TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der IT-Sicherheitsverband.

Berlin, 01.11.2016

Stellungnahme

zum "Referentenentwurf des 'eIDAS-Durchführungsgesetzes'" des Bundesministeriums für Wirtschaft und Energie

(TeleTrusT-Arbeitsgruppe "Forum elektronische Vertrauensdienste AK A")

TeleTrusT - Bundesverband IT-Sicherheit e.V.
Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.), "TeleTrusT Engineer for System Security" (T.E.S.S.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Qualitätszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

1 Einleitung

Das Bundesministerium für Wirtschaft und Energie (BMWi) hat am 18.10.2016 einen *Entwurf eines Gesetzes zur Durchführung der 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* an Zentral- und Gesamtverbände sowie Fachkreise versendet und eine Stellungnahme bis zum 01.11.2016 ermöglicht.

Hintergrundinformationen des BMWi:
Seit dem 01.07.2016 gilt die Verordnung (EU) Nr. 910/2014 (sog. eIDAS-Verordnung), mit der EU-weit einheitliche Anforderungen an elektronische Vertrauensdienste (elektronische Signaturen, Siegel, Zeitstempel, Zustelldienste und Webseitenauthentifizierung) gestellt werden. Ziel ist es, das Vertrauen der EU-Bürger in die grenzüberschreitende Anwendung der elektronischen Dienste und damit in den Digitalen Binnenmarkt zu stärken. Die Verordnung gilt in den Mitgliedstaaten unmittelbar. Mit dem vorliegenden Entwurf für ein eIDAS-Durchführungsgesetz soll sie effektiv durchgeführt und die Akzeptanz von Vertrauensdiensten in Wirtschaft und Verwaltung gesteigert werden. Als Artikelgesetz enthält das eIDAS-Durchführungsgesetz, das Vertrauensdienstegesetz sowie Folgeänderungen.

(1) Vertrauensdienstegesetz (VDG)
Das Vertrauensdienstegesetz soll insbesondere Zuständigkeiten und Befugnisse der beteiligten Behörden regeln und die Verordnung in einigen Punkten präzisieren. Dabei orientiert sich das VDG weitgehend an den vergleichbaren Vorschriften des bislang geltenden Signaturgesetzes (SigG). Mit dem VDG wird zudem das geltende Signaturgesetz aufgehoben. Parallel wird das BMWi eine Rechtsverordnung erarbeiten, die weitere Einzelheiten enthalten wird (Vertrauensdiensteverordnung, VDV)

(2) Folgeänderungen
Darüber hinaus enthält der Entwurf in den weiteren Artikeln notwendige Anpassungen an die eIDAS-Verordnung bzw. Neuregelungen von Verweisen, die mit dem Wegfall des Signaturgesetzes erforderlich werden

2 Vorbemerkungen

Zunächst begrüßen wir, dass das BMWi mit dem Referentenentwurf für ein Vertrauensdienstegesetz die Anwendungsmöglichkeiten für elektronische Vertrauensdienste erweitern und damit den Weg für eine effektive Durchführung der europäischen eIDAS-Verordnung freimachen möchte. So kann noch in dieser Legislaturperiode Klarheit über das Verhältnis der eIDAS-Verordnung zum (verbleibenden) nationalen Signaturrecht geschaffen werden.

Die eIDAS-Verordnung schafft nicht nur einen gemeinsamen digitalen europäischen Vertrauensraum, sondern ermöglicht auch die Einführung von innovativen neuen Technologien. Dafür benötigen die Unternehmen jene Rechtssicherheit, die das Vertrauensdienstegesetz schaffen soll. Andere europäische Länder haben bereits entsprechende nationale Umsetzungsgesetze verabschiedet. Dadurch können dort ansässige Unternehmen bereits jetzt neue Technologien entwickeln und anbieten. Aufgrund der mit der eIDAS-Verordnung einhergehenden grenzüberschreitenden und unmittelbaren Wirkung können eben diese Unternehmen ihre Dienstleistungen auch im deutschen Markt anbieten – ohne bislang auf deutsche Konkurrenz zu treffen. Vor diesem Hintergrund wäre mehr Agilität seitens der Bundesregierung wünschenswert gewesen.

Wir haben großes Interesse an einem zügigen Verfahrensablauf, und begrüßen die Möglichkeit, durch die Stellungnahme an einer fachlich angemessenen Umsetzung mitwirken zu können.

