EIDAS: INNERSTAATLICHE UMSETZUNG EINES NICHT UMSETZUNGSBEDÜRFTIGEN EU-RECHTSAKTES

Alexander Konzelmann

Abteilungsleiter, Richard Boorberg Verlag GmbH Co KG, Abteilung Rechtsdatenbanken
Scharrstraße 2, 70563 Stuttgart, DE
a.konzelmann@boorberg.de; http://www.boorberg.de

Schlagworte: ***eIDAS-Verordnung, Europarecht, Signaturgesetz, Vertrauensdienstegesetz, digitale Signatur, Fernsignatur, Vertrauensdienste, Zeitstempel, Siegel, Deutschland, Anbieter von Identifikations- und Vertrauensdiensten, Vertrauensliste, trusted list***

Abstract: *Nach dem Inkrafttreten der eIDAS-Verordnung (EU) Nr. 910/2014 am 1. Juli 2016 soll über die legislativen und praktischen Auswirkungen berichtet werden, die in Deutschland eintreten oder eingetreten sind.*

1. Überblick zum Inkrafttreten der eIDAS-VO und zum Entwurf des Vertrauensdienstegesetzes

1.1. Für Deutschland neuartige digitale Signaturen

Die Verordnung (EU) Nr. 910/2014 gilt unmittelbar und ersetzt das Framework der bisherigen Signaturrichtlinie 1999/93/EG. Die Richtlinie war zur Umsetzung durch nationale Regelungen bestimmt und führte zu einer Diversifikation, die einer rechtlich abgesicherten und vertrauensbildenden EU-weiten einheitlichen digitalen Kommunikation im Wege steht. Im zweiten Anlauf erließ die EU nach ausgiebigen Tests und unter Beteiligung öffentlicher und privater interessierter Stellen eine Verordnung. Diese regelt aber nicht mehr nur digitale Signaturen, sondern auch das gesamte technische und infrastrukturelle Umfeld. Aufgrund der Vorbereitungsphasen konnten die technischen Durchführungsvorschriften und die erforderlichen Standards parallel entwickelt werden und sie wurden ungefähr gleichzeitig mit der Verordnung publiziert. Die eIDAS-Verordnung verbietet keineswegs abweichende oder kompliziertere nationale Regeln zur digitalen Signatur und zu Vertrauensdiensten wie Zeitstempeln, elektronischen Einschreiben und Identifizierungsdiensten. Sie besagt aber, dass mit dieser Verordnung konforme technische Produkte EU-weit in eine online verfügbare «Vertrauensliste» (*trusted list*) aufgenommen werden können. Für Identifizierungsdienste haftet dann einerseits der Verantwortliche und auch der notifizierende Mitgliedstaat sowie der das Authentifizierungsverfahren durchführende Beteiligte; andererseits kann kein EU-Mitgliedstaat und kein dem EU-Recht unterliegender Adressat die Zuordnung einer Signatur anzweifeln, die von einer notifizierten Einrichtung stammt. Der internationale Wettbewerb soll dadurch gestärkt werden.

Während einer Übergangsfrist gelten Diensteanbieter nach altem Recht noch ohne Konformitätsbewertungsberichte auch als Diensteanbieter nach neuem Recht. Allerdings sind alle ausländischen in die Vertrauensliste aufgenommenen Anbieter nunmehr gleichwertige Konkurrenten. Zum Beispiel kann theoretisch die österreichische Handy-Signatur für deutsche Nutzer angeboten werden; diese ist für den Nutzer bequemer als die an ein Kartenlesegerät gebundene Signatur mit dem neuen deutschen Personalausweis. Die e-Residency-Card aus Estland[1] ist schon in Betrieb genommen und soll nach Herstellung der vollen Interoperabilität im Jahr

[1] http://www.howtostayin.eu/ (alle Websites aufgerufen am 23. Januar 2017), «About us», 2. Absatz, zur EIDAS-Konformität.

