Records Management

Theresa Vogt*

Die neue eIDAS-Verordnung – Chance und Herausforderung für die öffentliche Verwaltung in Deutschland

DOI 10.1515/iwp-2016-0011

Zusammenfassung: Die eIDAS-Verordnung bildet die neue EU-weite Rechtsgrundlage insbesondere für die Nutzung elektronischer Identifizierungsmittel und elektronischer Signaturen – zwei wesentliche Komponenten für die Realisierung eines sicheren und vertrauenswürdigen Records Managements. Durch den Anwendungsvorrang der Verordnung entsteht direkter Anpassungsbedarf bei relevanten nationalen Gesetzen. Die wichtigsten Neuerungen, die sich bei der Umsetzung für die öffentliche Verwaltung in Deutschland ergeben, werden in diesem Beitrag vorgestellt. Die Veränderungen werden anschließend in einer SWOT-Analyse untersucht und mögliche Anwendungsfälle aufgezeigt.

Deskriptoren: Öffentliche Verwaltung, Europa, Deutschland, Zertifizierung, eIDAS

The new eIDAS-regulation – Chance and challenge for the public administration in Germany

Abstract: The eIDAS-regulation is the new EU-wide legal basis particularly for the use of electronic identification means and electronic signatures – two significant components for the realization of a secure and trustworthy records management. National laws have to be alerted to fulfill the requirements of the regulation because of its primacy of application. The implementation of the regulation causes significant changes for the public administration in Germany. The most important ones will be presented in this article. Afterwards these changes will be examined using the method of a SWOT analysis and possible use cases will be identified.

Descriptors: Public administration, Europe, Germany, Certification, eIDAS

La nouveau règlement eIDAS – opportunité et défi pour l'administration publique en Allemagne

Résumé: La réglementation eIDAS est la nouvelle base juridique à l'échelon européen concernant l'utilisation des moyens d'identification électroniques et des signatures électroniques – deux éléments essentiels à la réalisation d'un records management sécurisée et fiable. La primauté du règlement nécessite une adaptation rapide de la législation nationale en la matière. Cet article présente les changements les plus importants pour l'administration publique en Allemagne à la suite de la transposition de la réglementation. L'auteur examine ensuite les modifications dans une analyse SWOT et présente les applications possibles.

Describeurs: Administration publique, Europe, Allemagne, Signature électronique, eIDAS

1 Ausgangslage

Bereits seit dem Jahr 2001 ist die Verwendung von elektronischen Signaturen im Signaturgesetz und der zugehörigen Signaturverordnung in Deutschland geregelt. Zudem werden Bundesbehörden durch das E-Government-Gesetz von 2013 dazu verpflichtet ihre Prozesse durchgängig elektronisch abzubilden. Dennoch hat sich der Einsatz von elektronischen Signaturen und elektronischen Identifizierungsmitteln in Deutschland – vor allem im Alltag der Bürger – nicht flächendeckend durchgesetzt. So bleibt z. B. der Einsatz der bereits 2010 eingeführten eID-Funktion des neuen Personalausweises hinter den Erwartungen zurück.¹

Dieses Defizit wird zudem im EU-weiten Kontext deutlich. Hier ist die Realisierung von sicheren und vertrauenswürdigen elektronischen Geschäftsprozessen kaum mög-

*Kontaktperson: Theresa Vogt, BearingPoint, Kurfürstendamm 207–208, 10719 Berlin, E-Mail: theresa.vogt@bearingpoint.com

¹ Vgl. Hoffman, Christian (2014).

lich. Gründe dafür sind u. a. unterschiedliche gesetzliche Grundlagen in den einzelnen Mitgliedstaaten sowie unterschiedliche technische Standards auf nationaler Ebene, was eine Interoperabilität zwischen den jeweiligen Systemen erschwert oder ausschließt.

