



Ulrich Emmert

Rechtsanwalt
Partner esb Rechtsanwälte
Lehrbeauftragter für
Wettbewerbs-, Urheber-
und Onlinerecht an der
Hochschule für Wirtschaft
und Umwelt in Nürtingen
Vorstand Reviscan AG
Vorstand des VOI e.V.

Informationssicherheit
Security Policies
Datenschutz
E-Mail-Archivierung
Haftungsrecht / AGB
Lizenzverträge
Unternehmensverkäufe
Kleine AG
Umwandlung

esb Rechtsanwälte PartG
Schockenriedstr. 8A
70565 Stuttgart
Tel. 0711/469058-0
Fax 0711/469058-99
ulrich.emmert@kanzlei.de

www.kanzlei.de
www.esb-rechtsanwaelte.de
www.emmert.de



Die neue EU-Signaturverordnung

Ulrich Emmert - esb Rechtsanwälte



SIEMENS



IBM



hp



T



AT&T



BT



COLT



EMC²
where information lives[®]



CISCO SYSTEMS



FUJITSU



EnBW



VATTENFALL



DIHK



Bundeswehr



EADS



Ohh... find'ich gut'



Roland Berger
Strategy Consultants



KPMG



DEKRA



Sun
microsystems



BECHTLE



F-Secure



NetApp



Deka
Investmentfonds



symantec



nextiraOne



ALCATEL



WEBSense

Stand 2014:

- 21 Mio KMU Kleine und mittlere Unternehmen
- 13 Mio EU Bürger arbeiten in einem anderen EU Mitgliedsstaat
- 150 Mio EU Bürger shoppen Online; nur 20% davon kaufen aus einem anderen EU Mitgliedsstaat

Daher:

- Elektronischen Zugang erleichtern
- Grenzüberschreitende elektronische Nutzung fördern
- Vertrauen und Sicherheit stärken
- Elektronischen „Vertrauensdiensten“ den selben Wert verleihen wie in der „Papierwelt“



Signaturgesetz 1997

- hoher Sicherheitsstandard
- Genehmigung BNA

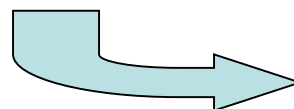
EU-Richtlinie
1999/93/EG

Signaturgesetz 2001

- Anpassung an EU-Richtlinie
- 2 Sicherheitsstufen

Signaturgesetz 2005

- Anpassung an
Massensignaturen
- Remotesignaturen /
Stichproben möglich



EIDAS-Verordnung 2014



Primäres Gemeinschaftsrecht (EU-Verträge)

Sekundäres Gemeinschaftsrecht
z.B. europäische Signaturverordnung



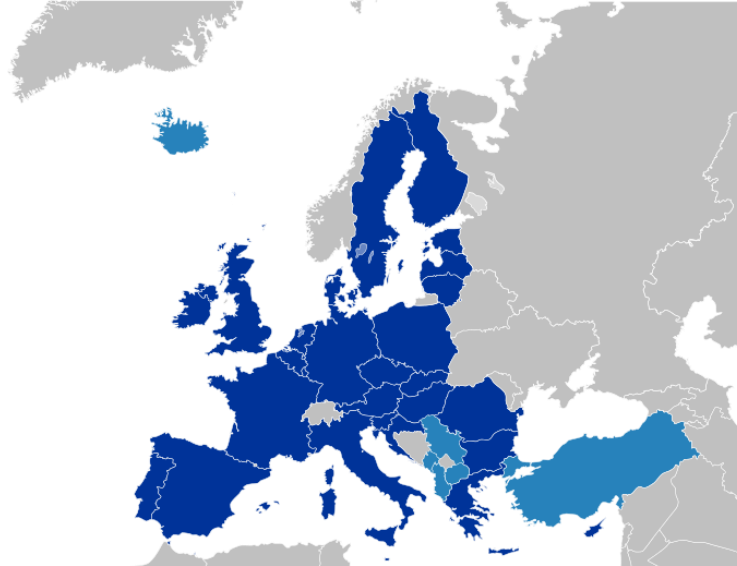
Nationales Verfassungsrecht
deutsches Grundgesetz

Übriges Bundesrecht




Landesrecht

- **Verordnungen**
 - Direkte Geltung in der ganzen EU ohne Umsetzung
 - EIDAS-VO