2018 europaweit gültiges elektronisches Signieren erlauben. Bei Signaturen ist für Deutschland neu, dass man das Schlüsselpaar nicht mehr selbst verwalten muss, sondern es kann von einem Dritten kommen, der einen authentifiziert hat. Dies betrifft Dienste wie SMS-TAN und «fernausgelöste» online-Signaturen. SMS-TANs werden häufig von Kreditkartenunternehmen als Sicherheitsfeature angeboten. Wenn nämlich die Informationen auf und in der Karte, die einem unbefugten Nutzer (Dieb, Räuber, Erpresser) gleichzeitig zugänglich werden können, mit einer weiteren Information verknüpft werden müssen, die den Besitz eines definierten Kommunikationsgerätes des Befugten im Zeitpunkt der TAN-Übermittlung voraussetzt, dann erhöht dies im Normalfall den Aufwand an krimineller Energie zur Durchführung einer wirksamen Täuschung. Auf dieselbe Weise können solche TANs auch zu reinen Identifikationszwecken verwendet werden: indem ein Dritter live online bestätigt, den Anforderer der TAN identifizieren zu können, erhöht er das Vertrauen eines noch unbekannten Vertragspartners in die elektronische Identität, welche der Anforderer in Anspruch nimmt. Damit kann ein externer Schlüsselverwalter eine Art Signatur mindestens gleich gut bereitstellen, wie es der Besitz einer Ausweiskarte und die Kenntnis einer PIN tun kann.

1.2. Zuständigkeiten und erste Diensteangebote

Die bundesdeutschen Zuständigkeiten für die Neuerungen aus der eIDAS-Verordnung sind bereits geregelt: die Bundesnetzagentur sorgt für die Konformität von Siegeln, Zeitstempeln und Signaturen, das Bundesamt für Sicherheit in der Informationstechnik (BSI) für SSL-Website-Zertifikate. Die Aufsichtsstellen und Zertifizierungsstellen sind an die Kommission gemeldet. Die ersten Verfahren sind ebenfalls in die Vertrauensliste aufgenommen, z.B. elektronischer Ausweis und DE-Mail. Die Bundesdruckerei hat eine 100%-Tochter D-Trust. Diese wird ab 2017 alle eIDAS-Standards einhalten und alle Dienste anbieten außer Einschreiben. Bereits jetzt wirbt sie mit Signaturen, Signaturkarten, persönlichen und Firmen-Identitätszertifikaten, Verschlüsselungstechnologie und Webserverzertifikaten. Andere deutsche Unternehmen sind aber auch bereits dabei, eIDAS-konforme Vertrauensdiente anzubieten. Künftig können und werden auch Banken eID-Provider sein, denn sie haben ihre Kunden bereits alle identifiziert.

1.3. Gesetzentwurf

Das VertrauensdiensteG löst die bisherigen Regelungen zur digitalen Signatur (SigG und SigV) ab, denn deren zum Teil engere Regeln werden durch die eIDAS-Verordnung derart überlagert, dass Verwirrung über nicht anwendbare Gesetzeswortlaute entstehen würde. Dieses neue Gesetz soll laut Plan im Jahr 2016 in der Bundesregierung beschlossen werden und im 2. Quartal 2017 in Kraft treten. Darin müssen z.B. die wichtigen Beweisregeln in §§ 126a BGB, § 37 Abs. 4 VwVfG und § 371b ZPO daran angepasst werden, dass nicht nur Signaturen, sondern auch Siegel Unterschriften gleichgestellt sind. Der Beitrag gibt nachfolgend einen Überblick über die geplanten ***Neuregelungen (2)***, über den ***Verfahrensstand (3)*** und über die laut Vertrauensliste bereits am Markt befindlichen deutschen (und teilweise nichtdeutschen) Anbieter sowie den **Stand der deutschen Vertrauensliste (4)**.

2. Spezielle Auswirkungen der eIDAS-Verordnung auf die deutsche Gesetzgebung im Rahmen des Vertrauensdienstegesetzes

Weil die Möglichkeit einer reinen Software-Signatur vom Archetyp der digitalen Signaturen in den deutschen bisherigen Regelungen stark abweicht und weil auch eine Signatur, die nicht einer natürlichen Person, sondern einer Institution (z.B. Unternehmen, Behörde, juristische Person, Körperschaft) zugeordnet ist, bisher einen Fremdkörper in der deutschen Legislatur zu digitalen Signaturen darstellt, erschien es angezeigt, mit dem Inkrafttreten der unmittelbar geltenden eIDAS-Verordnung auch einen Harmonisierungsprozess im innerstaatlichen Recht anzustoßen. Das zugehörige Projekt heißt Vertrauensdienstegesetz und zeigt, dass die nicht umsetzungspflichtige EU-Verordnung aufgrund ihrer unmittelbaren Geltung doch mindestens genauso stark fühlbare innerstaatlichen Umsetzungsakte auslösen kann wie eine EU-Richtlinie.

