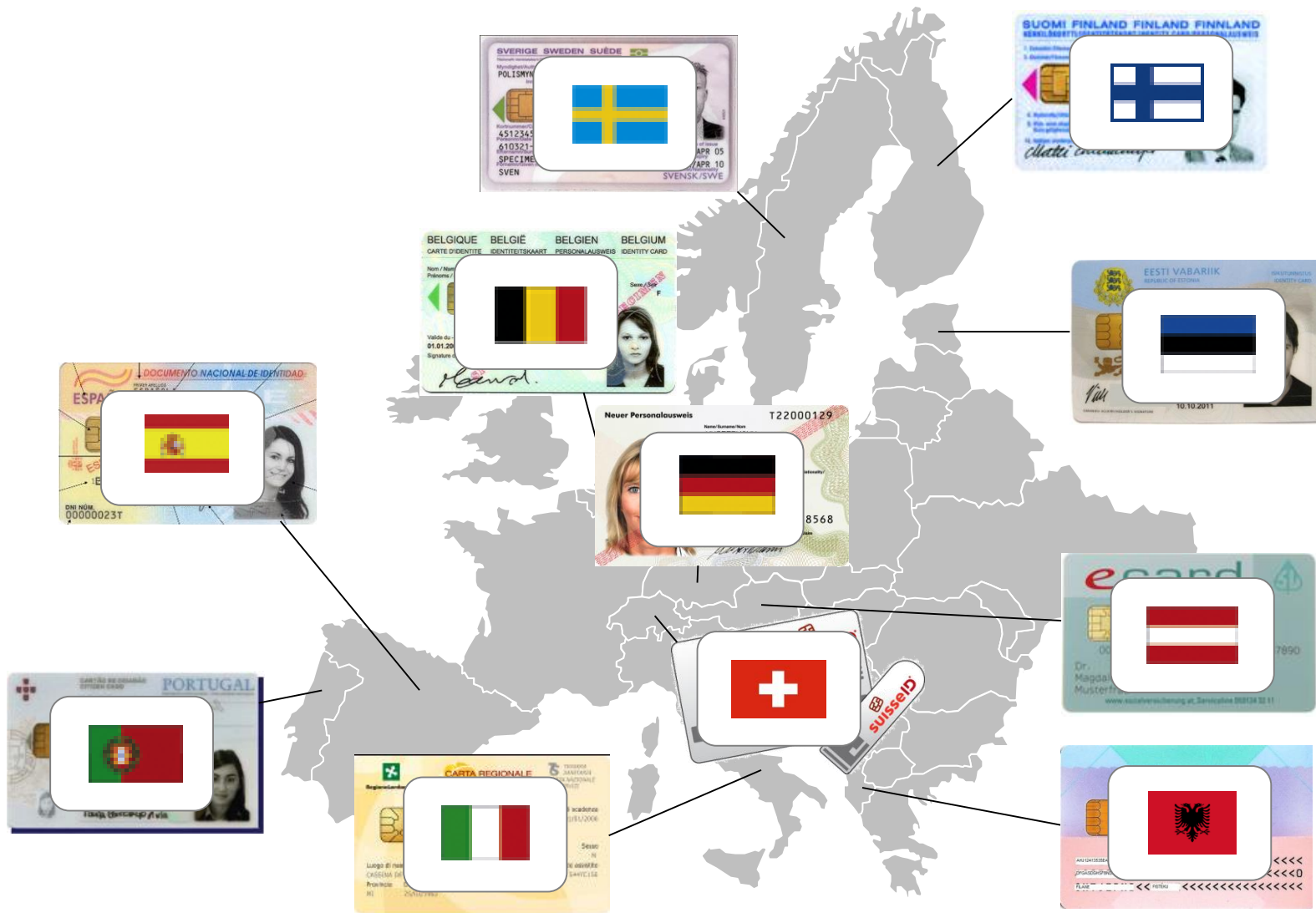
Open Signature Initiative launches Directory of Signature Creation Devices

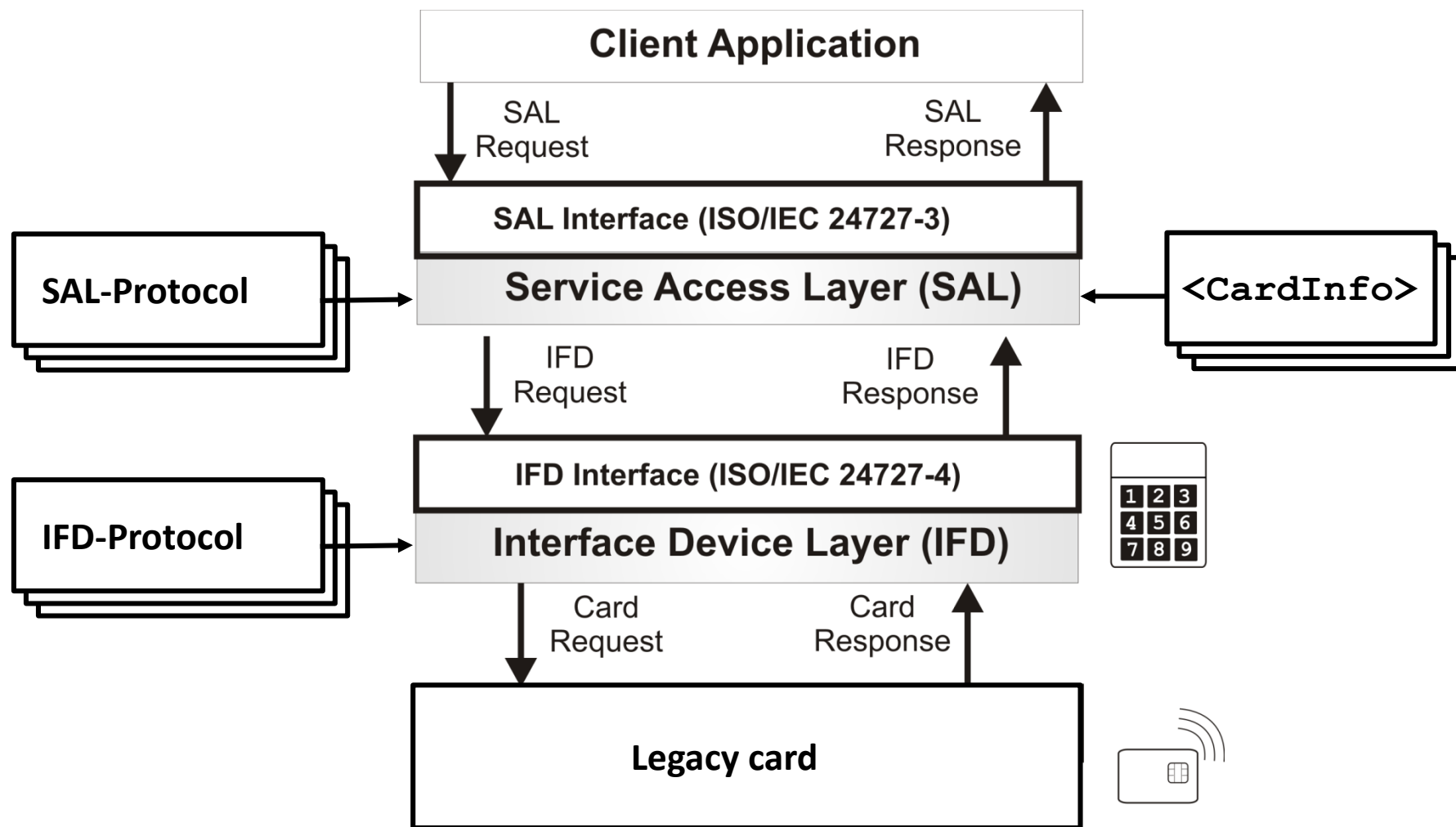
[Brussels, October 23rd, 2013] The non-profit Open Signature Initiative today launched the Directory of Signature Creation Devices (<http://opensignature.org/devices>), which aims at providing an overview of existing signature creation devices available in the market. Issuers and vendors of signature creation devices are encouraged to join the initiative and register their devices.