3 Allgemeine Anmerkungen zum Entwurf

Mit der eIDAS-Verordnung wurde nicht nur die EU-Signaturrichtlinie überarbeitet, sondern der thematische Regelungsbereich über das Signaturrecht hinaus erweitert und das Regulierungsinstrument geändert. Das hat Folgen für das nationale Signaturrecht in Deutschland. Der grundsätzliche Ansatz, Dienste aus der eIDAS-Verordnung aus dem SigG ableiten zu lassen und durch das VDG abzulösen ist aus unserer Sicht verständlich. In Ausnahmefällen wird das jedoch nicht ausreichen. Wir möchten explizit auf elektronische Einschreib- und Zustelldienste hinweisen, die eher im De-Mail Gesetz referenziert sind.

Der vorliegende Entwurf deckt zudem nicht alle neuen Dienste ab, die die eIDAS-Verordnung ermöglicht. Dies wird bereits in der Formulierung "Überleitung der Regelungen des Signaturgesetzes sowie der zugehörigen Verordnung zum Rechtsrahmen der Verordnung" in § 1, Absatz 1, Satz 2 des Entwurfs deutlich. Damit werden Vertrauensdienste vor allem auf Signaturen reduziert. Vielmehr sollten aber auch die Siegel, die Bewahrungsdienste und Kommunikationsdienste wie etwa elektronische Einschreiben und weitere Geschäftsmodelle wie Validierungsdienste deutlich stärker berücksichtigt und damit Rechtssicherheit hergestellt werden.

Weiterhin weist der Entwurf zahlreiche Regelungen auf, die entweder bereits in der eIDAS-Verordnung eindeutig beschrieben sind oder – im Gegenteil – nicht dem Geist der eIDAS-Verordnung entsprechen bzw. nicht eIDAS-konform gestaltet sind. Einige Regelungen gehen auch deutlich über die eIDAS-Verordnung hinaus. Es würden sich dadurch eben jene Wettbewerbsnachteile manifestieren, unter denen deutsche Anbieter bereits heute leiden.

In den im Entwurf enthaltenen Artikelgesetzen fehlen zudem wichtige betroffene Gesetze, etwa das Sozialgesetzbuch.

Im Folgenden möchten wir auf grundsätzlich zu beachtende Ziele eingehen, die Einfluss auf die Stellungnahme zu einzelnen Artikeln haben:

3.1 Rationalisierungspotentiale für Wirtschaft und Kommunen heben

Das im Gesetzentwurf beschriebene Rationalisierungspotential, das Umsetzungsaufwänden der Wirtschaft entgegengestellt wird, kann nur gehoben werden, wenn sich das Vertrauensdienstegesetz nicht zu eng am abzulösenden Signaturgesetz orientiert. Richtig ist zwar, das Signaturrecht eIDAS-konform zu aktualisieren. Notwendig ist es aber auch, neue Dienste nach eIDAS in Deutschland rechtssicher zu regeln. Hier bleibt der Gesetzentwurf hinter den Erwartungen zurück. Dies gilt auch für weitere Rationalisierungspotentiale bei Ländern und Kommunen. Nur wenn neue Dienste, wie etwa Siegel und Zeitstempel konkret gefasst werden, wären etwa die Kommunen in der Lage, ihre Erfüllungsaufwände exakt zu quantifizieren. Ein Beispiel wäre die Einführung eines elektronischen Siegels im Verwaltungsverfahrensgesetz

3.2 Wettbewerbsnachteile für deutsche Anbieter vermeiden

Auch das Aufziehen des Fokus weg von der engen Sichtweise auf Zertifizierungsdienste, Signaturen und Zeitstempel, hin zu Vertrauensdiensten mit Signaturen und Zeitstempeln, nun aber auch Siegeln, Einschreib-Zustelldiensten, Bewahrungsdiensten und Webseiten-Authentifizierung führt dazu, dass Vorgaben, die sich an die alten signaturgesetzkonformen Zertifizierungsdiensteanbieter richteten, nur sehr eingeschränkt auf Ver-

trauensdiensteanbieter übertragen lassen. An dieser Trennschärfe mangelt es dem vorliegenden VDG-Entwurf. Bestimmte Vorgaben und Ideen, die aus dem Signaturgesetz übernommen wurden, zielen oftmals ins Leere oder erzeugen Widersprüche.