2.1. Gliederung

Der Entwurf des deutschen Vertrauensdienstegesetzes enthält mit Stand Ende 2016 die folgenden wichtigen Gliederungspunkte:

§ 1 – Anwendungsbereich,

§ 2 – Aufsichtsstellen: Bundesnetzagentur für e-Signaturen, e-Siegel, e-Zeitstempel, e-Zustelldienste, Bewahrungsdienste; Bundesamt für Sicherheit in der Informationstechnik für Website-Authentifizierung,

§ 3 – Verfahren über den **einheitlichen Ansprechpartner** im Sinne der Dienstleistungsrichtlinie,

§ 4 – Voraussetzungen für **Untersagung des Betriebes** durch die Aufsichtsstelle,

§ 5 – **Mitwirkungspflichten** für Vertrauensdiensteanbieter: Gestattung des Betretens der Geschäftsräume durch Aufsichtsstelle, Vorlage von Schriftstücken, Auskunftserteilung,

§ 6 – Haftung: **Haftung für Dritte** wie für eigenes Handeln,

§ 7 – Datenschutz: Datenerhebung nur unmittelbar bei betroffener Person und sofern für die Erbringung des Vertrauensdienstes erforderlich,

§ 8 – **Vertrauensliste:** geführt durch BNetzA,

§ 9 – **Deckungsvorsorge** in Höhe von mindestens 250.000 EURO für Schaden, der durch ein haftungsauslösendes Ereignis verursacht wurde,

§ 10 – **Identitätsprüfung:** BNetzA legt fest, welche sonstigen Identifizierungsmethoden anerkannt sind und gleichwertige Sicherheit gegenüber persönlicher Anwesenheit bieten; «Vorratsidentifizierung» (Abs. 2),

§ 11 – **Attribute** in qualifizierten Zertifikaten,

§ 12 – Pflicht zur **Unterrichtung über Sicherheitsmaßnahmen** und deren Rechtswirkungen für qualifizierte Diensteanbieter und Nutzer qualifizierter Vertrauensdienste,

§ 13 – **Widerruf qualifizierter Zertifikate**,

§ 14 – **Aufzeichnungen**,

§ 15 – Beendigungsplan und **dauerhafte Prüfbarkeit**,

§ 16 – **Benannte Stellen**: die deutsche Akkreditierungsstelle erkennt private Zertifizierungsstellen an. Das BSI veröffentlicht dazu erforderliche fachliche Kriterien und ist «öffentliche Stelle» gemäß Art. 30 der eIDAS-VO,

§ 17 – Verweis auf Regelungen zu qualifizierten elektronischen **Signaturen**,

§ 18 – Dienste für die Zustellung elektronischer **Einschreiben**,

§ 19 – Bußgeldvorschriften,

§ 20 – Verordnungsermächtigung,

§ 21 – Übergangsvorschriften.

Artikel 2 ff. VDG-E: Folgeänderungen in Fachgesetzen, in denen bestimmte Vertrauensdienste genannt sind; teilweise mit Einführung des elektronischen **Siegels einer juristischen Person** als Äquivalent zur elektronischen Signatur einer natürlichen Person. Z.B. kann nach § 53 Abs. 3 der Vergabeverordnung ein öffentlicher Auftraggeber verlangen, dass Interessenbekundungen, Teilnahmeanträge oder Ähnliches mit einer fortgeschrittenen oder qualifizierten elektronischen Signatur oder entsprechenden Siegeln zu versehen sind.

Parallel zum Gesetz soll wegen der Durchführungsvorschriften zu den Details eine **Vertrauensdiensteverordnung** erlassen werden.

