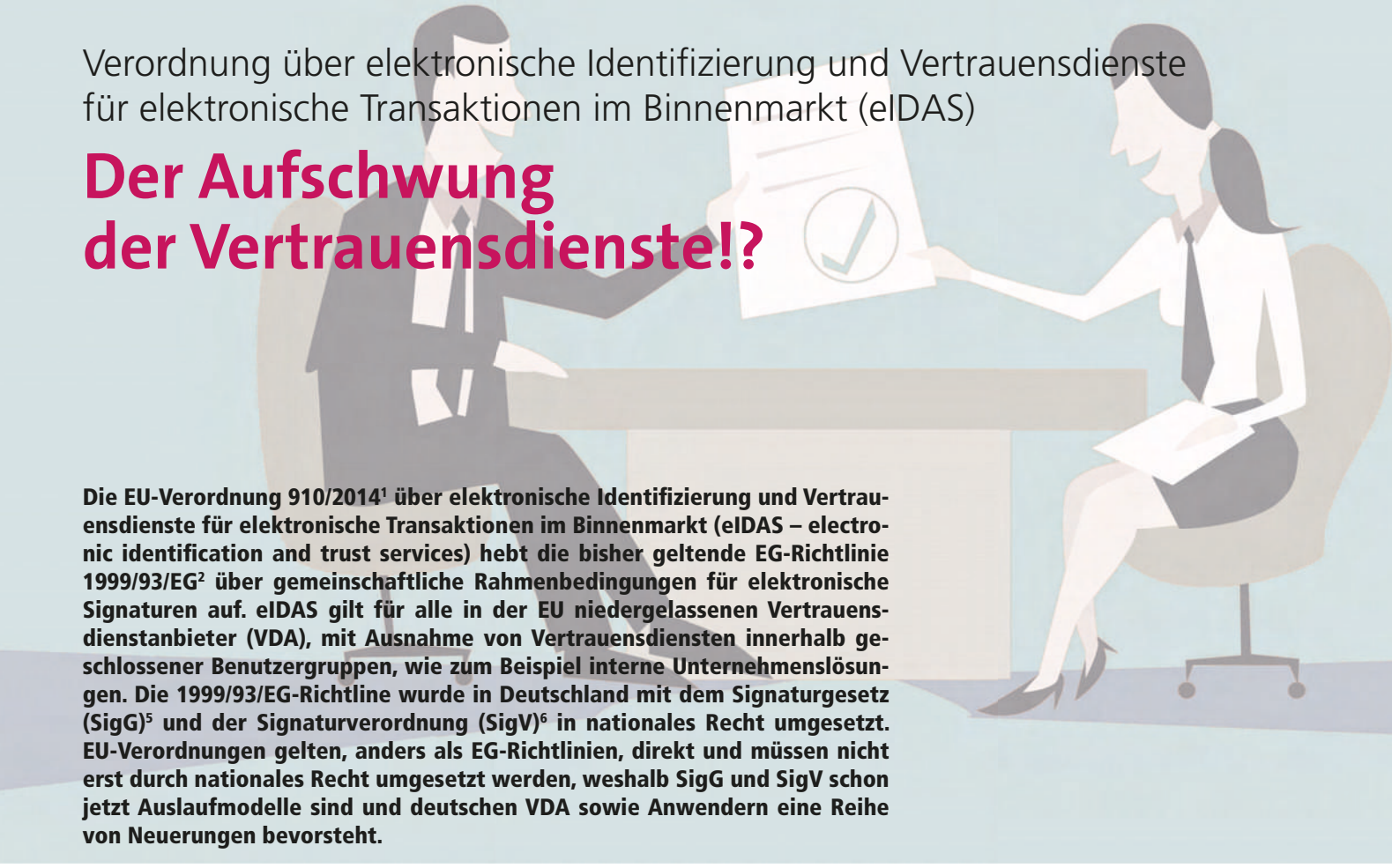
Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS)

Der Aufschwung der Vertrauensdienste!?