Wenn also bestimmte, klassisch deutsche Signaturgesetz-Regeln für alle Vertrauensdienste vorgeschlagen werden, muss zum einen klargestellt werden, dass diese Regeln tatsächlich angewendet werden können und zum anderen, dass nicht zusätzliche, nationale Anforderungen gestellt werden, die in der eIDAS-Verordnung und anderen Mitgliedstaaten nicht bestehen. Neben der Europarechtswidrigkeit aufgrund des Verstoßes gegen das Umsetzungsverbot aus Art. 288 AEUV würden so auch ungewollte Wettbewerbsnachteile für deutsche Anbieter entstehen.

3.3 eIDAS-Konformität sicherstellen

War der deutsche Gesetzgeber beim Signaturgesetz von 1997 noch frei davon, europäisches Recht beachten zu müssen, hatte er sich bei der Schaffung des Signaturgesetzes von 2001 an den Harmonisierungsauftrag aus der EU Signaturrichtlinie von 1999 zu halten. Es gab also einen gewissen Spielraum bei der Umsetzung der EU-Richtlinien. Bei der eIDAS-Verordnung von 2014 gibt es diesen Spielraum nicht mehr. Für EU-Verordnungen gilt ein Umsetzungsverbot der Verordnung. In einem Durchführungsgesetz können also nur Inhalte geregelt werden, zu denen es in der Verordnung einen klaren Gesetzgebungsauftrag an die Mitgliedstaaten der EU gibt und die nicht mit den Inhalten der Verordnung konkurrieren und diesen gar entgegenstehen. Einige Regelungen des Gesetzentwurfes sind nicht mit eIDAS-Verordnung in Einklang zu bringen, einige widersprechen ihrer Zielsetzung.

3.4 Normierten Stand der Technik berücksichtigen

Im Gesetzentwurf sind Regelungen zu technischen Spezifikationen enthalten, die bereits durch europäische Normung definiert sind. Es wird empfohlen, den Stand der Technik zu berücksichtigen.

3.5 Rolle des Algorithmenkatalogs der BNetzA

Weder die eIDAS-Verordnung selbst noch der vorgelegte Entwurf des VDG regelt eindeutig den Umgang mit den kryptographischen Algorithmen und Schlüssellängen im Bereich der qualifizierten Signaturen / Siegel / Zeitstempel. Die Bundesnetzagentur (BNetzA) schreibt mit dem eigenen Algorithmenkatalog (AlgKat) einen Geltungsbereich für Deutschland fest, nun aber es ist nach wie vor nicht klar, wie eine ausländische qualifizierte Signatur geprüft werden soll. Soll der Prüfung der AlgKat der BNetzA zugrunde gelegt werden, oder müssen die Vorgaben (falls vorhanden) des Ursprungslandes der Signatur berücksichtigt werden?

Zwar wird in der Begründung zum Durchführungsbeschluss (EU) 2016/650 der Kommission vom 25. April 2016 unter der Ziffer (8) auf die Notwendigkeit der Verwendung von geeigneten kryptographischen Algorithmen und Schlüssellängen verwiesen, jedoch ohne diesbezüglich verbindenden Vorgaben zu erlassen. Es wird gleichzeitig auf die notwendige Zusammenarbeit der Mitgliedsstatten zwecks einer Harmonisierung solcher Vorgaben verwiesen. Solange das Ziel der Harmonisierung nicht erreicht wird, bleibt das oben genannte Problem allerdings offen. Dies ist umso kritischer, als dass jede qualifizierte elektronische Signatur / Siegel / Zeitstempel durch öffentliche Stellen gem. eIDAS-Verordnung anzunehmen und zu prüfen ist, also auch von ausländischen Vertrauensdiensteanbietern.

Es wird daher empfohlen, eine Präzisierung des Umgangs mit der Eignung der kryptographischen Algorithmen und Schlüssellängen vorzunehmen, insbesondere bei der Prüfung von nicht deutschen qualifizierten Signaturen/Siegel und Zeitstempel im VDG.