2.2. Bereits bestehende Verpflichtungen zur volldigitalen Kommunikation

Bereits bestehende Pflichten zur volldigitalen Kommunikation können künftig gemäß eIDAS-VO erfüllt werden, auch wenn sie bisher dem Signaturgesetz unterworfen waren. Zur Illustration seien Beispiele aus dem

deutschen öffentlichen Recht genannt, in denen Firmenorgane oder deren Rechtsberater digitale Signaturen abgeben müssen:

- Im elektronischen Mahnverfahren werden Mahnanträge qualifiziert signiert über das elektronische Gerichts- und Verwaltungspostfach (EGVP) eingereicht[2].
- Eine sogenannte Vollständigkeitserklärung bezüglich Angaben für Verkaufsverpackungen müssen ca. 5‘000 Unternehmen in elektronischer Form an ihre IHK senden. Diese Vollständigkeitserklärung muss von einem Wirtschaftsprüfer, Steuerberater, vereidigten Buchprüfer oder unabhängigen Sachverständigen in elektronischer Form testiert werden. Die Bestätigung der Prüfung erfolgt durch eine qualifizierte elektronische Signatur[3].
- Ausschreibungen des Bundes über die e-Vergabe-Plattform www.evergabe-online.de werden vollständig elektronisch abgewickelt[4]. Bieter müssen dafür Identitäts-Zertifikate vorhalten (z.B. von D-Trust oder Telesec[5]).
- Anträge auf Ausgleich gemäß dem Erneuerbare-Energien-Gesetz müssen in elektronischer Form mit qualifizierter Signatur gestellt werden[6].
- Die elektronische Steuererklärung über das Portal www.elsteronline.de der Finanzverwaltung erfordert von Steuerberatern ebenfalls das Vorhalten eines Zertifikats, wobei die Infrastruktur von elsteronline.de die Erteilung und Verwaltung von Zertifikaten für Personen und Institutionen umfasst[7].
- Eine Vielzahl von Schutzrechten kann beim Deutschen Patent- und Markenamt mit einer qualifizierten Elektronischen Signatur angemeldet werden: Für die Patent-, Marken- und Gebrauchsmusteranmeldung sowie die Europäische Patentanmeldung und die PCT-Patentanmeldung steht dieser Weg der rechtswirksamen Online-Kommunikation offen[8]. Das Gleiche gilt für Einsprüche und Beschwerden in Patent- und Markenangelegenheiten.

3. Verfahrensstand VDG-E

Der Referentenentwurf wurde vorerst zur Stellungnahme an sogenannte interessierte Kreise versandt. Erste Stellungnahmen sind auch publiziert worden. Die **Bundesärztekammer**[9] hat sich am 1. November 2016 dahingehend geäußert, dass sie den Entwurf zwar begrüße, dass aber noch weiterer Regelungsbedarf bestehe, der im Gesetzesentwurf nicht berücksichtigt wurde: Hinsichtlich der Aufnahme qualifizierter Attribut-Zertifikate in § 11 sei zuerst ein internationaler Standard für Berufsgruppeninformationen in Attributen festzulegen, um die europaweite Interoperabilität nicht zu gefährden. Und es sei zu regeln, ob die Bestätigung der Attribute durch Signatur, Siegel, Schriftstück oder eine Kombination daraus erfolgen könne. Die Ärztekammer regt die Schaffung eines europäischen Algorithmenkatalogs an, um die Vertrauenswürdigkeit der verschiedenen kryptographischen Algorithmen und Schlüssellängen auch künftig einordnen zu können, nachdem das BSI nicht aufgrund europäischer Regelungen zu einer solchen Publikation verpflichtet sei. Der **Deutsche Industrie- und Handelskammertag DIHT** hat Vorbehalte gegenüber der Anerkennung privater Zertifizierungsstellen in § 16 und schlägt vor, dass die Abnahme und Bewertung auf Korrektheit der Implementierung kryptographischer Algorithmen und Zufallszahlengeneratoren durch das BSI erfolgen und europäische bzw. internationale Standards referenzieren solle. Und der DIHT lehnt die Einführung «gesonderter qualifizierter Zertifikate (qua-

2 § 690 Abs. 3 Satz 2 ZPO.
3 § 10 Abs. 5 VerpackV.
4 § 53 der Vergabeverordnung.
5 Vgl. http://www.evergabe-online.info/e-Vergabe/DE/5%20Service/Unterst%C3%BCtzte%20Zertifikate/node_zertifikate.html.
6 § 66 Abs. 2 EEG 2014.
7 https://www.elsteronline.de/eportal/Oeffentlich.tax.
8 https://www.dpma.de/service/e_dienstleistungen/dpmadirekt/allgemeineinformationen/digitalesignatur/.
9 www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Stellungnahmen/Vertrauensdienstegesetz.pdf.