Die EU-Verordnung 910/2014[1] über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS – electronic identification and trust services) hebt die bisher geltende EG-Richtlinie 1999/93/EG[2] über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen auf. eIDAS gilt für alle in der EU niedergelassenen Vertrauensdienstanbieter (VDA), mit Ausnahme von Vertrauensdiensten innerhalb geschlossener Benutzergruppen, wie zum Beispiel interne Unternehmenslösungen. Die 1999/93/EG-Richtline wurde in Deutschland mit dem Signaturgesetz (SigG)[5] und der Signaturverordnung (SigV)[6] in nationales Recht umgesetzt. EU-Verordnungen gelten, anders als EG-Richtlinien, direkt und müssen nicht erst durch nationales Recht umgesetzt werden, weshalb SigG und SigV schon jetzt Auslaufmodelle sind und deutschen VDA sowie Anwendern eine Reihe von Neuerungen bevorsteht.

Die Europäische Kommission verfolgt bei der eIDAS-Verordnung einen offenen und technologieneutralen Ansatz. Das Hauptaugenmerk liegt auf der Gleichstellung, Interoperabilität und gegenseitigen Anerkennung der Vertrauensdienste der Mitgliedsstaaten. Bürger, Unternehmen und öffentliche Verwaltung sollten dazu ermuntert werden, die Vorteile des integrierten digitalen Binnenmarktes voll auszuschöpfen. Ganz oben auf der Prioritätsliste steht deshalb die Schaffung von Vertrauen in die vom Vertrauensdienstanbieter (VDA) erbrachten Dienste. Untrennbar mit Vertrauen verbunden ist ein Anspruch auf Rechtssicherheit, ganz gleich aus welchem Mitgliedsstaat der Dienst erbracht wird. Ein elektronisches Dokument soll in der EU den gleichen Stellenwert erhalten wie ein analoges. Durch diese Rechtssicherheit wird es in Zukunft möglich sein, Unternehmen und öffentliche Verwaltungen durch den Wegfall von analogen Dokumenten deutlich effizienter zu gestalten und ganz nebenbei für Unionsbürger Hemmnisse bei der Ausübung ihrer Bürgerrechte aus dem Weg zu räumen. Was wird sich aus deutscher Sicht ändern?

Weniger Signaturstufen

In Deutschland werden Signaturen nach Signaturgesetz (SigG) aktuell in vier Arten unterteilt:

1. **Die elektronische Signatur (ES)** (§ 2 Nr. 1 SigG) als Beschreibung des rein technischen Verfahrens
2. **Die fortgeschrittene elektronische Signatur (FES)** (§ 2 Nr. 2 SigG), die vom Signaturschlüsselinhaber selbst erzeugt wurde, eindeutig dessen Identifizierung ermöglicht und nachträgliche Datenveränderungen ausschließt
3. **Die qualifizierte elektronische Signatur (QES)** (§ 2 Nr. 3 SigG), die neben den Eigenschaften der FES zum Zeitpunkt der Erzeugung auf einem gültigen qualifizierten Zertifikat beruht und mit einer sicheren Signaturerstellungseinheit (SSEE) erzeugt wurde
4. **Die qualifizierte elektronische Signatur mit Anbieterakkreditierung (akkreditierte Signatur)** (§ 15 Abs. 1 Nr. 4 SigG), die neben den Eigenschaften der QES eine im Abstand von drei Jahren wiederkehrende Zertifizierung eines Zertifizierungsdienstanbieters (ZDA) über die Bundesnetzagentur voraussetzt (§ 15 SigG, § 11 SigV)

Mit eIDAS geht eine Vereinfachung des Systems einher. eIDAS sieht nur noch qualifizierte und nicht-qualifizierte VDA vor. Dies heißt jedoch nicht, dass sich ein qualifizierter VDA keiner Überprüfung mehr unterziehen muss. Aktuell können sich qualifizierte ZDA freiwillig alle drei Jahre akkreditieren lassen (§ 11, Abs. 2, SigV). In Zukunft muss sich jeder qualifizierte VDA alle zwei Jahre einer Überprüfung unterziehen, welche auf europäischer Ebene nicht

eine Akkreditierung, sondern Konformitätsbewertung ist (Artikel 19, eIDAS). Der Konformitätsbewertungsbericht wird dabei jedoch von einer akkreditierten Konformitätsbewertungsstelle ausgestellt (Art. 3, Nr. 18, eIDAS). Ein qualifizierter VDA muss bis spätestens ab 1. Juli 2016 einen Konformitätsbewertungsbericht vorlegen, sofern er seinen Status nicht verlieren möchte (Art. 51, Abs. 3, eIDAS).

