Stellungnahme

Referentenentwurf einer Vertrauensdiensteverordnung

27. Juli 2018

Einleitung

Mit dem Inkrafttreten der Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt der Europäischen Union (eIDAS) wurde die Basis für eine europaweite, rechtsgültige elektronische Kommunikation und sichere elektronische Identifizierung geschaffen. Mit Hilfe der Vertrauensdienste - elektronischen Signaturen, Siegeln, Zeitstempeln, Zustelldiensten und Zertifikaten zur Authentifizierung - können Unternehmen, Verwaltungen und Privatpersonen jetzt digitale Dokumente wie Angebote, Bestellungen, Verträge u.v.m. innerhalb der Europäischen Union auf einer einheitlichen Rechtsbasis austauschen. Damit löste die neue EU Verordnung nicht nur das deutsche Signaturgesetz und Signaturverordnung ab, sondern schafft auch neue Anwendungsmöglichkeiten innerhalb und zwischen allen Ländern der Europäischen Union. Ergänzt wird die eIDAS Verordnung (eIDAS VO) durch das Vertrauensdienstegesetz (VDG), das am 29. Juli 2017 in Kraft getreten ist.

Das Ministerium für Wirtschaft und Energie (BMWi) hat kürzlich einen Referentenentwurf für eine das VDG ergänzende Vertrauensdiensteverordnung (VDV) veröffentlicht und die Fachöffentlichkeit zu einer Stellungnahme aufgefordert. Die bisherigen Erfahrungen mit der eIDAS VO und dem VDG haben aus Sicht des BMWi gezeigt, dass wenige letzte Präzisierungen erforderlich sind, damit Vertrauensdiensteanbieter und Zertifizierungsstellen ihre Anforderungen aus der eIDAS VO und dem VDG zuverlässig erfüllen können. Sie betreffen inhaltlich die Barrierefreiheit von Vertrauensdiensten, die Deckungsvorsorge qualifizierter Vertrauensdiensteanbieter, die Dokumentation bei der Ausgabe qualifizierter elektronischer Zertifikate, die Vorsorge für die dauerhafte Prüfbarkeit qualifizierter elektronischer Signaturen und Siegel sowie die Anzeigepflichten zu qualifizierten elektronischen Signatur- oder Siegelerstellungseinheiten. Die Verordnung soll die erforderliche Rechtssicherheit schaffen, damit Vertrauensdiensteanbieter mehr Klarheit darüber haben, wie sie bestimmte Anforderungen der eIDAS VO und des VDG zuverlässig erfüllen können.

Bitkom bedankt sich für die Gelegenheit zum Referentenentwurf der VDV Stellung zu

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Rebekka Weiß, LL.M.
Bereichsleiterin
Datenschutz & Verbraucherrecht
T +49 30 27576 161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

nehmen. Der Bitkom Arbeitskreis Anwendung elektronischer Vertrauensdienste ist das Gremium, das sich thematisch mit den Inhalten des Gesetzgebungsverfahrens und der eIDAS VO auseinandersetzt. Aus Sicht des Arbeitskreises ist es von besonderer Bedeutung, alle Regulierungsmaßnahmen stets im Zusammenhang zu betrachten und vor allem den einheitlichen eIDAS-Vertrauensraum zu stärken. Die Bedeutung dieser Einheitlichkeit und der notwendigen Harmonisierung zeigt sich sowohl z.B. in der Frage der national anerkannten Identifizierungsmethoden (siehe vor allem die kürzlich veröffentlichte Bitkom Stellungnahme zum Videoidentverfahren) als auch in nationalen Verordnungen wie der hier vorliegenden VDV.
Die nachfolgende Kommentierung ist in diesem Arbeitskreis erarbeitet worden und gibt den Eindruck der betroffenen Unternehmensbereiche, der Anbieter und Anwenderbranchen wieder.

A. Grundsätzliche Anmerkungen zum Inhalt der Vertrauensdiensteverordnung

I. Inhaltliche Beschränkung der VDV

Entgegen der eIDAS Verordnung bezieht sich der aktuelle Entwurf inhaltlich ausschließlich auf Signaturen und entsprechende Dienste. Die Verordnung stellt jedoch auch den Rahmen für weitere Vertrauensdienste wie z.B. die Zustellung elektronischer Einschreiben. Da für diese Dienstarten zum Teil unterschiedliche Anforderungen, Notwendigkeiten und Rahmenbedingungen existieren, sollten diese Dienste auch in der Verordnung entsprechend getrennt behandelt werden. Beispielhaft hat § 4 Absatz 1 für qualifizierte Einschreibedienste keine Relevanz, gilt aber für diese mit, da die VDV ausdrücklich Geltung für alle Qualifizierten Vertrauensdiensteanbieter beansprucht. Der Versuch einer einheitlichen Handhabung kann durch zusätzliche oder unpassende Regelungen ein Angebot solcher Vertrauensdienste aus Deutschland heraus unwirtschaftlich und bei Widersprüchen sogar unmöglich machen.