lifiziertes Attribut-Zertifikat)» gemäß §11 Abs. 3 VDG-E ab, da diese die Interoperabilität, insbesondere bei der Anerkennung durch Behörden anderer EU-Mitgliedstaaten, behinderten. Sie widersprächen auch dem Sinn des Art. 28 Abs. 3 der eIDAS-Verordnung, wonach zusätzliche fakultative die Interoperabilität und Anerkennung qualifizierter elektronischer Signaturen nicht berühren dürfen. Überdies weist er ausführlich darauf hin, dass die Potenziale des in Deutschland erst dank der eIDAS-Verordnung neu geschaffenen Produkts «elektronische Siegel» bei weitem nicht ausgeschöpft würden (Stellungnahme vom 9. November 2016[10]).

Im vollen Wortlaut scheint der Referentenentwurf im Herbst 2016 noch nicht allgemein zugänglich gemacht worden zu sein; die Homepage des Bundeswirtschaftsministeriums fragte bei einer Suche nach dem Stichwort «eIDAS-Verordnung» zurück: «Meinten Sie Adidas-Verordnung?» und hat nur zwei Treffer zum Stichwort «Vertrauensdienste» vorrätig, die beide nicht den Entwurf des Vertrauensdienstegesetzes betreffen. Angesichts der Bedeutung, die dieser Entwurf für die deutsche Wirtschaft haben sollte, erscheinen die amtlichen Veröffentlichungen dazu durchaus sparsam.

4. Aufnahmen in die deutsche Vertrauensliste

Das zentrale Dokument der EU ist die «list of the lists» unter der Adresse https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml. Die darin referenzierte deutsche Vertrauensliste «Trusted List» hat aktuell die Adresse «https://www.nrca-ds.de/st/TSL-XML.xml» und beinhaltet nach eigener Definition Angaben zu den qualifizierten Vertrauensdiensteanbietern, die vom ausstellenden Mitgliedstaat beaufsichtigt werden, sowie Angaben zu den von ihnen angebotenen qualifizierten Vertrauensdiensten gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. Ein Stylesheet ist mit dem XML-Format dieses Dokuments nicht unmittelbar verknüpft, sodass die Liste im Browser ohne Zusatzeinstellungen nicht ganz einfach zu lesen ist. Sie enthielt beim letzten Aufruf am 18. Dezember 2016 unter Anderem folgende Meldungen von Services:

4.1. Staatliche Stellen und staatsnahe Unternehmen

Bundesagentur für Arbeit: Erzeugen und Signieren qualifizierter Zeitstempel in Übereinstimmung mit der lokal geltenden Rechtslage oder mit der Verordnung (EU) Nr. 910/2014, je nachdem, welches Regime zur Zeit in Kraft ist. Die Liste verweist für die Definition und Klassifikation elektronischer Vertrauensdienste auf URI-Adressen, im konkreten Beispiel auf http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST/. Operativ tätig ist hierbei das organisatorisch selbstständige IT-Systemhaus der Bundesagentur für Arbeit; die tatsächliche Kundschaft («Bedarfsträger») scheint auf Stellen der Arbeitsverwaltung beschränkt zu sein. Dennoch ist es sicher sinnvoll, die Infrastruktur dieser Verwaltungseinheit aus Zertifikaten, Signaturen und Zeitstempeln EU-weit als vertrauenswürdig in die Liste aufzunehmen.

Bundesnetzagentur: Nationale Zentralstelle («root») zur Herausgabe von Zertifikaten für Root- Signaturdienste oder qualifizierter Zertifikate für Vertrauensdienste-Anbieter gemäß der Definition unter http://uri.etsi.org/TrstSvc/Svctype/NationalRootCA-QC/ in Übereinstimmung mit dem Europarecht. Und sie ist Herausgeberin der «Trusted List», sogenannter TLIssuer. Zusätzlich ist sie amtliche Aufsichtsstelle als Regulierungsbehörde für Telekommunikation und Post.

Bundesnotarkammer: Registrierung und Zertifizierung von Identitäten inklusive der Erzeugung und des Managements privater Schlüssel und der Vorhaltung einer Infrastruktur zur Validierung der Gültigkeit der ausgegebenen Zertifikate; es soll eine vertrauenswürdige Zertifizierung der Identität der kammerangehörigen Notare auf der Basis EU-konformer digitaler Vertrauensdienste ermöglicht werden. Die Vertrauensliste verweist für das diesbezügliche Tätigkeitsfeld der Notarkammer auf die Definitionen unter http://uri.etsi.org/TrstSvc/

[10] http://www.dihk.de/themenfelder/recht-steuern/rechtspolitik/nationale-stellungnahmen/dihk-positionen-zu-nationalen-gesetzesvorhaben/dihk-stellungname-vertrauensdienste.pdf.