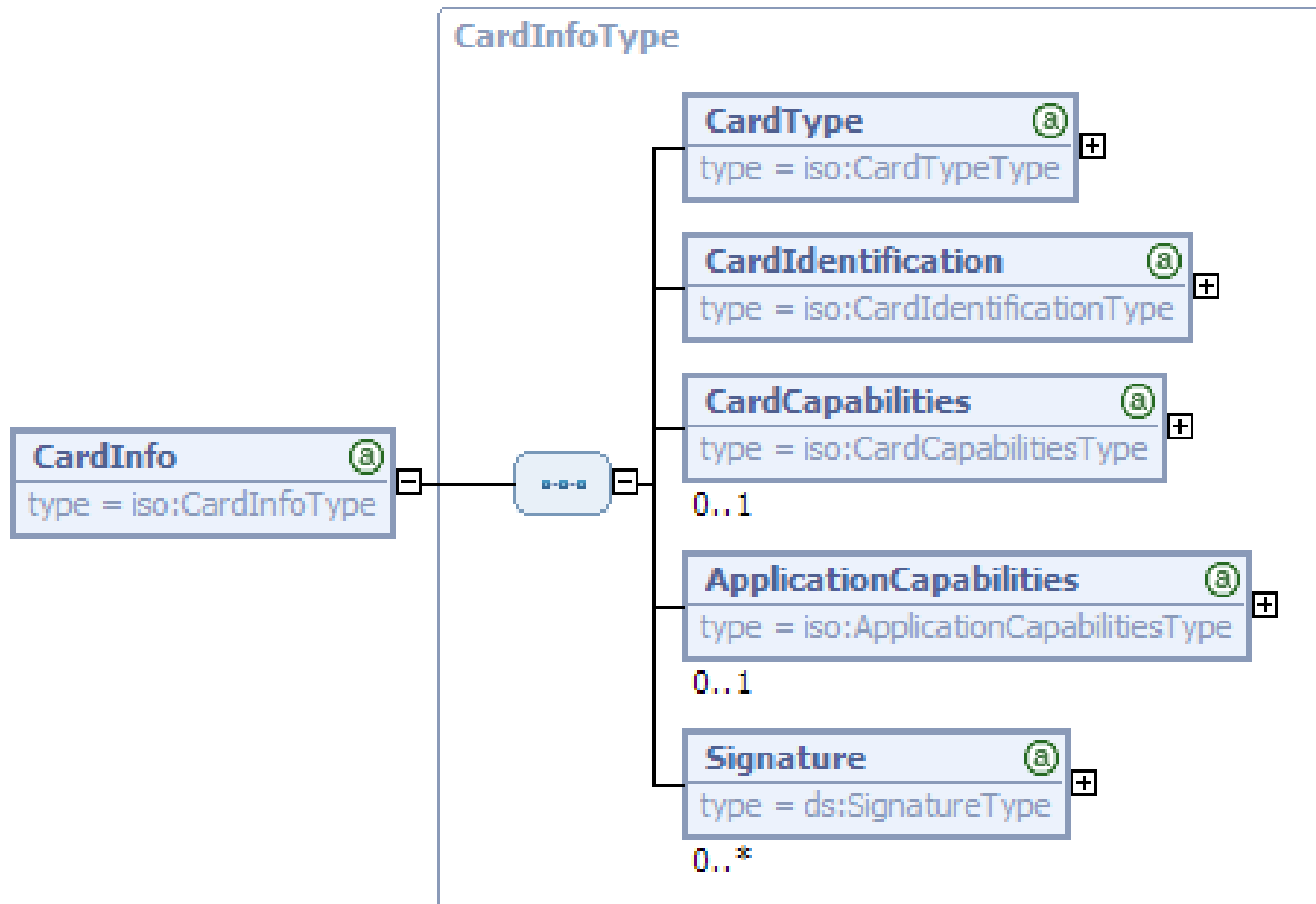
	Austria	  
	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH	
	SV-Chipkarten Betriebs- und Errichtungsgesellschaft m. b. H.	 
	Belgium	  
	Certipost NV SA	
	Society for Worldwide Interbank Financial Telecommunication SCRL	
	Bulgaria	  
	BORICA - BANKSERVICE AD	
	InfoNotary PLC	