4 Antworten auf Referentenfragen im Gesetzesentwurf

- § 11 Absatz 1: Referentenfrage: "Sind auch bei e-Siegeln Attributzertifikate sinnvoll, etwa um die Vertretungsverhältnisse offenzulegen?"
  Antwort: Ja, auch bei e-Siegeln machen *Attribute in Zertifikaten* Sinn, bspw., wenn ein Rechenzentrum im Auftrag einer Bank Konto-Auszüge signiert, aber keine separaten Attributzertifikate.
- § 13 Absatz 1 Nr 2: Referentenfrage: "Ist Widerruf bei Website-Zertifikaten üblich/möglich/sachgerecht?"
  Antwort: Ja, eine Sperre durch die Zertifizierungsstelle ist möglich. Die Gründe dafür sind üblicherweise in den begleitenden Dokumenten CP / CPS der Zertifizierungsstelle beschrieben.
- § 14 Absatz 1 Nr 1: Referentenfrage: "Ist das auch bei Websitezertifikaten üblich?
  Antwort: Ja, das ist auch bei Websitezertifikaten möglich.
- § 15 Absatz 1 Nr 2: Referentenfrage: "Ist das (Übernahme / Sperrung) bei Websitezertifikaten möglich?"
  Antwort: Dieses ist bei Websitezertifikaten nicht möglich, Die Zertifikate müssen von einem alternativen Anbieter nach vorheriger Beantragung neu ausgestellt werden.

Im Folgenden finden sich Anmerkungen zum Gesetzestextentwurf in der Reihenfolge der Artikel.

5 Kritik anhand des Gesetzestextes

Bezug	Empfehlung	Begründung/Ziel
§ 1, Absatz 2	Streichung des Absatzes	Das eIDAS-Durchführungsgesetz soll den europäischen Binnenmarkt stärken. Über die Verordnung hinausgehende nationale Regulierungen konterkarieren dieses Ziel zum Nachteil von Verwaltung und Verbrauchern. § 1, Absatz 2 würde als deutsche Sonderlösung Innovationen ausbremsen und damit erhebliche Wettbewerbsnachteile für die Unternehmen im deutschen Markt nach sich ziehen. *Zu diesem Punkt konnte im Verlauf der verbandsinternen Erörterungen kein abschließender Konsens erzielt werden. Er ist insofern nicht Teil der TeleTrusT-Stellungnahme, sondern hier nur informativ wiedergegeben.*
§ 2, Absatz 1	Es wäre grundsätzlich wünschenswert, nur einer Aufsichtsbehörde, idealerweise der Bundesnetzagentur, rechenschaftspflichtig zu sein.	So könnten Aufwände für Organisation, Verwaltung und Bürokratie für deutsche Anbieter minimiert und die Wettbewerbsfähigkeit erhöht werden. Durch zusätzliche Aufwände für Anbieter werden deren Produkte entsprechend teurer und sind somit ggf. nicht marktfähig. Es wird eine Klarstellung dahingehend angeregt, dass Unternehmen bei einer Meldung an nur eine Stelle jedenfalls nicht mit Bußgeldern belegt werden können. Idealerweise würde diese Stelle relevante Informationen mit der entsprechenden Behörde teilen und den Unternehmen damit mehr Zeit für die Bewältigung eines eventuellen Ernstfalles verschaffen. *Zu diesem Punkt konnte im Verlauf der verbandsinternen Erörterungen kein abschließender Konsens erzielt werden. Er ist insofern nicht Teil der TeleTrusT-Stellungnahme, sondern hier nur informativ wiedergegeben.*
§ 2, Absatz 2	Streichung des Absatzes	Die in der Folge des IT-Sicherheitsgesetzes geregelten Meldepflichten nach IT-KRITIS lassen hier eine unnötige doppelte Meldepflicht entstehen. *Zu diesem Punkt konnte im Verlauf der verbandsinternen Erörterungen kein abschließender Konsens erzielt werden. Er ist insofern nicht Teil der TeleTrusT-Stellungnahme, sondern hier nur informativ wiedergegeben.*
§ 4	kritische Prüfung des Paragraphen	Ist das in der eIDAS-Verordnung (Artikel 17 Absatz 4) bereits vollständig geregelt?
	ODER Die Festlegung auf Kettenmodell streichen, da ETSI-Norm keinen der genannten Ansätze favorisiert.	Die ETSI Standards und insbesondere der ETSI-Standard EN 319 102-1 V1.1.1 2016, lassen sowohl das Schalen- wie auch das Kettenmodell zu, so dass sowohl eine Prüfung nach dem Kettenmodell, aber eben auch nach dem Schalenmodell möglich ist. Es hängt immer von dem Signierenden oder dem Prüfenden ab, welches Modell zur Anwendung kommt. Daher empfehlen wir zur Vermeidung von Fehlinterpretationen, auf eine Nennung des Kettenmodells in der Begründung zu verzichten.
§ 5, Absatz 1	kritische Prüfung des Absatzes	Die Anforderungen an Mitwirkungspflichten für Vertrauensdiensteanbieter gehen weit über die eIDAS-Verordnung hinaus. Dadurch entstehen Kosten und Wettbewerbsnachteile für deutsche Anbieter. Die wesentlichen Punkte sind bereits im Konformitätsbewertungsbericht gemäß eIDAS definiert.
§ 7	Anwendbarkeit prüfen	Die Anwendbarkeit des § 7 auf die übrigen Vertrauensdienste (außer Vertrauensdiensteanbieter zur Erzeugung und Validierung qualifizierter Zertifikate) sollte überprüft werden.
§ 7, Absatz 1	Streichung des Absatzes	Entsprechende Regelungen sind sowohl im Bundesdatenschutzgesetz als auch in der europäischen Datenschutzgrundverordnung enthalten. So regelt Artikel 5 der eIDAS-Verordnung bereits die Vorgaben für den Datenschutz.
§ 7, Absatz 1	ODER Es sollte für die Anwendung in Bewahrungsdiensten zumindest das Wort "unmittelbar" entfallen	Ein Bewahrungsdienst muss in der Lage sein, die Zertifikatskette bis zur Root einer zu bewahrenden Signatur prüfen zu dürfen, um die "long-term validity of signatures, seals, timestamps", wie es in eIDAS-