Svctype/CA/QC/ (Identitäten-Management) und http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST (Zeitstempel). Die Bundesrechtsanwaltskammer findet sich nicht auf der Vertrauensliste, denn die Signaturkarte für das besondere elektronische Anwaltspostfach «beA» und die «Bundesrechtsanwaltskammer Signaturkarte» werden im Auftrag der Rechtsanwaltskammer von der Bundesnotarkammer herausgegeben.

Die D-Trust GmbH, eine 100-prozentige Tochter der **Bundesdruckerei**, bietet im Zusammenhang mit dem Personalausweis eine Reihe von Vertrauensdiensten an, die bereits in der Vertrauensliste stehen. Sie ermöglicht eine digitale Signatur und bietet Hard- und Softwarekomponenten an, um elektronisch zu unterschreiben, zentral hierbei eine Chipkarte mit individuellem Personenzertifikat, Lesegeräte, SSL-Zertifikate, Gateway-Zertifikate, Zeitstempel, ein Signed Data Service und Signatursoftware mit sogenannten «Softtokens» der Sicherheitsklasse II zum Authentisieren, Signieren und Verschlüsseln insbesondere von E-Mails; oft handelt es sich bei «Softtokens» um einmalige Schlüssel aus einem Zufallsgenerator.

Deutsche Telekom (Telesec): Sie bietet die Registrierung und Zertifizierung von digitalen Identitäten, die Erzeugung und das Managements privater Schlüssel sowie eine Infrastruktur zur Validierung der Gültigkeit der ausgegebenen Zertifikate, die auf einer Signaturkarte verkörperlicht sind. Den ausgegebenen Zertifikaten ist jeweils ein qualifiziertes Signaturerzeugungsgerät (Qualified Signature or Seal Creation Device, QSCD) zugeordnet, bei welchem der dem öffentlichen Schlüssel im Zertifikat entsprechende private Schlüssel im Signaturerstellungsgerät selbst abgespeichert ist, konform zur jeweils anwendbaren EU-Gesetzgebung. Für die Definition dieses Signaturdienstes verweist die Vertrauensliste auf folgende URI: http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD/.

Die **Deutsche Rentenversicherung** Bund und Rheinland finden sich ebenfalls als Anbieter in der Vertrauensliste. Die Rentenversicherung bietet eine Wurzelzertifizierung, qualifizierte Zertifikate zur Identifikation von Mitarbeitern, Serverzertifikate und Zeitstempel; allerdings sind die neuesten Zertifikate von 2014 und die neuesten Certification Policies von 2011[11].

4.2. Private Unternehmen

Aus dem Bereich privater Unternehmen findet sich als erstes in der Vertrauensliste die **DATEV e.G.**, der zentrale Dienstleister für Steuerberater in Deutschland. Sie bietet den genossenschaftlich verbundenen Berufsträgern die Registrierung und Zertifizierung ihrer digitalen Identitäten, die Erzeugung und das Managements privater Schlüssel sowie eine Infrastruktur zur Validierung der Gültigkeit der ausgegebenen Zertifikate, die auf einer Signaturkarte verkörperlicht sind. Den ausgegebenen Zertifikaten ist jeweils ein Signaturerzeugungsgerät (Secure Signature Creation Device, SSCD) zugeordnet, bei welchem der dem öffentlichen Schlüssel im Zertifikat entsprechende private Schlüssel im Signaturerstellungsgerät selbst abgespeichert ist, konform zur jeweils anwendbaren EU-Gesetzgebung. Im Unterschied zum vorgenannten Gerät der Telesec also nicht «qualifiziert» und nur für personengebundene Signaturen, nicht für Siegel.