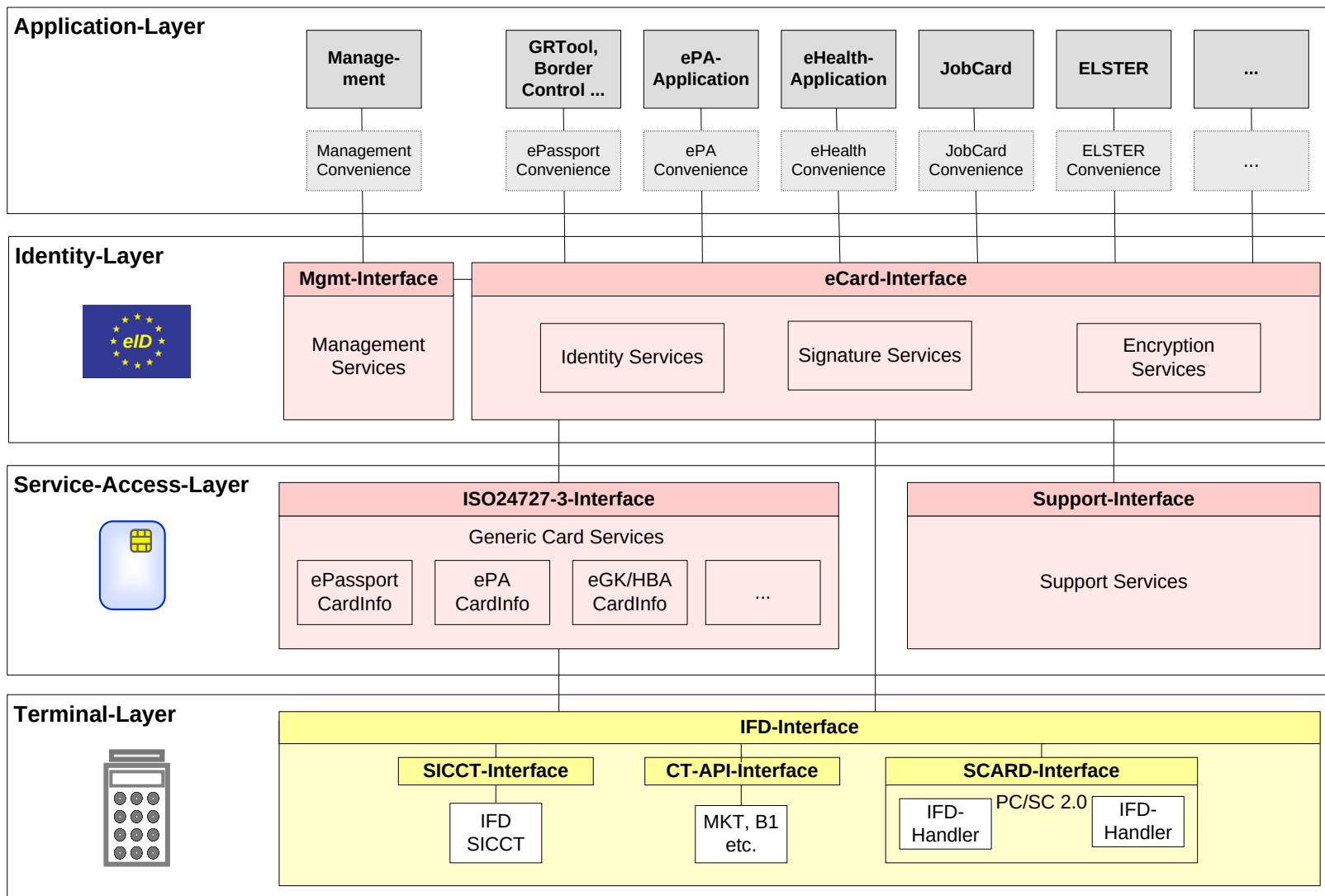
<http://opensignature.org/devices>

- Einleitung
- Offene Initiativen
 - ETSI/CEN M/460
 - Open Signature
 - **Open eCard**
 - SkIDentity
 - Common-eID
 - FutureID
- Zusammenfassung