Gleiches gilt grundsätzlich auch für das Vertrauensdienstegesetz.

Bitkom fordert daher, die gesamte VDV dahingehend anzupassen, dass zwischen den einzelnen Vertrauensdiensten differenziert wird. Die VDV muss sämtliche Vertrauensdienste erfassen und darf weder sprachlich noch inhaltlich auf Siegel und Signaturen beschränkt sein.

II. Ergänzung eines Verweises auf die Sicherheitsniveaus „substanziell“ oder „hoch“ gemäß Anhang Durchführungsverordnung (EU) 2015/1502 zur Beurteilung der Eignung innovativer Identifizierungsmethoden

§11 Absatz 3 VDG regelt die Bedingungen, zu denen die BNetzA innovative Identifizierungsmethoden gemäß Art. 24 Absatz 1 lit. d der eIDAS VO genehmigen kann.

Die eIDAS VO macht zu dem zur Zulassung innovativer Identifizierungsmethoden geforderten Sicherheitsniveau jedoch keine Vorgaben, sondern fordert lediglich eine „gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit“. Im VDG wird ebenfalls keine weitere Vorgabe zu dem für die Zulassung einer innovativen Identifizierungsmethode notwendigen Sicherheitsniveau gemacht.

„Persönliche Anwesenheit“ definiert jedoch kein Sicherheitsniveau, so dass hinsichtlich der Sicherheitsanforderungen an innovative Identifizierungsmethoden eine Regelungslücke besteht. Diese Regelungslücke erschwert die Beurteilung innovativer Identifizierungsmethoden hinsichtlich ihrer gleichwertigen Sicherheit.

Bitkom fordert deshalb, diese Regelungslücke in der VDV zu schließen und die Beurteilung des Sicherheitsniveaus von innovativen Identifizierungsmethoden an Art. 24 Absatz 1 lit. b eIDAS VO auszurichten. Dort wird die Überprüfung hinsichtlich des Sicherheitsniveaus „substanziell“ oder „hoch“ gemäß Art. 8 eIDAS VO gefordert. Die dabei anzuwendenden Anforderungen sind im Anhang der Durchführungsverordnung (EU) 2015/1502 technologieneutral aufgeführt.

III. Hinweis auf die Zulässigkeit zur Regelung der Sicherheitsniveaus im Rahmen der VDV durch die Verordnungsermächtigung nach § 20 VDG

In §20 Absatz 2 Nr. 1 VDG wird die Bundesregierung ermächtigt, weitere Vorgaben zu erlassen über

> *„die Ausgestaltung der Pflichten der Vertrauensdiensteanbieter bei der Betriebsaufnahme, während des Betriebs und bei der Einstellung des Betriebs nach den Artikeln 17 bis 24 der Verordnung (EU) Nr. 910/2014 und nach den §§ 4 und 5, 9 bis 18“*

Die Anforderungen an innovative Identifizierungsmethoden sind in Art. 24 eIDAS VO sowie in § 11 VDG geregelt, so dass die Konkretisierung der Sicherheitsniveaus im Rahmen der Verfügung zulässig ist.

B. Bitkom Anmerkungen zu den einzelnen Abschnitten der Vertrauensdiensteverordnung:

I. Zu § 1 Anforderungen an die Barrierefreiheit

Wortlaut des Entwurfs:
Barrierefreie Dienste gemäß § 7 Absatz 1 des Vertrauensdienstegesetzes und die Hinweise und Informationen zur Barrierefreiheit nach § 7 Absatz 2 des Vertrauensdienstegesetzes sollen wahrnehmbar, bedienbar, verständlich und robust sein. Dabei sollen sie sich am Stand der Technik orientieren.

Bitkom schlägt vor, § 1 zu streichen oder alternativ redaktionell anzupassen und inhaltlich zu präzisieren
Barrierefreie Dienste gem. § 7 Abs.1 des VDG sollen, soweit technisch möglich, für Menschen mit Behinderungen bedienbar und robust sein. Hinweise und Informationen zur Barrierefreiheit nach § 7 Abs. 2 Satz 3 VDG sollen barrierefrei wahrnehmbar und verständlich sein.