		Verordnung gefordert wird, sicher zu stellen. Dabei muss es auch möglich sein, dass (neben dem Signatur-/Siegel-/Zeitstempel- Ersteller) Bewahrungsdienste Maßnahmen zur Beweiswerterhaltung im Rahmen der gesetzlich vorgeschriebenen Aufbewahrungszeit vornehmen können, ohne direkte Einbeziehung der ursprünglichen Siegnatur-/Siegel-/Zeitstempel-Ersteller, zu denen der Bewahrungsdienst u. U. gar keine Geschäftsbeziehung hat.
§ 7, Absatz 2, Nr. 1	keine Pflicht zur Übermittlung von Daten für die Verfolgung von Ordnungswidrigkeiten und keine Datenübermittlung zu Zwecken der Erfüllung der gesetzlichen Aufgaben der Finanzbehörden	Es wird sich gegen eine Pflicht zur Übermittlung von Daten für die Verfolgung von Ordnungswidrigkeiten ausgesprochen. Weiterhin wird empfohlen, keine Datenübermittlung zu Zwecken der Erfüllung der gesetzlichen Aufgaben der Finanzbehörden vorzusehen. Neben grundsätzlichen datenschutzrechtlichen Bedenken entstünden unzumutbare Verwaltungsbelastungen für deutsche Unternehmen.
§ 9	Schadenshöchstsumme reduzieren UND Deckelung der Gesamthaftung bzw. Formulierung "haftungsauslösenden Ereignisses" durch eine enger gefasste Regelung ersetzen	Die vorgesehene Schadenshöchstsumme sollte reduziert und am EU-Durchschnitt orientiert werden. Zusätzlich sollte eine Deckelung der Gesamthaftung bei mehreren miteinander verbundenen haftungsauslösenden Ereignissen erwogen werden oder die Formulierung des "haftungsauslösenden Ereignisses" durch eine enger gefasste Regelung (etwa "verursachten Schaden") ersetzt werden. Niedrigere Deckungsniveaus in anderen EU-Staaten können zu Wettbewerbsnachteilen für deutsche Anbieter führen, die deutlich höhere Kapital- bzw. Versicherungsnachweise vorhalten müssten.
§ 10, Absatz 1	kritische Prüfung des Absatzes	Durch Einschränkung der zugelassenen Identifizierungsmöglichkeiten durch die BNetzA kann ein Wettbewerbsnachteil für deutsche Vertrauensdiensteanbieter entstehen, da diese dann u. U. in anderen Ländern zugelassene Identifizierungsverfahren nicht nutzen können. Daher sollte jede rechtliche Festlegung mit größter Sorgfalt und möglichst unter Rücksprache interessierter Kreise erfolgen.
§ 11	Anmerkungen zur Validierung "deutscher Attribute"	Die Ansätze, einige wenige Regelungen aus dem Signaturgesetz zu übernehmen und die Möglichkeiten zur Konkretisierung durch den nationalen Gesetzgeber auszunutzen, sind in einzelnen Fällen ggf. sinnvoll, können aus internationaler Sicht jedoch Probleme bei der Validierung verursachen. Zu nennen sind hier die Regelungen zu den Attributen, die für den elektronischen Rechtsverkehr in Deutschland unerlässlich sind. Nach Artikel 28 Absatz 3 der eIDAS-Verordnung sind Attribute in Zertifikaten fakultativ zulässig und dürfen die Interoperabilität von Signaturen lediglich nicht beeinträchtigen. Die technische Umsetzung muss dementsprechend erfolgen, damit keine Probleme bei der internationalen Validierung mit Wettbewerbsnachteilen entstehen.
§ 11, Absatz 3	Streichung des Absatzes	So widerspricht die Regelung in § 11, Absatz 3 den Vorgaben der eIDAS-Verordnung. Gesonderte Qualifizierte Attribut-Zertifikate wären eine deutsche Sonderausprägung, die international nicht zu validieren wären.
§ 12, Absatz 1	Aufzählung 1-3 streichen	Der Stand der Technik ist durch europäische Normen bereits hinreichend definiert. Der Standard für Trust Service Provider wäre EN 319 401 in denen die Belehrung geregelt wäre.
§ 13	kritische Prüfung des Absatzes	Art. 24 Absatz 3 der eIDAS-Verordnung regelt den Widerruf hinlänglich. Zu prüfen wäre, ob § 13 wäre damit vollständig verzichtbar ist. Offen ist, weshalb das BMWi von einer Regelung von "Suspendierungen qualifizierter Zertifikate" abgesehen hat. Im Übrigen ist ein Widerruf bei Website-Zertifikaten möglich und sinnvoll.
§ 13, Absatz 1	Das Wort "unverzüglich" sollte gestrichen werden.	Außerdem stellt eine zeitliche Definition "unverzüglich" eine unzulässige Verschärfung der in der eIDAS-Verordnung vorgesehenen Regelung "innerhalb von 24 Stunden" dar. Es sollte dem Vertrauensdiensteanbieter ggf. freigestellt sein, Zeitfenster zum Stellen von Sperranträgen zu definieren (z.B. zu seinen üblichen Geschäftszeiten).