Da die Anforderungen beider Überprüfungen nahezu gleich sind und das Prüfungsintervall zudem verkürzt wurde, ist somit kein Sicherheitsverlust zu erwarten. Für den Kunden wurde zudem die Auswahl eines VDA vereinfacht: Die unnötig komplizierte Unterscheidung zwischen fortgeschrittenen, qualifizierten und sowohl qualifizierten als auch akkreditierten VDA entfällt.[4]

Die QES nach SigG bleibt auf jeden Fall noch bis zum 1. Juli 2016 erhalten. Inwieweit in Zukunft die QES nach SigG sowie die Anbieterakkreditierung nach SigG als nationale Insellösungen noch Fortbestand haben werden, ist aktuell noch offen.

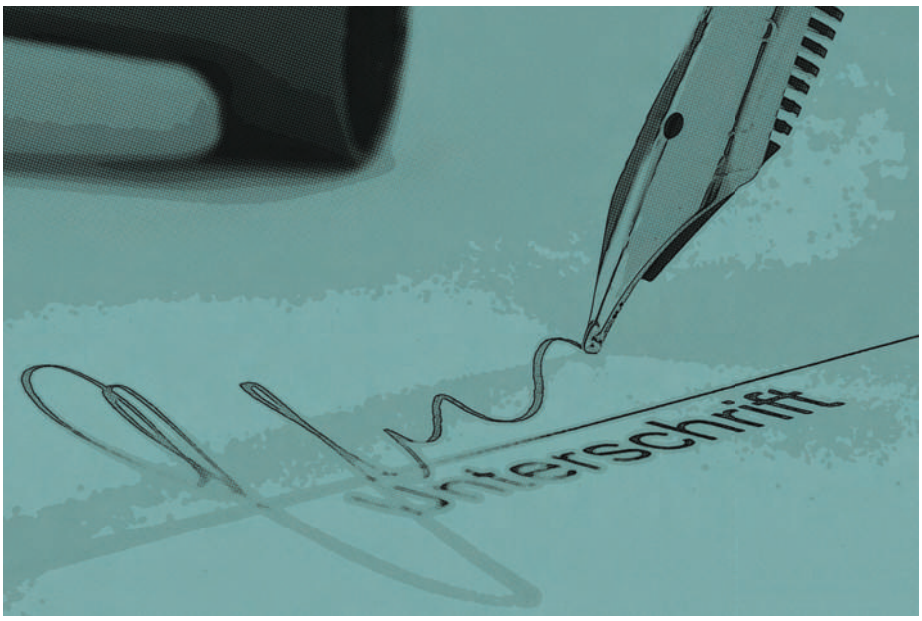
EU-Vertrauenssiegel (Art. 23)

VDA können in Zukunft freiwillig mit einem EU-Vertrauenssiegel darauf aufmerksam machen, dass sie ein auf europäischer Ebene qualifizierter VDA sind. Das EU-Vertrauenssiegel verfolgt dabei einen ähnlichen Ansatz wie zum Beispiel das „IT Security made in Germany"-Qualitätssiegel des TeleTrusT – Bundesverband IT-Sicherheit e.V.[7], mit dem ein Anbieter den Kunden auf einen Blick über den praktizierten Qualitätsstandard informieren kann. Dies ist insbesondere für ausländische Anbieter und Startups wichtig, da sie dem Kunden in der Regel weniger geläufig sind, was instinktiv mit einer niedrigen Vertrauenswürdigkeit assoziiert wird. Das Siegel schafft die Möglichkeit der Vertrauensbildung, was gerade im E-Commerce-Umfeld eine essenzielle Voraussetzung ist. Alle VDA mit EU-Vertrauenssiegel werden zudem in einer zentralen Liste aufgeführt, was die Findung eines VDA erleichtert.

Suspendierung von qualifizierten Zertifikaten (Art. 28)

Bislang konnten Kunden nach SigG nur neue Zertifikate ausstellen oder diese endgültig sperren lassen. Nicht berücksichtigt wurde der Anwendungsfall, dass ein Kunde sein Zertifikat (zum Beispiel in Form einer Smartcard) kurzfristig verlegt, dann aber doch wiederfindet, was nach alter Regel bedeuten würde, dass die alte Smartcard wertlos wäre.