Begründung:
Der Mehrwert von § 1 im Vergleich mit § 7 VDG erschließt sich bisher nicht. Insbesondere sollte § 1 VDV hinsichtlich der Anforderungen an die Barrierefreiheit nicht über das VDG hinausgehen (die Konkretisierung der Anforderungen „soweit möglich“ muss daher auch in der VDV aufgegriffen werden). Der Referentenentwurf berücksichtigt zudem nicht hinreichend, dass die Anforderungen an die barrierefreien Dienste i.S.v. § 7 Abs. 1 inkl. der dazu benötigten Hardware naturgemäß nicht identisch sein können mit denen, die für Hinweise und Informationen i.S.v. § 7 Abs. 2 Satz 3 VDG gelten. Daher ist eine Differenzierung nach Diensten und Informationen geboten. Außerdem muss für Dienste entsprechend der Einschränkung des VDG die technische Machbarkeit als restriktives Kriterium Berücksichtigung finden. Die im Referentenentwurf vorgesehene „Orientierung am Stand der Technik“ erscheint unscharf und begründet die Gefahr von Auslegungsschwierigkeiten.

II. Zu § 2 Ausgestaltung der Deckungsvorsorge für qualifizierte Vertrauensdiensteanbieter

Bitkom schlägt vor, eine maximale Deckungsvorsorge in § 2 aufzunehmen

Begründung:
Die Mindestsumme zur Deckungsvorsorge laut § 10 VDG sieht jeweils 250.000 Euro für einen Schadensfall vor. Hier ist ein maximaler Wert für entstehende Schäden als Vorgabe wünschenswert. In der Signaturverordnung regelte hierzu der folgenden Passus: *Wird eine Jahreshöchstleistung für alle in einem Versicherungsjahr verursachten Schäden vereinbart, muss sie mindestens das Vierfache der Mindestversicherungssumme betragen* (siehe § 9 Ausgestaltung der Deckungsvorsorge in (2) Punkt 2. der Signaturverordnung). Dies sollte daher auch in der VDV entsprechend Anwendung finden.

III. Zu § 3 Dokumentation der Ausgabe qualifizierter Zertifikate für Vertrauensdienste

Wortlaut des Entwurfs

(1) Soweit der Vertrauensdiensteanbieter bei der Ausgabe qualifizierter Zertifikate die Identität oder Attribute an Hand öffentlicher und auf Dauer zugänglicher Register oder Dokumente überprüft, genügt es, dass er vermerkt, in welches Register oder Dokument er Einsicht genommen hat und ob die verarbeiteten Daten mit denen im Register übereinstimmen. Ein Auszug des Registers oder Dokuments muss nicht zur Dokumentation genommen werden.

(2) Nach § 12 des Vertrauensdienstegesetzes erforderliche Vollmachten, Einwilligungen oder Bestätigungen müssen qualifiziert elektronisch signiert, qualifiziert elektronisch gesiegelt oder handschriftlich unterschrieben sein.

Bitkom schlägt vor, § 3 Abs. 2 inhaltlich wie folgt anzupassen:
(2) Nach § 12 des Vertrauensdienstegesetzes erforderliche Vollmachten, Einwilligungen oder Bestätigungen müssen qualifiziert elektronisch signiert, qualifiziert elektronisch gesiegelt, handschriftlich unterschrieben oder erfolgen in einem organisatorisch-technischen Prozess, der einer eIDAS-Konformitätsbewertung unterliegt.

Begründung:
eIDAS-konforme organisatorisch-technische Prozesse stellen eine technikneutrale Öffnung dar, die es ermöglicht, auf technische Entwicklungen zu reagieren, ohne dass ein Verlust an Sicherheit einhergeht. Letzteres wird durch die Konformitätsbewertung gegen die EU-Verordnung eIDAS sichergestellt.