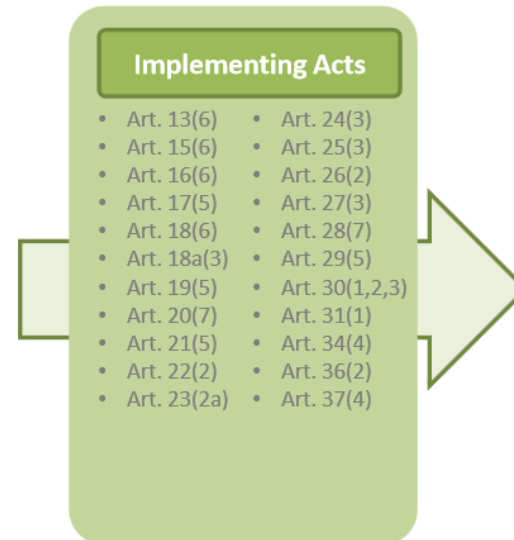
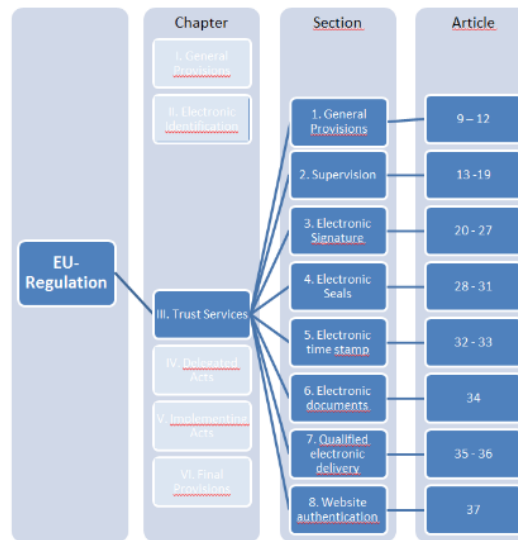
- **Richtlinien**
 - Vorgaben an Mitgliedsstaaten
 - Umsetzung in nationales Recht notwendig
 - Einräumung einer Umsetzungsfrist
 - Danach in Mitgliedsstaaten ohne Umsetzung direkte Geltung der Richtlinie

- 
- 2011: Kommissions-Vorschlag zur Überprüfung der eSignatur-Richtlinie, um einen Rechtsrahmen für die grenzübergreifende Anerkennung und Interoperabilität gesicherter elektronischer Authentifizierungssysteme zu schaffen
 - –2012: Kommissions-Vorschlag für einen Beschluss zur EU-weiten gegenseitigen Anerkennung der elektronischen Identität und Authentifizierung.
 - –2012-2014: Einführung und Anwendung von eID-Systemen in den Mitgliedsstaaten

- 28.08.2014 Veröffentlichung im Amtsblatt der EU
- Entwicklung der Durchführungsbestimmungen z.B. nach Art. 8 der VO
- Freiwillige Anerkennung der eID ab September 2015
- Anwendungsbeginn Vertrauensdienste 1.7.2016
- Verpflichtende Anerkennung der eID September 2018




Legal Framework



Technical Framework




- 
- Kapitel I: Allg. Bestimmungen
 - Kapitel II: **Elektronische Identifizierung**
 - Kapitel III: **Vertrauensdienste**
 - Kapitel IV: Delegierte Rechtsakte
 - Kapitel V: Durchführungsrechtsakte
 - Kapitel VI: Schlussbestimmungen
 - 4 Anhänge (Anforderungen an qual. Zertifikate/ Signaturerstellungseinheiten/ el. Siegel/ Website-Authentifizierung)

- Einfache Signaturen
- Fortgeschrittene Signaturen
- qualifizierte Signaturen
- eID-Verfahren der Mitgliedsländer




- "**Elektronische Identifizierung**" ist der Prozess der Verwendung von Personenidentifizierungsdaten in elektronischer Form, die eine natürliche oder juristische Person oder eine juristische Person vertretende natürliche Person eindeutig repräsentieren
- "**Personenidentifizierungsdaten**" sind ein Datensatz, der es ermöglicht, die Identität einer natürlichen oder juristischen Person oder einer eine juristische Person vertretenden natürlichen Person festzustellen
- "**Elektronisches Identifizierungsmittel**" ist eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird


- 
- § 8 EIDAS VO
 - Niedrig – Substanziell - Hoch
 - Kriterien werden erst durch Durchführungsrechtsakt festgelegt
 - eID-Verfahren der Stufen substanziell und hoch müssen von den anderen Mitgliedsstaaten anerkannt werden
 - Es können Mindestlevels für einzelne Verfahren festgelegt werden
 - Für eID-Verfahren privater Anbieter nicht verpflichtend