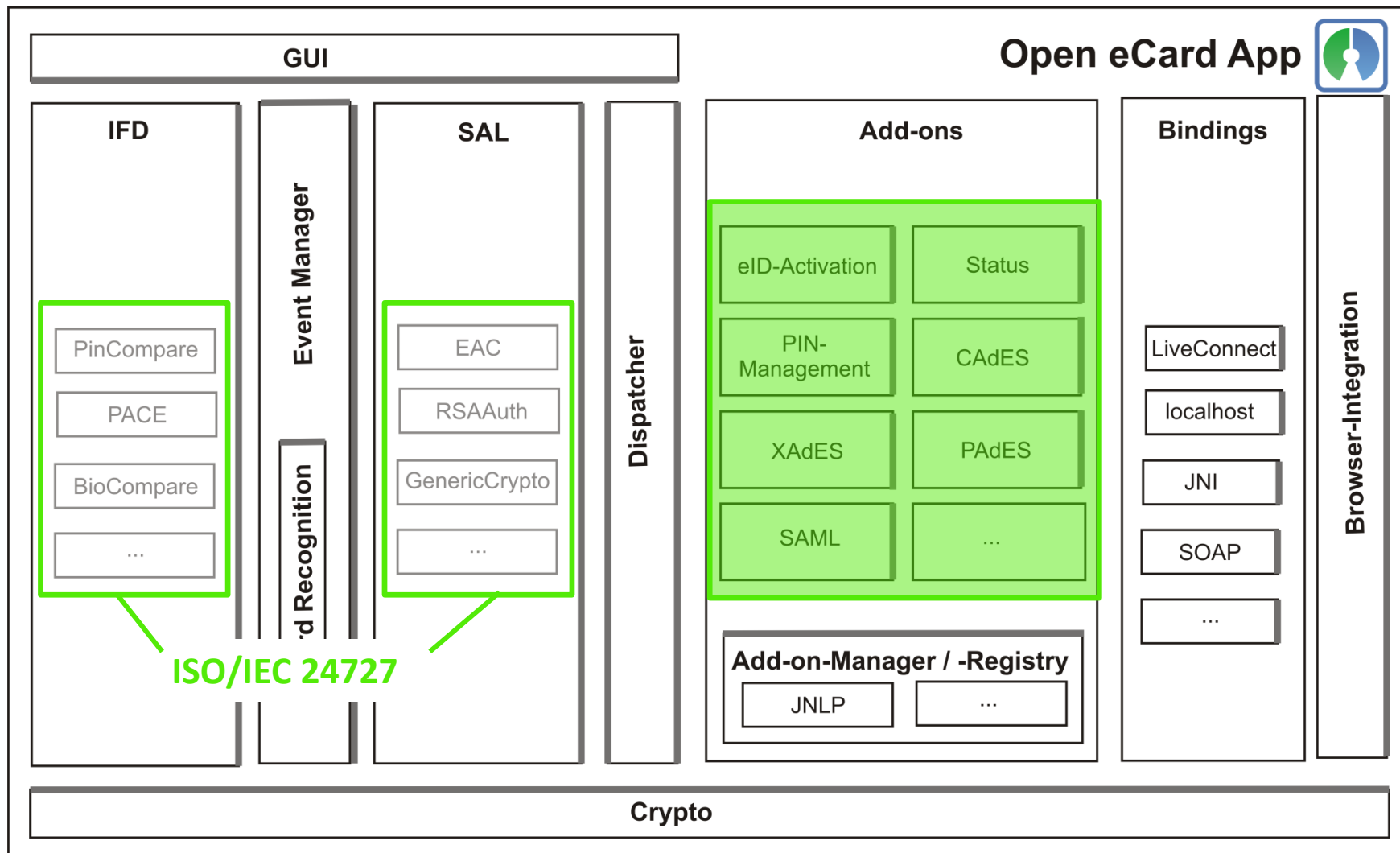


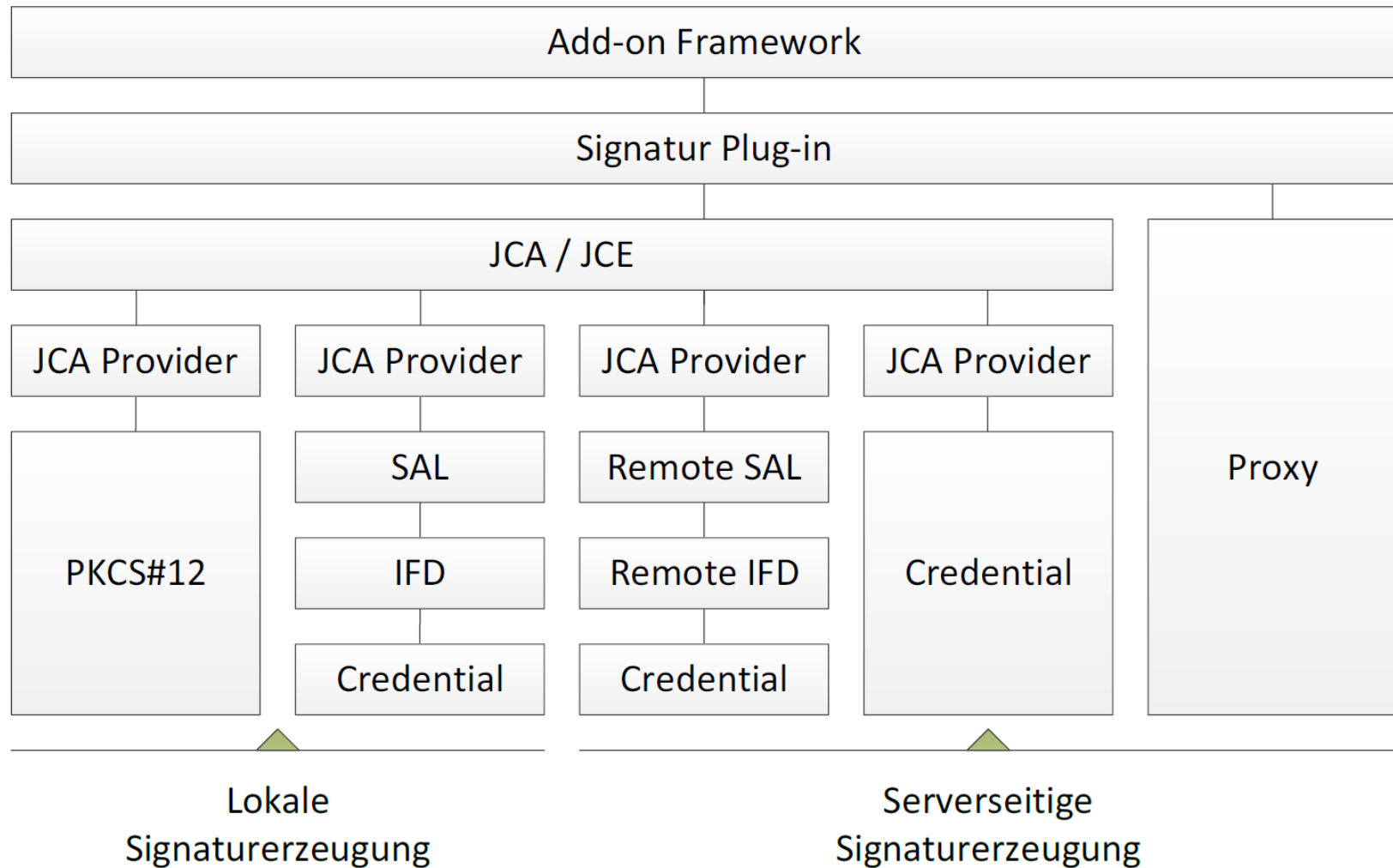




- eID-Client gemäß BSI-TR-03112 / BSI-TR-03124
 - Localhost-basierte eID-Aktivierung
 - EAC-basierte Authentisierung
 - TLS-basierte Authentisierung
- Unterstützung für CardInfo-files (CIF) gemäß ISO/IEC 24727-3
 - Karte wird unterstützt, sobald entsprechendes CIF verfügbar ist
 - Existierende CIF für Personalausweis, Gesundheitskarte, e-Arzttausweis light, e-card (AT), Estonian eID, diverse Signatur- und Bankkarten (D-Trust, S-Trust, GAD, DATEV etc.)
- Plattform-unabhängige GUI-Schnittstelle
- Modulare Architektur
- Clients für Java SE (Desktop & Applet) und Android