Um eine grenzüberschreitende Interoperabilität und Harmonisierung auf dem Gebiet der elektronischen Geschäftsprozesse zu schaffen, gilt seit September 2014 die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen (eIDAS-Verordnung). Sie bildet die neue rechtliche Grundlage für die Nutzung elektronischer Identifizierungsmittel und sogenannter elektronischer Vertrauensdienste zu denen u. a. elektronische Signaturen zählen. Dadurch ergeben sich weitreichende rechtliche Veränderungen im Bereich der beweissicheren Kommunikation, die sich EU-weit sowohl in der Privatwirtschaft als auch im öffentlichen Sektor niederschlagen. Die wichtigsten Neuerungen für die öffentliche Verwaltung in Deutschland werden im Folgenden vorgestellt.

2 Änderung der rechtlich-fachlichen Rahmenbedingungen

Die eIDAS-Verordnung löst die Signaturrechtlinie aus dem Jahr 1999 ab und stellt durch ihren Anwendungsvorrang direkt geltendes Recht in allen EU-Mitgliedstaaten dar. Die elektronische Kommunikation innerhalb geschlossener Nutzerkreise, z. B. einer Behörde, ist von den Regelungen nicht betroffen. Die Vorgaben können auf nationaler Ebene detaillierter ausgestaltet werden. In diesem Zusammenhang ist es wichtig, dass die Vorschriften der eIDAS zügig in die deutsche Gesetzgebung einbezogen und die vorhandenen Regelungen angepasst werden. Nur so kann eine umfassende Rechtssicherheit für den Anwender geschaffen werden.² Betroffen von diesen Veränderungen sind vor allem das Signaturgesetz sowie die Signaturverordnung, das E-Government-Gesetz und das De-Mail-Gesetz hinsichtlich sicherer elektronischer Prozesse und Nachweisbarkeit elektronischer Dokumente.

Die eIDAS-Verordnung gliedert sich in die beiden Kapitel zur elektronischen Identifizierung und zu elektronischen Vertrauensdiensten. Einen Überblick über die enthaltenen Dienste gibt die Grafik in Abbildung 1.

Abbildung 1: Übersicht über Inhalte der eIDAS-Verordnung (Quelle: BearingPoint).

Im vorliegenden Artikel liegt der Fokus insbesondere auf der Betrachtung elektronischer Signaturen und Siegel im Kontext der Kommunikation zwischen Bürgern und Behörden sowie zwischen Behörden auf nationaler und europäischer Ebene.

Vertrauensdienste, zu denen elektronische Signaturen und Siegel zählen, werden von sogenannten Vertrauensdiensteanbietern (VDA) erbracht. Diese können sich nach einem standardisierten Verfahren zertifizieren lassen. Die Zertifizierung wird in jedem Mitgliedstaat von einer zuständigen nationalen Stelle durchgeführt. In Deutschland wird dies voraussichtlich die Bundesnetzagentur in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik sein. Nach erfolgreicher Zertifizierung, darf sich der VDA als qualifizierter Vertrauensdiensteanbieter bezeichnen und das eigens dafür entworfene europäische Vertrauenssiegel auf seiner Webseite anbringen. Zudem werden der qualifizierte VDA und die von ihm angebotenen Dienste in öffentlich zugänglichen sogenannten Vertrauenslisten aufgeführt. Qualifizierte Vertrauensdienste können nur von qualifizierten Vertrauensdiensteanbietern erbracht werden. Dies ist im Hinblick darauf, dass der qualifizierten elektronischen Signatur sowie dem qualifizierten elektronischen Siegel durch die eIDAS-Verordnung der höchste Beweiswert zugeschrieben wird, eine wichtige Tatsache, die von Anwendern berücksichtigt werden muss.

Ab 1. Juli 2016 gelten die Artikel der Verordnung, die sich speziell auf die Regelung der Vertrauensdienste beziehen. Ab diesem Zeitpunkt sind alle öffentlichen Stellen innerhalb der EU dazu verpflichtet qualifizierte elektronische Signaturen und Siegel von zertifizierten Vertrauensdiensteanbietern anzuerkennen – unabhängig davon, in welchem Mitgliedstaat der Diensteanbieter seinen Sitz

² Vgl. Roßnagel, Alexander (2015) S. 364.