Für genau diesen Anwendungsfall ist in eIDAS die Möglichkeit der zeitlichen Suspendierung von Zertifikaten geschaffen worden (Artikel 28, Abs. 5, eIDAS; Erwägungsgrund 53). Das Zertifikat verliert dabei nur während der Aussetzung die Gültigkeit, kann aber nach der Reaktivierung wieder verwendet werden. Die Dauer der Aussetzung muss dabei klar in der Zertifikatsdatenbank angegeben werden.



Elektronische Siegel (Art. 35 bis 40)

Das SigG sieht nur elektronische Signaturen für natürliche Personen vor (§ 2 Nr. 2a, SigG). Diese Beschränkung ist für Organisationen jedoch eher hinderlich, wie das Beispiel einer Angebots deutlich macht: Ein Angebot, welches mit einer FES, beziehungsweise QES signiert wurde, beinhaltet implizit die Identität des Verfassers des Angebots. Der Mitarbeiter kann das Unternehmen jedoch wechseln, wodurch das Zertifikat gesperrt wird. Dem Empfänger ist ab diesem Zeitpunkt nicht mehr klar, ob das Angebot gültig ist. Natürlich wäre es möglich, das Angebot mit einem Pseudonym zu signieren (§ 5, Abs. 3, SigG), jedoch wirkt ein Pseudonym im Geschäftsverkehr nicht sonderlich vertrauenserweckend.

Elektronische Siegel stellen jetzt mit eIDAS das Pendant zu elektronischen Signaturen dar, mit dem Unterschied, dass elektronische Siegel auch von Organisationen verwendet werden können. Elektronische Siegel beinhalten ein großes Potenzial zur Bekämpfung von Cybercrime. Jedes Jahr gibt es tausende von Fällen, in denen Verbraucher auf gefälschte Rechnungen und Mahnungen hereinfallen. Würden alle Firmen in der EU ausnahmslos ihren Geschäftsverkehr mit elektronischen Siegeln versehen, so wäre es für Verbraucher deutlich einfacher, Phishing-E-Mails als solche zu entlarven.

Elektronische Fernsignaturen

Qualifizierte Signaturen nach SigG setzen voraus, dass der Kunde selbst eine sichere Signaturerstellungseinheit (SSEE) besitzen muss (§ 5, Abs. 6, SigG). In Zeiten, in denen immer mehr Dienste über die Cloud, Tablets, Smartphones und andere weit verbreitete Gadgets benutzt werden, wirkt eine lokale Signaturerstellungseinheit jedoch eher bremsend auf eine weitere Verbreitung von QES.

Genau hier setzt in eIDAS die Fernsignatur an. Die Idee ist, dass die SSEE beim qualifizierten VDA bleibt und nur der eigentliche Auslöser der Signatur mit technischen Mitteln verlängert wird. Der VDA hat dafür zu sorgen, dass unter anderem durch abgesicherte elektronische Kommunikationskanäle

eine vertrauenswürdige Umgebung zur Erstellung elektronischer Signaturen hergestellt wird, und muss gewährleisten, dass die Umgebung unter alleiniger Kontrolle des Unterzeichners ist (Erwägungsgrund 52, eIDAS).

In Österreich, Finnland und Estland sind mit der „Handy-Signatur" bereits seit längerem ähnliche Lösungen im Einsatz.[9] Zum Schutz der Kunden dürfen Fernsignaturen nur von einem qualifizierten VDA angeboten werden (Anhang II, Abs. 3, eIDAS).

Haftung und Beweislast (Art. 11, 13)

Bei einem qualifizierten VDA wird von Vorsatz oder Fahrlässigkeit ausgegangen, es sei denn, er kann nachweisen, dass der Schaden auf andere Weise entstanden ist. Im Fall von Fernsignaturen muss also der VDA nachweisen, dass er sichere Systeme zur Verfügung gestellt hat. Bei nicht-qualifizierten VDA liegt die Nachweispflicht hingegen beim Kunden.

In jedem Fall haftet der VDA, wenn er die in der eIDAS-Verordnung genannten Pflichten nicht eingehalten hat, beispielsweise wenn er Dienste anbietet, die nicht dem neuesten Stand der Technik entsprechen (Art. 19, Abs. 1, eIDAS). Der VDA hat jedoch im Vorfeld die Möglichkeit, seine Haftung zu beschränken, indem er die Verwendungszwecke der vom ihm erbrachten Dienste beschränkt.