§ 14, Absatz 1	Es wird folgende Formulierung empfohlen:	"Der qualifizierte Vertrauensdiensteanbieter hat die nach Art. 24, Absatz 2 Buchstabe h der Verordnung (EU) Nr. 910/2014 aufzuzeichnenden einschlägigen Informationen aufzuzeichnen und aufzubewahren." Der Regelungsgegenstand ist in Art. 24, Absatz 2 Buchstabe h der eIDAS-Verordnung abschließend geregelt.
§ 15, Absatz 3 und 4	kritische Prüfung der Absätze	Es besteht der Anschein, dass durch die Privilegierung qualifizierter Vertrauensdiensteanbieter, die einen Beendigungsplan besitzen, als "Anbieter von auf Dauer prüfbaren Vertrauensdiensten" ein Typ von Vertrauensdiensteanbietern und Zertifikaten eingeführt wird, die in dieser Form in der eIDAS-Verordnung nicht vorgesehen sind. Faktisch wird hier die qualifizierte elektronische Signatur mit Anbieterakkreditierung für eIDAS-Verordnung spezifiziert – ein Signaturtyp, den die Verordnung selbst nicht definiert. Der Bedarf einer solchen neuen Zertifikatskategorie resp. Privilegierung von Vertrauensdiensteanbietern besteht nach unserer Erfahrung branchenübergreifend nicht. Ohne eine sorgfältige Abgrenzung stellt das eine Markteinschränkung für ausländische Vertrauensdiensteanbieter dar, da eine solche Regelung außerhalb Deutschlands unüblich ist. Daneben erscheint es europarechtlich kritisch, einen "auf Dauer prüfbaren Vertrauensdienst" auf Basis einer faktisch weiteren Zertifikatskategorie zu schaffen. Beides ist je nach Auslegung in der eIDAS-Verordnung nicht vorgesehen, da die eIDAS-Verordnung auch nicht die Möglichkeit eröffnet, neue Typen von Vertrauensdiensteanbietern oder Zertifikaten für die durch die Verordnung harmonisierten Vertrauensdienste zu schaffen. Da die Langzeit-Prüfbarkeit von Zertifikaten nach einigen Rechtsvorschriften im öffentlichen Bereich zwingend gegeben sein muss, z.B. bei der Erstellung von Urkunden nach § 39a Satz 3 des Beurkundungsgesetzes oder nach § 33 Absatz 5 Satz 1 Nummer 2 Halbsatz 2 des Verwaltungsverfahrensgesetzes, sollte eine kritische Prüfung des Absatzes unter Berücksichtigung dieser Anmerkungen erfolgen.
	Aufnahme eines neuen § 16 im allgemeinen Teil und damit Änderung der folgenden Paragraphen zu §§ 17 ff.	eIDAS definiert derzeit keine verbindlichen Standards zur Beweiswerterhaltung, sondern nur die rechtliche Verpflichtung dazu. Es liegen keine Implementing Acts zur Beweiswerterhaltung vor, ob und wenn ja wann welche kommen ist derzeit unklar. Es liegen keine EU-weit einheitlichen Standards zur Beweiswerterhaltung vor, ob und wenn ja wann welche kommen ist unklar. Daher hat der Anwender im Ergebnis, ohne den Verweis auf ein etabliertes wie valides Verfahren im VDG, derzeit keinerlei rechtssicheres Verfahren zur Beweiswerterhaltung. Wir empfehlen eine Regelung dieses Verfahrens wie folgt: **§ xx (z.V. § 16) Zeitraum und Verfahren zur langfristigen Beweiswerterhaltung von und mit digitalen Signaturtechniken** (1) Qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten sind neu zu sichern, wenn diese für eine längere Zeit in gesicherter Form benötigt werden, als die für die Erstellung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter der vorhandenen digitalen Signaturtechniken (z. B. qualifizierten elektronischen Signaturen, Siegeln oder elektronischen Zeitstempel, etc.) als sicherheitsgeeignet beurteilt sind. (2) Ebenso ist die Bewahrung der digitalen Signaturtechniken, z. B. der elektronischen Signaturen, Siegeln oder Zertifikaten nach Artikel 3 Nummer 16 Buchstabe c der Verordnung (EU) Nr. 910/2014, bei Bedarf durch eine neue Sicherung sicher zu stellen, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zertifikate durch Zeitablauf geringer wird. (3) In den Fällen gemäß Satz (1) und (2) sind die Daten oder die digitalen Signaturtechniken vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer

		neuen Sicherung zu versehen. Diese neue Sicherung muss nach dem Stand der Technik mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen und frühere Sicherungen einschließen. (4) Der Stand der Technik, wie in den einschlägigen Standard beschrieben, ist anzuwenden. Hinweis: Für den Erhalt des Beweiswerts qualifiziert elektronisch signierter Dokumente kann z. B. die Technische Richtlinie des BSI (TR-03125 (TR-ESOR)) als Stand der Technik herangezogen werden. Diese ist abrufbar unter: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html.
§ 17	die Streichung des Paragraphen	Hier werden zusätzliche Regeln für Konformitätsbewertungsstellen formuliert, die mutmaßlich an Vertrauensdiensteanbieter weitergegeben und damit zu Wettbewerbsnachteilen führen werden.
§ 18	kritische Prüfung des Paragraphen Streichung der einseitigen Bevorzugung von De-Mail Festlegung des Zertifizierungsverfahrens für Einschreib- und Zustelldienste und Präzisierung des Umgangs/der Anerkennung ausländischer Vertrauensdiensteanbieter und Darstellung für den Umgang mit den Zustelldiensten	Der Paragraph geht in seiner Ausführung ausschließlich auf die De-Mail ein und schafft somit einen Eindruck, dass der genannte Zustelldienst bevorzugt wird. Der Umgang mit ausländischen (bereits zertifizierten) Einschreib- und Zustelldiensten und vor allem die Vorgaben zur Zertifizierung anderer Zustelldiensten wird weder präzisiert noch angesprochen. Es bleibt unklar, warum die De-Mail-Dienste keiner erneuten Prüfung nach eIDAS-Verordnung bedürfen. Ebenso bleibt ungeregelt, wie mit der derzeitigen Privilegierung von De-Mail im E-Government-Gesetz, eJustice-Gesetz etc. umgegangen wird. Diese kann als Markteinschränkung gegenüber anderen Einschreib- und Zustelldiensten betrachtet werden, was im Kontext der eIDAS-Verordnung zumindest kritisch geprüft werden sollte, da auch Einschreib- und Zustelldienste nach eIDAS-Verordnung die Eigenschaften der De-Mail-Dienste umfassen können. Weitere Verfahren zur Zulassung von Einschreib- und Zustelldienste könnten durch die VDV geregelt werden.
§ 19, Absatz 2, Nr. 7	Ergänzung:	"entgegen Artikel 24 Absatz 2 Buchstabe e oder f, jeweils in Verbindung mit einer Rechtsverordnung nach § 20 Absatz 1 Nummer 1, ein gemäß eIDAS vertrauenswürdiges System oder Produkt nicht verwendet," Im Sinne einer Harmonisierung des europäischen Binnenmarktes sollte eine eindeutige Regelung im Sinne der eIDAS-Verordnung getroffen werden.
§ 20, Absatz 1	Nummern 1 und 2 streichen UND Änderung:	Der Regelungsgegenstand ist durch europäische Normen (EU) Nr. 910/2014 und EN 319 411-2 bereits hinreichend definiert. "Die Bundesregierung wird ermächtigt, durch Rechtsverordnung die zur Durchführung der Verordnung (EU) Nr. 910/2014 und dieses Gesetzes erforderlichen Rechtsvorschriften nach vorheriger Anhörung zu erlassen"
	zusätzliche Ziffer "6."	"[…] 6. weitere Details zu den elektronischen Vertrauensdiensten. Es sollte eine Möglichkeit eingeräumt werden, potentielle Regelungslücken, die möglicherweise nicht durch die EU-Regularien geschlossen werden, in der VDV anzusprechen.
§ 21	Vertrauensdienstegesetz gemeinsam mit oder in unmittelbarer zeitlicher Nähe zu der geplanten Vertrauensdiensteverordnung verabschieden	Sollte die geplante Vertrauensdiensteverordnung mit zeitlicher Verzögerung verabschiedet werden, entstünde erneut Rechtsunsicherheit für deutsche Unternehmen. Dies gilt es zu vermeiden.
§ 21, Absatz 2 Satz 2	Festsetzung einer Frist für die Anerkennung durch die Aufsichtsstelle nach § 15 Absatz 3 Satz 1.	Die Regelung könnte die Umsetzungsfrist nach eIDAS zum 1.7.2017 aufheben. Offen ist zudem, welche Dienste von der Regelung eingeschlossen sind. Andernfalls müsste die eIDAS- Konformität (Art. 51) bezweifelt werden.