Folgt man dem Link aus der Vertrauensliste zum angebotenen Dienst, dann stellt sich heraus, dass der Vertrauensdienste-Markt für private Unternehmer zwischen den etablierten Angeboten staatlicher bzw. halbstaatlicher Stellen zum Start der Anwendung der eIDAS-Verordnung wenig Chancen auf Gewinn zu versprechen scheint. Denn dort steht mit Datum vom 11. November 2016, dass die DATEV die zertifizierte Signaturkarte für Berufsträger zum 31. März 2017 einstellt. Es werden keine neuen Signaturkarten mehr ausgegeben. Bestehende Karten können bis zum 31. März 2017 uneingeschränkt weitergenutzt werden. Für neue Karten wird verwiesen auf die Internetseiten der bereits oben erwähnten Bundesnetzagentur und D-Trust.

Auch die Firma **openlimit.com** unterstützt ihre Signatursoftware CCSign augenscheinlich nur noch bis zum Ende der Übergangszeit der eIDAS-Verordnung am 30. Juni 2017: https://www.openlimit.com/de/produkte/

[11] http://www.deutsche-rentenversicherung.de/Bund/de/Inhalt/5_Services/05_fachinformationen/Trustcenter/_Uebersicht_Certs.html und http://www.deutsche-rentenversicherung.de/Bund/de/Inhalt/5_Services/05_fachinformationen/Trustcenter/_Uebersicht_Policys.html.

cc-sign/aktuelles.html. Sie ist auch nicht in der Vertrauensliste enthalten. Die Signaturservices von **secrypt.de** (digiseal) sind laut deren Homepage zwar «eIDAS-ready», tauchten aber im Herbst 2016 in der Vertrauensliste noch nicht auf. Die von **intarsys.de** angebotenen umfassenden Vertrauensdienste basieren derzeit auf Smartcards und auf Lösungen der **Telesec**. Die Produkte dieser Firma tauchen ebenfalls nicht in der deutschen Vertrauensliste auf. Unter dem Stichwort «Fernsignatur nach EU VO eIDAS»[12] bietet sie lediglich die Vermittlung zu einer eIDAS-konformen Fernsignatur der swisscom an, die für das rechtssichere Signieren mit Smartphones geeignet ist.

Als Zertifikateanbieter ist auch die Firma **TC TrustCenter GmbH** aus Mainz in der Vertrauensliste aufgeführt. Allerdings steht unter der angegebenen Internet-Domain www.trustcenter.de Ende 2016 nur noch Folgendes: «Die Produkte und Services der TC TrustCenter GmbH stehen nicht mehr zur Verfügung.» und man möge sich an den telefonischen Support von Symantec TC TrustCenter wenden. In der Vertrauensliste taucht weiterhin die **Deutscher Sparkassen Verlag GmbH** auf, mit Zertifizierungs- und Identifizierungsdiensten, die aber praktisch nicht mehr von dieser Firma verantwortet werden, sondern für welche die Bundesnetzagentur als «taken over by» angezeigt wird. Folgt man den entsprechenden Links, stößt man auf die Seite https://www.nrca-ds.de/en/repository_e.htm der Bundesnetzagentur, die besagt, dass sie Zertifikate folgender Unternehmen weiter verwaltet, welche ihre eigenen Vertrauensdienste in den Jahren 2013 bis 2016 eingestellt haben: TC Trustcenter GmbH, Deutsche Post Com GmbH, Deutsche Post Signtrust und DMDA GmbH, Deutscher Sparkassen Verlag GmbH. – Goldgräberstimmung sieht anders aus.

Die Firma **Exceet** Secure Solutions GmbH als Tochter der schweizerischen Exceet AG Mitglied der Exceet Group SE, die als Winter AG die deutsche elektronische Gesundheitskarte für die Gematik GmbH realisiert hat, bietet als eIDAS-konformen Vertrauensdienst die Erzeugung, den Abruf und die Überprüfung qualifizierter Zeitstempel an[13], hält eine entsprechende Hochverfügbarkeitsinfrastruktur als Cloud-Service vor und ist in der Vertrauensliste enthalten.

Im Auftrag der **medisign GmbH** stellt die DGN Deutsches Gesundheitsnetz Service GmbH für Ärzte, Zahnärzte und Psychotherapeuten eine kartengebundene Infrastruktur mit persönlich identifizierenden Zertifikaten, Signaturmöglichkeiten und Zeitstempeln zur Verfügung, welche als Vertrauensdienste in der Vertrauensliste aufgeführt sind. Eine Produktübersicht findet sich unter der Adresse https://www.dgn.de/produkte/fuer-den-rechtsgueltigen-elektronischen-datenverkehr-signaturkarten-zubehoer/.