- Keine übergeordnete Stelle
- Notifikation durch Mitgliedsstaaten
- Haftung der notifizierenden Mitgliedsstaaten und der Dienstleister




- 
- Elektronische Signaturen
 - Elektronische Siegel
(Organisationszertifikat)
 - Elektronische Zeitstempel
 - Elektronische Dokumente
 - Elektronische Zustelldienste
 - Website Authentifizierung

- Qualifizierte/ Nicht-qualifizierte Vertrauensdiensteanbieter
- Haftung: Beweislastumkehr bei qual. Vertrauensdiensteanbieter
- Aufsicht über qual. Vertrauensdiensteanbieter / na Nachträgliche Kontrolle bei nicht-qual. Vertrauensdiensteanbieter
- Anforderungen an IT-Sicherheit an Vertrauensdiensteanbieter mit Meldepflichten bei Kompromittierungen (alle Anbieter)
- Audit und Konformitätsprüfungen der qual. Vertrauensdiensteanbieter
- Vorabgenehmigungsverfahren für qual. Vertrauensdiensteanbieter und Vertrauensliste (TL) mit konstitutiver Wirkung
- „Gütezeichen“ (trustmark) für qual. Vertrauensdienste
- Anerkennung von qual. Vertrauensdiensteanbieter aus Drittstaaten nur bei Abkommen mit EU

- 
- A vertical image on the left side of the slide shows a close-up of a fountain pen nib, with the pen body extending downwards. The image is in a light blue, semi-transparent style.
- Identifikationsmechanismen bei Ausgabe von qual. Zertifikaten
 - Verlässlichkeit Mitarbeiter
 - Finanzielle Mindestanforderungen/
Versicherungspflicht
 - Informationspflichten
 - Sicherheitsanforderungen bzgl. Systeme und Produkte
 - Dokumentationspflichten
 - Verzeichnis- und Sperrdienste etc.
 - Notfallpläne zur Sicherstellung der Business Continuity


- Ähnlich wie im dt. SigG seit 2005
- Möglichkeit der Massensignatur
- Serversignaturen und Remotesignaturen sind möglich
- Siegel: Organisationszertifikate können für jur. Personen / Personenmehrheiten ausgestellt werden (bisher nicht möglich)





- 
- Erbringung nur durch Qualifizierten Vertrauensdiensteanbieter
 - Korrekte Identifizierung von Absender und Empfänger
 - Integritätsschutz durch fortgeschrittenes Zertifikat des TSP
 - Änderung der Daten bei Kenntlichmachung möglich
 - Absendung, Änderung und Empfang muss durch einen qualifizierten Vertrauensdienst belegt werden