IV. Zu § 4 Vorsorge für die dauerhafte Prüfbarkeit qualifizierter Zertifikate

Wortlaut des Entwurfs:
(1) Qualifizierte Vertrauensdiensteanbieter haben Vorsorge zu treffen, dass ihre Zertifikatsdatenbank im Falle einer Betriebseinstellung im Sinne des § 16 Absatz 1 Satz 1 des Vertrauensdienstegesetzes von einem anderen qualifizierten Vertrauensdienste-anbieter oder der Bundesnetzagentur übernommen werden kann.
(2) Die Bundesnetzagentur veröffentlicht Kriterien, die eingehalten werden sollen, um eine Übernahme durch die Bundesnetzagentur zu ermöglichen.
(3) Liegt die Dokumentation, die nach § 16 Absatz 1 Satz 3 des Vertrauensdienste-gesetzes zu übergeben ist, noch in Papierform vor, soll sie, soweit möglich und zweckmäßig, vor der Übergabe in elektronische Dokumente überführt werden. Für die Bewertung der Durchführbarkeit von Maßnahmen nach Satz 1 sind auch technische und wirtschaftliche Belange zu berücksichtigen. Für die Bewertung der Zweckmäßigkeit ist der Aufwand daran zu messen, ob das Ziel erreicht werden kann, auf die weitere Aufbewahrung der Papierdokumente zu verzichten.
(4) Ein qualifizierter Vertrauensdiensteanbieter soll die Bundesnetzagentur über eine beabsichtigte Betriebseinstellung im Sinne des § 16 Absatz 1 Satz 1 des VDG unverzüglich unterrichten.

Bitkom schlägt vor, § 4 Abs. 1 inhaltlich anzupassen und § 4 Absatz 2 zu streichen
In § 4 Absatz 1 sollte inhaltlich angepasst und folgender Passus gestrichen werden: „oder der Bundesnetzagentur“. Weiterhin sollte § 4 Absatz 2 gestrichen werden und eine Regelung zur Begrenzung der Speicherdauer aufgenommen werden.

(1) Ergänzung von Abs. 1:
Qualifizierte Vertrauensdiensteanbieter haben Vorsorge zu treffen, dass ihre Zertifikatsdatenbank im Falle einer Betriebseinstellung im Sinne des § 16 Absatz 1 Satz 1 des Vertrauensdienstegesetzes von einem anderen qualifizierten Vertrauensdiensteanbieter übernommen werden kann. Der qualifizierte Vertrauensdiensteanbieter ist verpflichtet hierfür den Stand der Technik zu berücksichtigen.

Begründung:
Im Markt sind verschiedene technische Lösungen verfügbar, die eine Übergabe der Zertifikatsdatenbank ermöglichen. Darüber hinaus gibt es für die langfristige Beweiswerterhaltung spezialisierte (zum Beispiel qualifizierte) Vertrauensdienste gemäß der eIDAS VO, die mit der Aufgabe der Verwahrung der Zertifikatsdatenbank betraut werden können.

(2) Streichung von „oder der Bundesnetzagentur“ in Abs. 1:

Begründung:

Die weiteren Festlegungen in Absatz 1 sind hinreichend, um die Verfügbarkeit der Zertifikatsdatenbank eines Vertrauensdiensteanbieters (VDA) im Falle einer Betriebseinstellung sicherzustellen. Dank eIDAS wird es im Europäischen Markt eine hinreichende Anzahl an VDA geben, die diese Dienste anbieten. Es ist zu erwarten, dass „Qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen“ gemäß Art. 34 eIDAS VO oder „Qualifizierte Validierungsdienste für qualifizierte elektronische Signaturen“ gemäß Art. 33 diese Aufgabe zusätzlich übernehmen.

Eine nationale Regulierung und eine Beauftragung einer Bundesbehörde mit diesen Aufgaben sind aus Gründen einer langfristigen Beweiswerterhaltung nicht erforderlich. Seitens der Wirtschaft werden technische Verfahren eingesetzt, die die langfristige Verfügbarkeit von Zertifikatsdatenbanken auch im Falle der Betriebseinstellung sicherstellen können. Durch eine Versicherung kann die entsprechende Deckungsvorsorge zur Beauftragung Dritter (QVDA) garantiert werden.

(3) Streichung von Abs. 2

Die Streichungen werden empfohlen, da eine nationale Regelung mit einer Zuweisung von Aufgaben an die Bundesnetzagentur einen deutlich erhöhten „Erfüllungsaufwand der Verwaltung“ bedingt und Bürokratie aufbaut. Für die Wirtschaft bereitet die Vorbereitung auf die "Erfüllung der Kriterien" einen zusätzlichen Erfüllungsaufwand und benachteiligen die VDA durch höhere Kosten im Vergleich zum Europäischen Wettbewerb.
Sollte dennoch an einer Beauftragung der Bundesnetzagentur festgehalten werden, so sollte es Voraussetzung sein, das diese Aufgabe im Rahmen eines "Qualifizierten Bewahrungsdienstes" erbracht wird. Dabei ist zu berücksichtigen, dass sich auch die Strukturen und Aufgaben von Bundesbehörden regelmäßig ändern (z. B. Bundesgesundheitsamt), so dass auch eine Betriebseinstellung seitens der Bundesnetzagentur nicht völlig ausgeschlossen werden kann.