1&1 De-Mail GmbH, GMX EU-Mail, 1&1 EU-Mail und web.de EU-Mail sind als Töchter der United Internet AG zusammengefasst in der Vertrauensliste aufgeführt als Provider für einen qualifizierten und der eIDAS-Verordnung in der jeweiligen Fassung entsprechenden registrierten E-Mail-Zustellungsdienst gemäß der Definition unter der URI http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q/. Gesondert aufgeführt ist für einen solchen E-Mail-Zustellungsdienst noch die Firma **Mentana Claimsoft**, die als Tochtergesellschaft der Francotyp Postalia AG neben der Telekom AG und der United Internet AG für das DE-Mail-System akkreditiert wurde. Ihr Produkt ist unter der Adresse https://www.FP-DEMAIL.de beschrieben. Insbesondere müssen De-Mail-Anbieter für die eIDAS-Konformität Unterschiede von De-Mail zu eIDAS beachten, laut Norbert Pohlmann[14] insbesondere:

– Bei De-Mail versehe nach De-Mail-Gesetz (De-Mail-G) immer der akkreditierte Anbieter selbst die Nachrichten mit einer qualifizierten Signatur.[15] Es sei also nur eine Art der Fernsignatur zulässig.

[12] http://www.intarsys.de/produkte/fernsignatur.

[13] http://www.exceet-secure-solutions.de/it-security/elektronische-zeitstempel-nach-eidas/.

[14] http://norbert-pohlmann.com/app/uploads/2015/11/336-Der-Aufschwung-der-Vertrauensdienste-Verordnung-%C3%BCber-elektronische-Identifizierung-und-Vertrauensdienste-f%C3%BCr-elektronische-Transaktionen-im-Binnenmarkt-%E2%80%93-eIDAS-Prof-Norbert-Pohlmann.pdf, insb. Seite 53.

[15] § 5 Abs. 7 De-Mail-G.

- Überall, wo in der eIDAS-Verordnung qualifizierte Zeitstempel vorgesehen seien, benutze De-Mail Prüfsummen und qualifizierte Signaturen.
- De-Mail schreibe zwingend eine Transportverschlüsselung zwischen den Anbietern vor[16].
- De-Mail überlasse es den Anbietern, eine sichere Dokumentenablage anzubieten.[17]

De-Mail ist aktuell demnach nicht vollständig eIDAS-konform. Laut einem Zwischenbericht der Bundesregierung[18] soll De-Mail aber ab Geltung der Regelungen zu elektronischen Zustelldiensten den Anforderungen der eIDAS-Verordnung entsprechen und auf dieser Grundlage mit elektronischen Zustelldiensten anderer Mitgliedstaaten interoperabel werden.

5. Ausblick

Sowohl legislativ als auch in der direkten wirtschaftlichen Betätigung ist also derzeit viel Bewegung zu verzeichnen. Es ist interessant zu sehen, dass eine EU-Vorschrift, deren Entstehung unmittelbar von den interessierten Kreisen mitgeplant und -verantwortet wurde, bereits parallel zu ihrem Inkrafttreten messbare Auswirkungen zeitigen kann. Das könnte zum Teil daran liegen, dass die notwendigen technischen Standards und Umsetzungsvorschriften parallel dazu geschaffen und getestet werden konnten, d.h. die Vorschrift wurde nicht «am grünen Tisch» formuliert. Und zum Anderen daran, dass im zweiten Anlauf nicht mehr auf die Prozedur der Richtlinienumsetzung kraft vertraglicher Verpflichtung gesetzt wurde, sondern auf eine unmittelbar geltende Verordnung, zu deren Ausfüllung nicht nur die Mitgliedstaaten, sondern durchaus auch Unternehmen in eigener Verantwortung etwas beitragen können. Insofern ist zu vermuten, dass auch die nächsten Jahre noch viel Bewegung folgen wird. Offenbar erscheinen aber die prozeduralen Hürden noch immer so hoch, dass einige nichtstaatliche Mitbewerber bereits wieder ausgestiegen sind.

16 § 5 Abs. 3 Satz 1 De-Mail-G.
17 § 8 De-Mail-G.
18 BT-Drs. 18/4042, http://dip21.bundestag.de/dip21/btd/18/040/1804042.pdf.