Elektronische Einschreiben (Art. 43 bis 44)

Elektronische Einschreiben sind ein weiterer Weg, um den analogen Schriftverkehr überflüssig zu machen. Die Anforderungen an qualifizierte Dienste für die Zustellung elektronischer Einschreiben nach eIDAS sind:

- Identifizierung des Absenders mit hohem Maß an Vertrauenswürdigkeit
- Identifizierung des Empfängers vor Zustellung der Daten
- Absenden und Empfang ist durch fortgeschrittene elektronische Signatur oder ein fortgeschrittenes elektronisches Siegel eines qualifizierten VDA vor Veränderung geschützt
- Jede Veränderung von Daten wird deutlich angezeigt
- Zeit und Datum von Versand, Empfang oder Änderung der Daten wird durch qualifizierte elektronische Zeitstempel angezeigt

Auf nationaler Ebene existiert in Deutschland mit der De-Mail bereits ein ähnlicher Dienst. Es existieren jedoch einige kleine Unterschiede:

1. **Bei De-Mail versieht nach De-Mail-Gesetz (De-Mail-G) [10] immer der akkreditierte Anbieter selbst die Nachrichten mit einer qualifizierten Signatur (§ 5, Abs. 7, De-Mail-G). Es ist also nur eine Art Fernsignatur zulässig.**
2. **Überall, wo in eIDAS qualifizierte Zeitstempel vorgesehen sind, benutzt De-Mail Prüfsummen und qualifizierte Signaturen**
3. **De-Mail schreibt zwingend eine Transportverschlüsselung zwischen den Anbietern vor (§ 5, Abs. 3, Satz 1, De-Mail-G)**
4. **De-Mail überlässt es den Anbietern, eine sichere Dokumentenablage anzubieten (§ 8, De-Mail-G)**

De-Mail ist aktuell also nicht vollständig eIDAS-konform. Laut einem Zwischenbericht der Bundesregierung 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.[16]

Sicherheitsanforderungen an Vertrauensdienstanbieter (Art. 19)

Alle qualifizierten und nicht-qualifizierten VDA müssen unter Berücksichtigung des jeweils neuesten Stands der Technik gewährleisten, dass das Sicherheitsniveau der Höhe des Risikos angemessen ist. Besteht ein Sicherheitsvorfall, so muss der VDA innerhalb von 24 Stunden die zuständige nationale Stelle beziehungsweise Datenschutzbehörde sowie die betroffenen natürlichen oder juristischen Personen informieren. Betreffen Sicherheitsverletzungen oder Integritätsverlust mehrere Mitgliedsstaaten, so müssen die Aufsichtsstellen der betroffenen Mitgliedsstaaten und die ENISA davon in Kenntnis gesetzt werden. Besonders heikel für VDA ist jedoch, dass die Aufsichtsstelle entscheiden kann, ob bei einem Sicherheitsvorfall oder Integritätsverlust die Öffentlichkeit informiert wird, falls dies im öffentlichen Interesse ist. Für jeden VDA stellt schließlich ein Vertrauensverlust den höchsten denkbaren Wertverlust dar.

Kritik an der eIDAS-Verordnung

Die vielleicht größten Kritikpunkte an eIDAS sind die mangelnden technischen Anhaltspunkte für die Umsetzung, gerade im Hinblick auf die Interoperabilität,[8] und der daraus resultierende sportliche Zeitplan.[13]

Gerade in der Übergangsphase gibt es zudem ein Problem mit dem Sprachgebrauch: Qualifizierte Zertifikate nach SigG und eIDAS beschreiben zwei unterschiedliche Vertrauensstufen; ein qualifiziertes Zertifikat für fortgeschrittene Signaturen gibt es nach SigG gar nicht. Hier muss noch viel Aufklärungsarbeit für den Kunden betrieben werden.

Aus juristischer Sicht gibt es zwei Probleme: Zum Ersten existiert keine übergeordnete Stelle für Interpretation und Schlichtung.[12] Zum Zweiten verweist eIDAS zwar auf EG-Datenschutzrichtlinie 95/46/EG[3], jedoch fehlt im Verordnungstext eine genaue Definition, was eigentlich Identifizierungsdaten sind,[11] da diese Definition in jedem EU-Mitgliedsstaat unterschiedlich ausgelegt wird.[8]

Stärken, Schwächen, Möglichkeiten, Bedrohungen der eIDAS-Verordnung

Was eIDAS aus geschäftlicher Sicht für einen deutschen VDA bedeutet, soll im Folgenden an der SWOT-Analyse gezeigt werden.