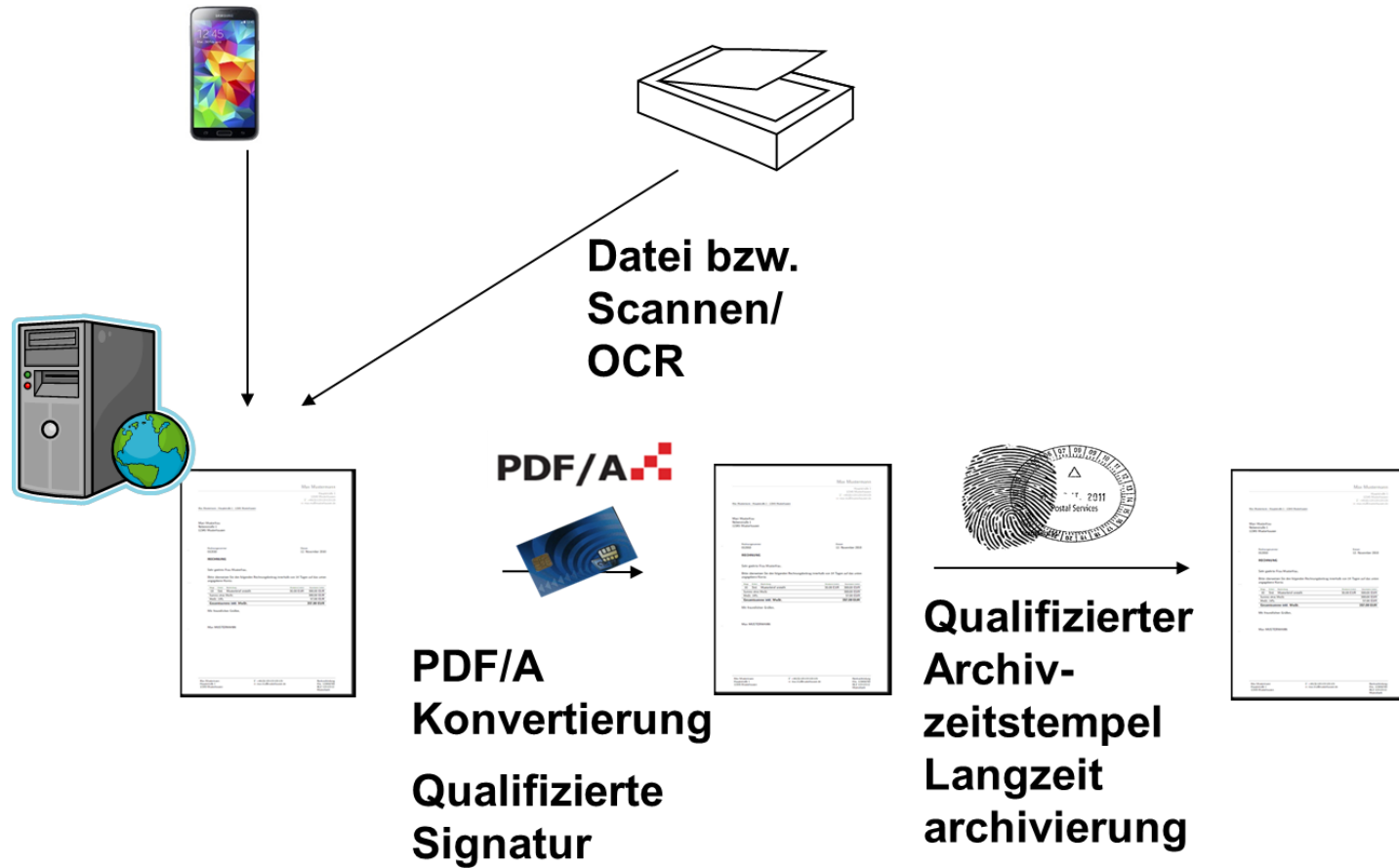
- Qual. Validierungsdienste von Signaturen können nur von qualifizierten Vertrauensdiensteanbietern nach Art. 33 erbracht werden
- Kann fortgeschrittene Signatur des qual. Vertrauensdiensteanbieters enthalten
- Qual. Archivierungsdienste können nur von qualifizierten Vertrauensdiensteanbietern nach Art. 34 erbracht werden



- 
- Kein echter Vertrauensdienst
 - Einem elektronischen Dokument darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in elektronischer Form vorliegt.
 - In Deutschland durch Justizkommunikationsgesetz 2005 und E-Justiz-Gesetz 2013 bereits eingeführt

- 
- § 416 ZPO Privaturkunde kann durch qualifizierte Signatur weitgehend beweiserhaltend digitalisiert werden (Verfahrensbeschreibung erforderlich)
 - § 437 ZPO Öffentl. Urkunde birgt auch Vermutung der Richtigkeit
 - Die §§ 371a, 371b, 416 und 437 ZPO sind auf elektronische Dokumente bei Verwendung elektronischer Signaturen entsprechend anwendbar
 - Erschütterung der Beweiskraft ist möglich, wenn durch Tatsachen ernstliche Zweifel am Aussteller bestehen

- 
- Bisher keine Ausführungsbestimmungen vorhanden
 - Browserhersteller fast ausschließlich außerhalb der EU
 - Wirtschaftlicher Druck zur Anpassung zukünftig möglich



Schulungen

Internet-Sicherheit
Datenschutz
Urheberrecht

Workshops

Security Policies
Nutzungsbedingungen
Haftungsklauseln
Einführung von PKI-Systemen

Datenschutz- und
Datensicherheitskonzepte
E-Mail Archivierungslösungen
VoIP und Mobile Security

Beratung

Internet-Sicherheit
Datenschutz
AGB
Vertragsgestaltung, z.B.
Lizenzverträge, ASP-,
Outsourcing-, Hosting-,
Wartungs-Verträge
Existenzgründungsberatung
Business Pläne

Auditing

Security Policies
IT Risk Management
Datenschutzaudit
Datenschutzbeauftragter