Zudem sollten keine zusätzlichen Kriterien zur Ermöglichung der Übernahme der Zertifikatsdatenbank des Vertrauensdiensteanbieters durch die Bundesnetzagentur definierbar sein, da dies einen nicht kalkulierbaren Aufwand auf Seiten des VDA darstellt. Die Anforderungen könnten beliebig oft und detailliert angepasst werden. Dies stellt eine Benachteiligung deutscher VDA gegenüber europäischen VDA dar.

(4) Änderung in Absatz 3

Bitkom schlägt folgende Änderung des Absatzes 3 vor:

Liegt die Dokumentation, die nach § 16 Absatz 1 Satz 3 des Vertrauensdienstegesetzes zu übergeben ist, noch in Papierform vor, soll sie, soweit möglich und zweckmäßig, vor der

Übergabe in elektronische Dokumente überführt werden. Dabei ist der Stand der Technik zu beachten.

In Absatz 3, Satz 1 sollte klargestellt werden, dass die Überführung der papiergebundenen Dokumentation in eine elektronische Dokumentation (Scannen) gem. dem Stand der Technik zu erfolgen hat. Dies ist umso mehr entscheidend, wenn das Papier-Original vernichtet wird. Dies sollte erfolgen, um einen Gleichklang z.B. mit dem eGovG bzw. Anlage R zur BSI TR-03138 TR-RESICAN herzustellen.

(5) Einführung einer zusätzlichen Regelung zur Begrenzung der Speicherdauer
Bitkom schlägt vor, einen zusätzlichen Absatz aufzunehmen:
Die Prüfbarkeit von qualifizierten Zertifikaten und qualifizierten elektronischen Zeitstempeln, die in der Datenbank nach § 16 Abs. 4 gespeichert sind, ist nach Ablauf des Gültigkeitszeitraum, wie im Zertifikat angegeben, für die Dauer von mindestens einem Monat durch den qualifizierten Vertrauensdiensteanbieter sicherzustellen.

Begründung:
In den internationalen Standards wird davon ausgegangen, dass die Zeitdauer für die eine CA die Zertifikate überprüfbar hält, im Zertifikat selber angegeben wird (siehe hierzu RFC 5280, EN 319 412-5). Wir empfehlen, dass der Gesetzgeber sich an den internationalen Standards orientiert, um einen unnötigen Nachteil für deutsche Zertifizierungsanbieter zu verhindern. Eine Überprüfbarkeit, die sich möglicherweise aus verschiedenen Branchenanforderungen ergibt (z.B. ob 10 Jahre Speicherdauer gem. HGB oder über 100 Jahre in der Bergbau- oder Luftfahrtbranche), sollte dann von dem jeweiligen VDA je nach Businessmodell angeboten werden können. Diese Dienste können auch von einem Archivdienstleister angeboten werden, da die Dokumentationspflichten üblicherweise weit über die reine Überprüfbarkeit von Zertifikaten hinausgehen. Auch aus den Grundgedanken der Datensparsamkeit und Speicherbegrenzung (DS-GVO) ist eine Überprüfbarkeit der Zertifikate über den im Zertifikat genannten Zeitraum hinaus abzulehnen.

V. Zu § 5 Anzeigen zu qualifizierten elektronischen Signatur- oder Siegelerstellungseinheiten

Wortlaut des Entwurfs:
Die Zertifizierungsstellen nach § 17 des Vertrauensdienstegesetzes sind verpflichtet, der Bundesnetzagentur neue Zertifizierungen qualifizierter elektronische Signatur- oder Siegelerstellungseinheiten unverzüglich anzuzeigen. Annullierungen der Zertifizierungen oder Informationen über nicht mehr zertifizierte elektronische Signatur- der Siegelerstellungseinheiten sind ebenfalls unverzüglich anzuzeigen.

Bitkom schlägt vor, § 5 inhaltlich anzupassen

Eine Differenzierung hinsichtlich der QSCD gilt es zu vermeiden. Die Anforderungen für eine QSCD werden im Anhang II der eIDAS VO dargestellt. Dort wird nur von „SIGNATURERSTELLUNGSEINHEIT“ gesprochen, somit gäbe es eigentlich keine Differenzierung in der Zertifizierung. Jedoch wird in Abschnitt 4 von Signaturkarten und Abschnitt 5 von Siegelkarten gesprochen. Aus unserer Sicht wäre der Verzicht auf eine Differenzierung wünschenswert, um Rechtssicherheit zu erzeugen, dass Differenzierungen der Anforderungen nicht existieren.

Eine Lösung hierfür könnte sein, von „Signaturerstellungseinheiten gemäß Anhang II der eIDAS VO“ zu sprechen.