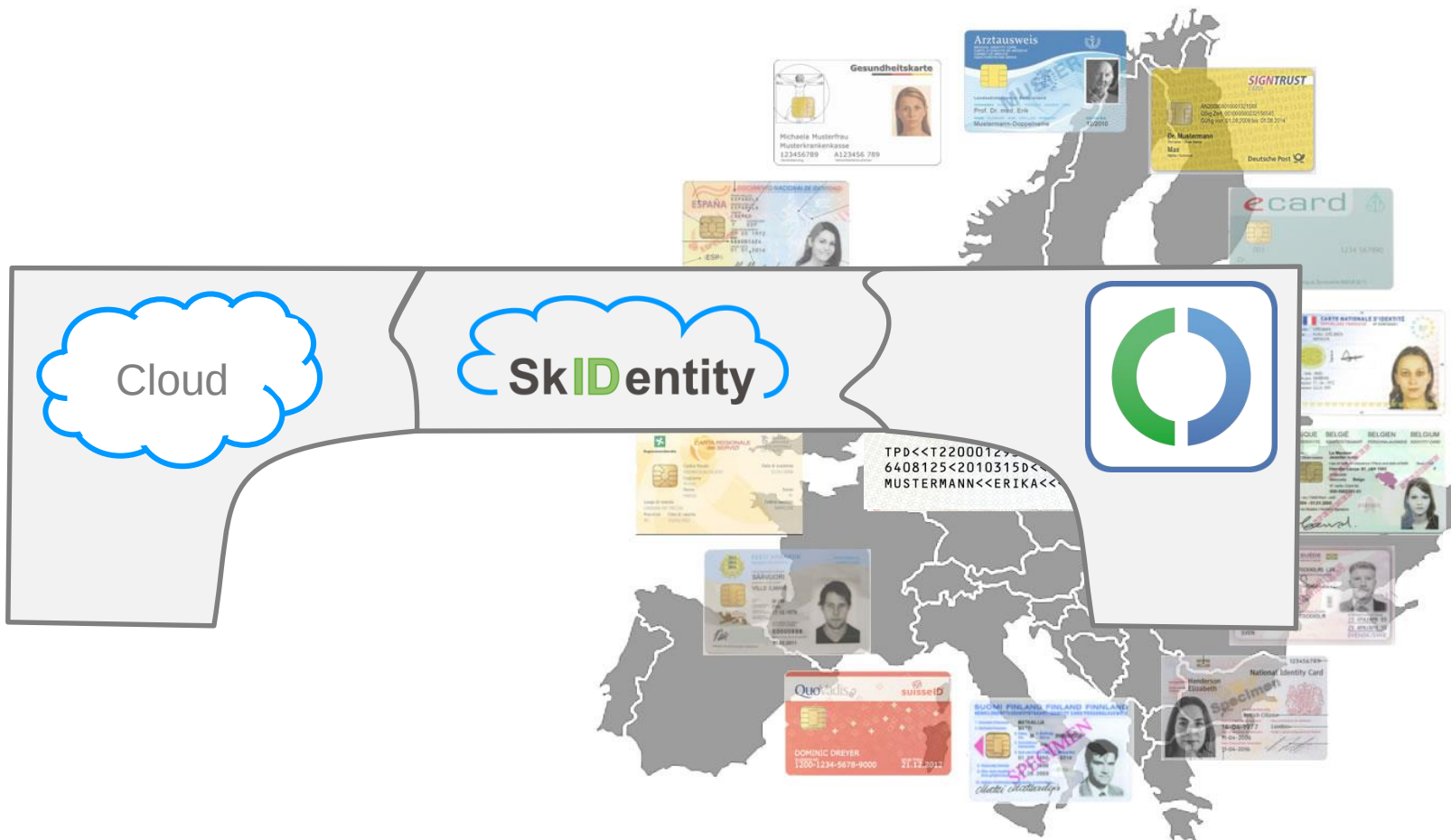
<http://openecard.org>





aus: David Derler, Christof Rath, Moritz Horsch, Tobias Wich: „*Design und Implementierung eines Localhost Signaturgateways*“, Proceedings D-A-CH Security 2014

- Einleitung
- Offene Initiativen
 - ETSI/CEN M/460
 - Open Signature
 - Open eCard
 - **SkIDentity**
 - Common-eID
 - FutureID
- Zusammenfassung