Stärken (intern):

- Bereits hoher gelebter Sicherheitsstandard in Deutschland
- Gute Qualitätsreputation der deutschen Anbieter im Ausland
- Hohes Datenschutzniveau in Deutschland vorhanden
- Vergleichsweise großer Kundenstamm in Deutschland

Schwächen (intern):
- Hohe Fixkosten (Personal, Energie)
- Hohe bürokratische Auflagen (Datenschutz, Steuersystem)
- Technologischer Rückstand im Bereich Fernsignatur (Handy etc.)

Möglichkeiten (extern):
- Mehr Produkte und Dienstleistungen (Siegel etc.)
- Zugang zu ausländischen Märkten
- Gesteigerte Nachfrage durch Rechtssicherheit
- Firmenzusammenschlüsse und Akquisitionen werden vereinfacht (kann auch Risiko sein)
- Trusted Lists und EU-Gütesiegel als Marketinginstrument

Risiken (extern):
- Konkurrenz durch ausländische Anbieter
- Günstigere und schlechtere Verfahren werden als gleichwertig anerkannt

Nachdem die Konkurrenzsituation für VDA in Deutschland durch das Aus von TC Trustcenter und SignTrust im letzten Jahr abgenommen hat, wird sie also in Zukunft durch europäische Konkurrenten wieder ansteigen. Durch das Aus können aber gleichzeitig die bestehenden großen Anbieter in Deutschland, insbesondere DTrust und Telesec gestärkt der neuen Situation entgegentreten.[15] Vertrauensdienste aus Deutschland und/oder aus Europa sind insbesondere nach der NSA-Affäre eine absolute Notwendigkeit.

Vorbereitungs- und Einflussmaßnahmen

Die meisten großen deutschen Zertifizierungsdienstanbieter sowie Anbieter von qualifizierten elektronischen Signaturen verfügen bereits jetzt schon über die notwendigen Voraussetzungen, sofern sie nach ETSI-Standards zertifiziert sind.[14] Die ETSI-Standards bilden ab Mitte 2016 die Grundlage für eIDAS-konformen Betrieb.

Alle Unternehmen, die Validierungsdienste, elektronische Einschreibdienste oder Archive anbieten, sollten frühestmöglich prüfen, ob sie von eIDAS betroffen sind. Falls sie es sind, müssen sie klären, ob sie den ETSI-Anforderungen entsprechen, da Abweichungen bis zum Juli 2016 behoben sein müssen.

Quellen:

[1] Amtsblatt der Europäischen Union, VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&from=EN Stand: 05.01.2015

[2] Amtsblatt der Europäischen Gemeinschaften, RICHTLINIE 1999/93/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31999L0093&from=EN Stand: 05.01.2015

[3] Amtsblatt der Europäischen Gemeinschaften, Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:31995L0046&from=en Stand: 21.01.2015

[4] Christian Segebarth, Perspektiven der eIDAS Verordnung – Die Sicht eines qualifizierten Trust Service Providers, DuD, Datenschutz und Datensicherheit 10/2014, Springer Gabler

[5] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) http://www.gesetze-im-internet.de/sigg_2001/BJNR087610001.html Stand: 22.01.2015

[6] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) http://www.gesetze-im-internet.de/sigv_2001/ Stand: 22.01.2015

[7] TeleTrusT Bundesverband IT-Sicherheit e.V., IT Security made in Germany – Quality Seal https://www.teletrust.de/itsmig/ Stand: 27.01.2015

[8] BCS, The Chartered Institute for IT, eIDAS Regulation and Implementing the Act https://www.youtube.com/watch?v=V5vzZipQc2I Stand: 28.01.2015

[9] A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH; So funktioniert die Handy-Signatur: https://www.handy-signatur.at/ Stand: 29.01.2015

Die neue TeleTrusT-Arbeitsgruppe „Forum elektronische Vertrauensdienste" ist Teil der gemeinsamen Diskussionsplattform deutscher Verbände und Zusammenschlüsse zur eIDAS-Verordnung.[17] Die Arbeitsgruppe beteiligt sich an der Ausarbeitung der „Implementing Acts" zur Verbindung von Gesetzgebung und Standardisierung und der Anpassung der deutschen Gesetzgebung. Interessengruppen sind in den nächsten zwei Jahren dazu eingeladen, sich frühzeitig aktiv in die Gestaltung einzubringen.