6 Ausblick/Offene Fragen klären

Es besteht in einigen Zusammenhängen inhaltlicher Klärungsbedarf.

- § 3 "Verwaltungsverfahren nach diesem Gesetz oder nach einer Rechtsverordnung nach § 20 können über eine einheitliche Stelle im Sinne des Verwaltungsverfahrensgesetzes abgewickelt werden."
  Es ist nicht hinreichend deutlich, wer die einheitliche Stelle im Sinne des Verwaltungsverfahrensgesetzes ist. Es besteht Konkretisierungsbedarf.
- § 8 "Der Bundesetzagentur obliegt das Führen von Vertrauenslisten nach Artikel 22 Absatz 1 der Verordnung (EU) Nr. 910/2014"
  Wir regen an, die Zusammenarbeit und die Fristen für die Aktualisierung der Trust-Service-Status-Lists (TSL) für Behörden zu regeln.
- Folgeänderungen
  Die Folgeänderungen in weiteren Gesetzen beschränken sich unseres Erachtens derzeit zurecht auf den Austausch der Bezugsnormen (eIDAS-Verordnung statt Signaturgesetz). Ob und wie die durch die eIDAS-Verordnung neu geschaffenen Vertrauensdienste mit rechtlichen Wirkungen ausgestattet werden sollten, bedarf dagegen weiterer genauer Betrachtung, die in der Kürze der zur Verfügung stehenden Zeit nicht geleistet werden kann. Da eine gesetzliche Klarstellung im Hinblick auf das Signaturgesetz aber so bald wie möglich erfolgen sollte, halten wir den "schlanken Ansatz" des BMWi zunächst für hinnehmbar.

Aus unserer Sicht ist eine Beteiligung der interessierten Kreise bei der Gestaltung der Verordnung dringend geboten.

Ansprechpartner für Rückfragen:

Christian Seegebarth
Leiter der TeleTrusT-AG "Forum elektronische Vertrauensdienste AK A"