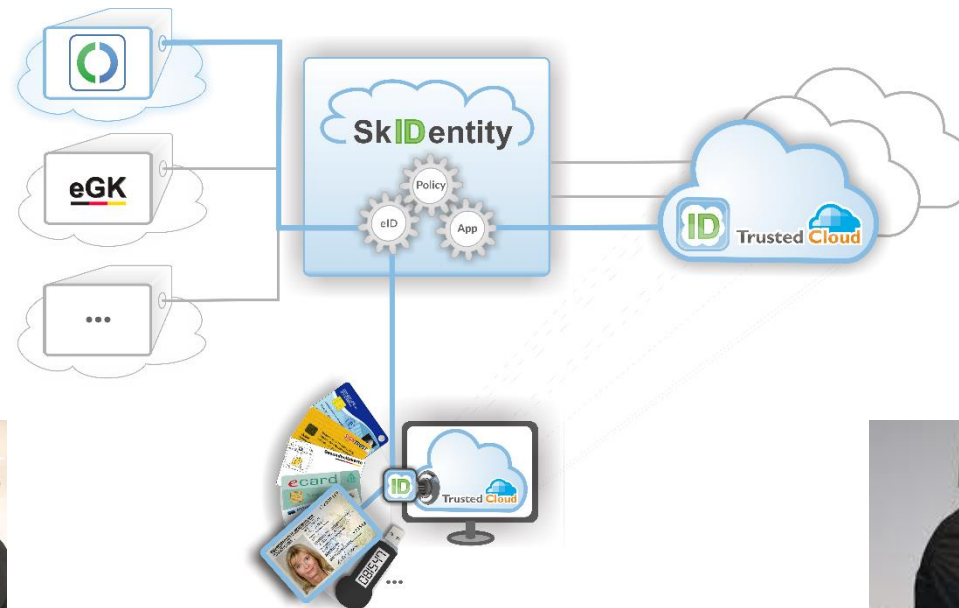




Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages



<http://trusted-cloud.de>



Deutschland
Land der Ideen



Ausgewählter Ort 2013/14

Nationaler Förderer
Deutsche Bank



<http://www.land-der-ideen.de/>

<http://BürgerCloud.de>



Bundesverwaltungsamt

Bundesverwaltungsamt, 50728 Köln

ecsec GmbH
z.Hd. Herrn Dr. Hühnlein
Sudetenstraße 16
96247 Michelau

HAUSANSCHRIFT: Barbarastr. 1, 50735 Köln
POSTANSCHRIFT: 50728 Köln
TELEFON: +49(0)22899358-3300 oder +49(0)221 758-3300
TELEFAX: +49(0)2289910358-1357
ANSPRECHPARTNER: Oliver-Stephan Jolk
E-MAIL: oliver-stephan.jolk@bva.bund.de
INTERNET: www.bundesverwaltungsamt.de

Ihr Zeichen, Ihre Nachricht vom
Antrag auf ein Berechtigungs-
zertifikat vom 22.08.2014

Mein Zeichen, meine Nachricht vom
VfB-01.02.05-6657-37309

Datum
01.09.2014

Erteilung einer Berechtigung nach § 21 des Gesetzes über Personalausweise und elektronischen Identitätsnachweis (PAuswG) und § 78 Aufenthaltsgesetz (AufenthG)

Sehr geehrte Damen und Herren,

auf Ihren Antrag vom 22.08.2014 erteile ich Ihnen die Berechtigung, für die Wahrnehmung Ihrer Aufgaben bzw. Ihres Geschäftszwecks

- Management von Cloud Identitäten (SkIDentity) -

Daten im Wege des elektronischen Identitätsnachweises bei Inhabern des Personalausweises und des elektronischen Aufenthaltstitels mittels eines Berechtigungszertifikates anzufragen.

Die Berechtigung wird Ihnen erteilt für:

ecsec GmbH
Sudetenstraße 16
96247 Michelau
detlef.huehnlein@ecsec.de

Seite 1 von 3

Diensträume
Barbarastr. 1, Köln (Rhein)
Erreichbar mit öffentlichen Verkehrsmitteln
Straßenbahnlinie 13 und 15, Bushaltestelle 140,
Haltestelle: Amsterdamer Straße/Gürtel

Servicezeit
Besuche und Anrufe bitte möglichst
Mo.-Fr. 08.00 – 16.30 Uhr

Überweisungsempfänger
Bundeskasse Trier
Konten
Deutsche Bundesbank Filiale Saarbrücken
IBAN: DE81590000000059001020
BIC:

Die Berechtigung wird für folgende Datenfelder erteilt:

- Familienname (§ 18 Abs. 3 Nr. 1 PAuswG)
- Vornamen (§ 18 Abs. 3 Nr. 2 PAuswG)
- Tag der Geburt (§ 18 Abs. 3 Nr. 4 PAuswG)
- Ort der Geburt (§ 18 Abs. 3 Nr. 5 PAuswG)
- Anschrift (§ 18 Abs. 3 Nr. 6 PAuswG)
- dienste- und kartenspezifisches Kennzeichen (§ 18 Abs. 3 Nr. 8 PAuswG)

Auf der Grundlage dieser Berechtigung darf Ihnen von einem Berechtigungszertifikateanbieter ein Berechtigungszertifikat für den elektronischen Identitätsnachweis bereitgestellt werden. Das Berechtigungszertifikat darf eine Gültigkeitsdauer bis zum 31.08.2017 nicht überschreiten und ist alle 2 Tage bei dem von Ihnen ausgewählten Berechtigungszertifikateanbieter zu erneuern. Sie sind verpflichtet, die Bereitstellung eines Berechtigungszertifikates unter Nennung des Berechtigungszertifikateanbieters unverzüglich anzuzeigen.

Die für Sie zuständige Datenschutzbehörde ist:

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27
91522 Ansbach
0981/53-1300
poststelle@lda.bayern.de

Für die Erteilung dieser Berechtigung erhebe ich gemäß § 3 Nr. 1 PAuswG GebV eine Gebühr in Höhe von **102,00 €**.

Überweisen Sie diese Gebühr bitte innerhalb einer Frist von 10 Tagen nach Zustellung dieser Berechtigung an:

Kontoinhaber: Bundeskasse Trier
Bankverbindung: IBAN: DE81590000000059001020
BIC: MARKDEF1590 (für Auslandszahlungen)
Deutsche Bundesbank – Filiale Saarbrücken

Verwendungszweck: 115752088908, ecsec GmbH

Hinweis: Bitte stellen Sie unbedingt sicher, dass die Gebühr in voller Höhe bei der Bundeskasse Trier unter Nennung des o. a. Verwendungszwecks eingeht, um eine sichere Zuordnung Ihrer Zahlung zu gewährleisten. Bei Nichtzahlung der Gebühr liegt eine Ordnungswidrigkeit vor, die mit einem Bußgeld von bis zum 30.000,00 € geahndet werden kann.