Das Forum „elektronische Vertrauensdienste" dient der:

- Bildung gemeinsamer Standpunkte zur Unterstützung der deutschen Interessen
- Mitarbeit bei der nationalen Gesetzgebung und Information nationaler Gremien
- fachlichen Unterstützung von Ausschussvertretern bei regulären EU-Veranstaltungen und beteiligten Standardisierungsgremien (z.B. DIN, CEN, ETSI)

Fazit

In Deutschland werden das Signaturgesetz und die Signaturverordnung zum 1. Juli 2016 zusammen mit der Richtlinie 1999/93/EG aufgehoben; allenfalls diejenigen Bestandteile können beibehalten werden, die die EU-Verordnung nicht regelt. Die deutsche Wirtschaft begrüßt eIDAS als massive legislative und technische Vereinfachung und sieht darin einen Wachstumsmotor.[13] Öffentliche Verwaltungen werden es bis Mitte 2018 den EU-Bürgern ermöglichen müssen, digi tale Dokumente anzunehmen. Anwender können durch die neuen Möglichkeiten wie Fernsignaturen eine Reihe von neuen Innovationen erwarten, die das Leben deutlich komfortabler machen werden. Die Herausforderung wird sein, die bestehenden Systeme anhand der ausstehenden Durchführungsverordnungen zu transformieren. Jetzt muss sich zeigen, ob der straffe Zeitplan eingehalten werden kann. Selbst wenn die eine oder andere Deadline nicht eingehalten werden sollte, überwiegen die mit eIDAS verbundenen Vorteile jedoch auf ganzer Linie. ■

[10] *De-Mail-Gesetz (De-Mail-G) http://www.gesetze-im-internet.de/de-mail-g/ Stand: 30.01.2015*

[11] *Die Zukunft der Vertrauensdienste: CAST-Workshop zu eIDAS http://www.heise.de/newsticker/meldung/Die-Zukunft-der-Vertrauensdienste-CAST-WorkshopzueIDAS-2249714.html Stand: 03.02.2015*

[12] *Clemens Wanko, TÜV Informationstechnik, eIDAS – Chancen und Risiken https://www.teletrust.de/uploads/media/1_TeleTrusT-VOIInfotag_eSignatur_Wanko.pdf Stand: 03.02.2015*

[13] *BITKOM ECM Forum 2014, Auswirkungen von eIDAS auf den deutschen ECM-Markt https://www.youtube.com/watch?v=5DkaX_MjZp8 Stand: 05.02.2015*

[14] *Presseinformationen, TÜV NORD GROUP, Neue EU-Verordnung eIDAS: Vertrauensdienste sollten sich rechtzeitig auf Neuregelung vorbereiten http://www.tuev-nord.de/de/pressemitteilungen-575-eidas-vertrauensdienste-sollten-neue-eu-verordnung-beachten-112453.htm Stand: 05.02.2015*

[15] *Heise.de, Aus für Signtrust führt zur Neuordnung bei Trustcentern http://www.heise.de/newsticker/meldung/Aus-fuer-Signtrust-fuehrt-zur-Neuordnung-bei-Trustcentern-2304983.html Stand: 06.02.2015*

[16] *Deutscher Bundestag, Drucksache 18/4042, Zwischenbericht der Bundesregierung nach Artikel 4 des Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften http://dip21.bundestag.de/dip21/btd/18/040/1804042.pdf Stand: 23.02.2015*

[17] *TeleTrusT – Bundesverband IT-Sicherheit e.V., Neue TeleTrusT-Arbeitsgruppe „Forum elektronische Vertrauensdienste" ist Teil der gemeinsamen Diskussionsplattform deutscher Verbände und Zusammenschlüsse zur eIDAS-Verordnung https://www.teletrust.de/startseite/pressemeldung/?tx_ttnews%5Btt_news%5D=785&cHash=1c0eef6eaefa8df051bafc3fb0d06d1c Stand: 25.02.2015*

GERO NIESSEN (B.SC.)
Wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen

NORBERT POHLMANN
Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen. Außerdem ist er Studienbeauftragter für den Master Internet-Sicherheit.