Seite 2 von 3

Diensträume
Barbarastr. 1, Köln (Rhein)
Erreichbar mit öffentlichen Verkehrsmitteln
Straßenbahnlinie 13 und 15, Bushaltestelle 140,
Haltestelle: Amsterdamer Straße/Gürtel

Servicezeit
Besuche und Anrufe bitte möglichst
Mo.-Fr. 08.00 – 16.30 Uhr

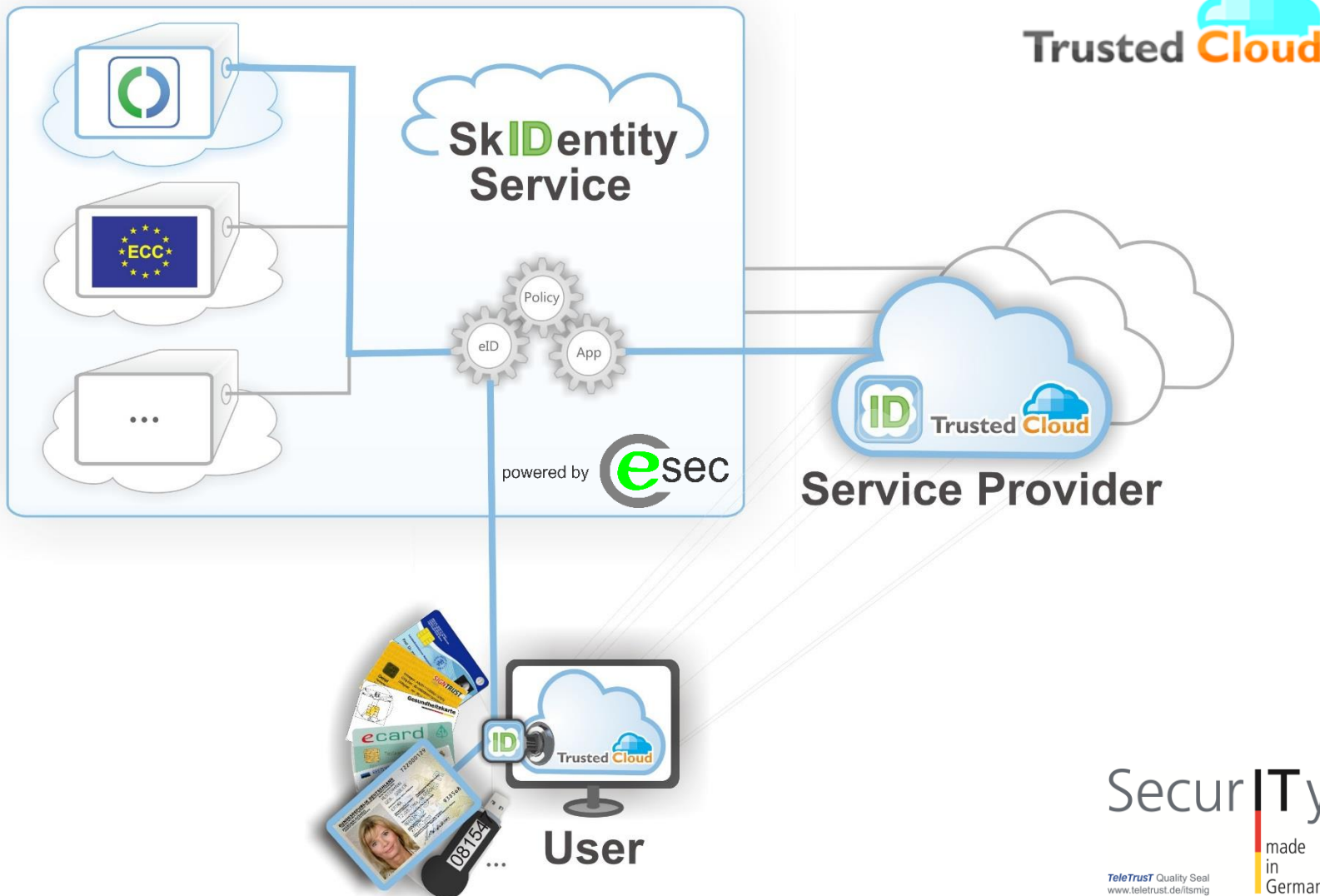
Überweisungsempfänger
Bundeskasse Trier
Konten
Deutsche Bundesbank Filiale Saarbrücken
IBAN: DE81590000000059001020
BIC:

Gefördert durch:



Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages



Deutschland
Land der Ideen



Ausgezeichneter Ort 2013/14

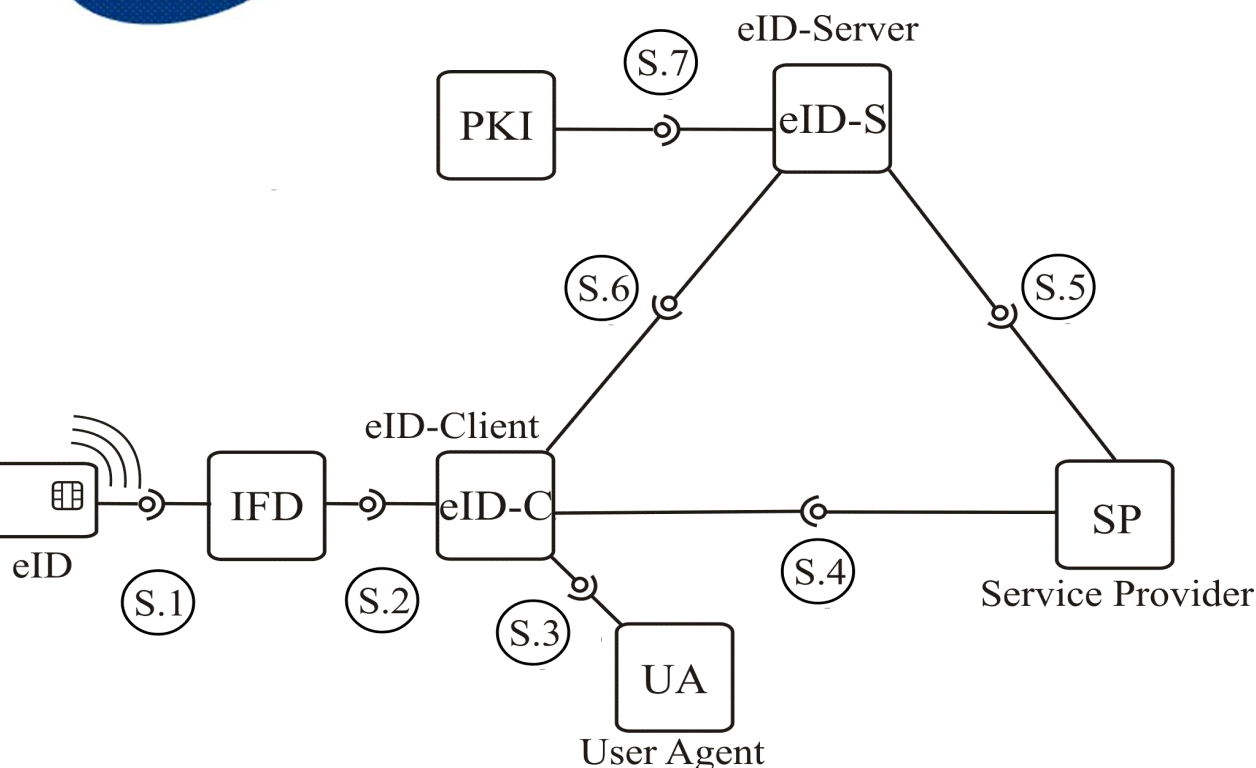
Nationaler Förderer
Deutsche Bank



SecurITy
made
in
Germany

TeleTrust Quality Seal
www.teletrust.de/itsmig

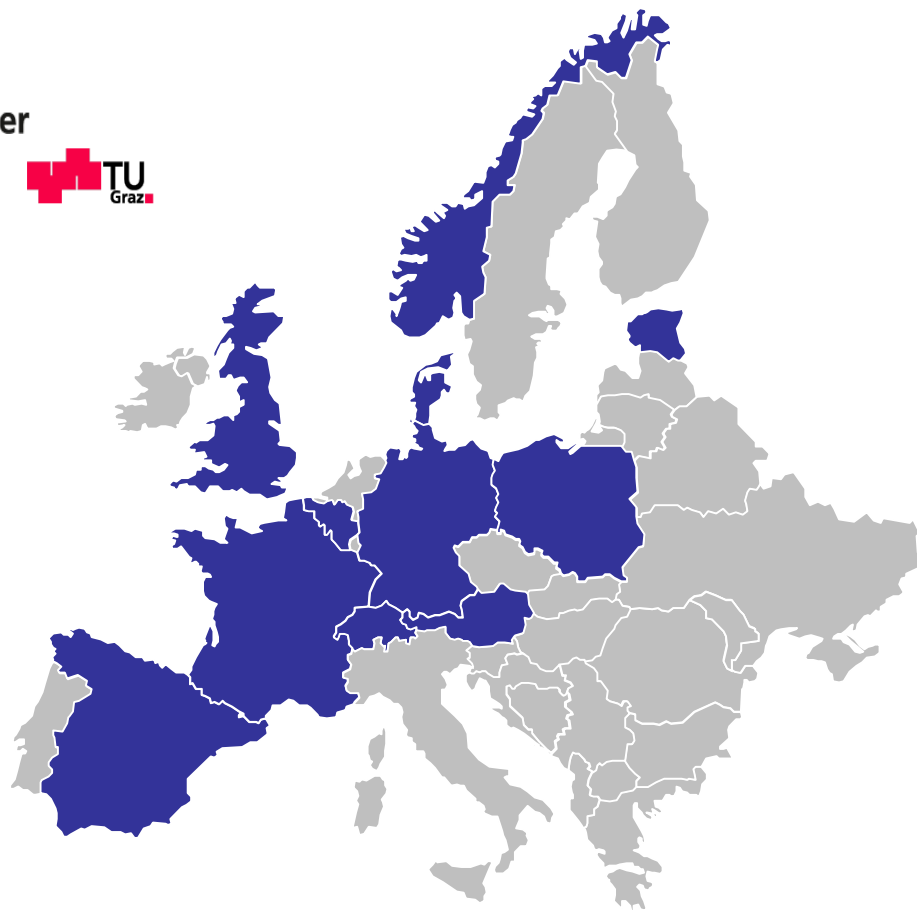
- Einleitung
- Offene Initiativen
 - ETSI/CEN M/460
 - Open Signature
 - Open eCard
 - SkIDentity
 - **Common-eID**
 - FutureID
- Zusammenfassung



com- plianz	Legacy- TL Ss	Ignore- N Ss	sessi- onida	CARs	functi- onala
nein	x			x	nein
nein	x			x	nein
nein	x	x		x	ja
nein		x		x	ja
nein		x		x	ja
nein				x	ja
ja					ja
nein				x	ja
nein				x	ja
nein				x	ja
ja					ja
nein		x		x	ja
ja					ja
nein				x	ja
nein		x		x	ja
ja					ja
ja					ja

<http://common-eid.org/>

- Einleitung
- Offene Initiativen
 - ETSI/CEN M/460
 - Open Signature
 - Open eCard
 - SkIDentity
 - Common-eID
 - FutureID
- Zusammenfassung



<http://FutureID.eu>





- Einleitung
- Offene Initiativen
 - ETSI/CEN M/460
 - Open Signature
 - Open eCard
 - SkIDentity
 - Common-eID
 - FutureID
- **Zusammenfassung**

- eIDAS-Verordnung bringt **Chancen** für leichtere Nutzung von Authentisierung und Signatur in Europa
- Wesentliche Meilensteine schon in 2015, 2016 und 2018
- Aktuell diverse offene Initiativen im eIDAS-Umfeld
 - Standardisierung insbesondere bei ETSI / CEN
 - Nationale Abstimmung (z.B. bei BMWi, BNetzA, BMI, BSI, TeleTrust, BITKOM)
 - Initiativen für Transparenz und Interoperabilität (z.B. Open Signature, Common-eID)
 - Offene Technologien für leichte Nutzbarkeit (z.B. Open eCard, SkIDentity, FutureID)
- **Seien Sie offen und nutzen Sie die Chancen!**

Herzlichen Dank für Ihre Aufmerksamkeit!

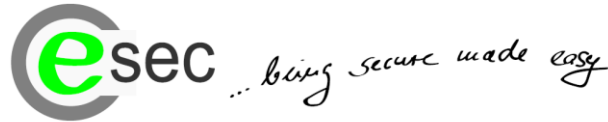
Deutschland
Land der Ideen



Ausgezeichneter Ort 2013/14

Nationaler Förderer
Deutsche Bank 

Kontakt



ecsec GmbH

Sudetenstr. 16
96247 Michelau, Germany
Telefon + 49 9571 896479
Mobil + 49 171 9754980
detlef.huehnlein@ecsec.de
<http://www.ecsec.de>

Dipl.-Inform. (FH)
Dr. Detlef Hühnlein
Geschäftsführer