Bedeutung der eIDAS-Verordnung am Beispiel der Bundesrepublik Deutschland

Abbildung 2: Relevanz der eIDAS-Verordnung (Quelle: BearingPoint).

hat. Gleiches gilt ab 18. September 2018 für die Anerkennung und Prüfung von elektronischen Identifizierungsmitteln.

Der qualifizierten elektronischen Signatur (QES) wird durch die Verordnung die gleiche Rechtswirkung wie einer handschriftlichen Unterschrift zugesprochen.³ Dies entspricht dem aktuellen Stand im Signaturgesetz, wonach die QES einer handschriftlichen Unterschrift gleichgesetzt werden kann.⁴ Weiterreichend ist die Festlegung, dass eine qualifizierte elektronische Signatur, die sich auf ein Zertifikat bezieht, welches in einem Mitgliedstaat ausgegeben wurde, in jedem anderen Mitgliedstaat ebenfalls als QES anerkannt werden muss. Somit haben QES beruhend auf einem Zertifikat eines qualifizierten VDA aus einem anderen EU-Land ebenfalls den Beweiswert einer handschriftlichen Unterschrift.⁵

Die Regelungen der Verordnung werden durch sogenannte Durchführungsrechtsakte ergänzt. Diese verwei-

sen auf technische Normen, welche wiederum von den Normungsorganisationen ETSI und CEN erarbeitet werden. Einigen dieser Durchführungsrechtsakte wird durch die eIDAS-Verordnung ein verpflichtender Charakter zugesprochen. So werden u. a. vier technische Formate für elektronische Signaturen und Siegel verbindlich festgelegt. Um eIDAS-konforme Signaturen zu erzeugen und deren Validierung zu ermöglichen, müssen sie im CAdES-, XAdES-, PAdES- oder ASiC-Format vorliegen.

Einen Überblick über die Relevanz der eIDAS-Verordnung im fachlich-rechtlichen Rahmen des Records Managements in Deutschland gibt die Grafik in Abbildung 2.

Grundsätzlich bleibt abzuwarten, wie die Vorschriften der eIDAS-Verordnung in künftigen Gerichtsverfahren von der Justiz interpretiert und in der Rechtsprechung konkret umgesetzt werden. Schlussendlich wird der Beweiswert elektronischer, eventuell langzeitgespeicherter Daten dadurch bestimmt, welche Wege und Maßnahmen die Beweisgegner finden, um die Glaubhaftigkeit der Daten zu widerlegen.⁶

³ Vgl. Verordnung (EU) Nr. 910/2014, Art. 25.

⁴ Vgl. Roßnagel, Alexander; Altenhain, Karsten (2013), S. 425–426.

⁵ Vgl. Verordnung (EU) Nr. 910/2014, Art. 25.

⁶ Vgl. Jandt, Silke (2015), S. 1209.

3 Wichtigste Neuerungen

Elektronisches Siegel

Eine der größten Veränderungen mit Folgen für den Handlungsspielraum einer deutschen Behörde bewirkt die Einführung des qualifizierten elektronischen Siegels als technisches Pendant zur qualifizierten elektronischen Signatur (QES). Durch das Inkrafttreten der Verordnung wird in Deutschland erstmals die Vergabe von Organisationszertifikaten für juristische Personen ermöglicht. Aktuell ist es gemäß dem Signaturgesetz (SigG) nur natürlichen Personen als Signaturschlüssel-Inhaber möglich, eine QES im Sinne des SigG zu erzeugen.⁷

Damit wird die rechtliche Schieflage bereinigt, bei der Verwaltungsmitarbeiter meist Bescheide der Behörde mit ihrer eigenen QES versehen, obwohl sie damit nicht ihren eigenen Willen belegen, sondern im Namen der Organisation handeln. Es liegt keine persönliche Willenserklärung des Signierenden vor, obwohl dies durch das Anbringen einer QES suggeriert wird.⁸ Das Nachweisen der Authentizität eines Behördenschreibens durch die QES eines Mitarbeiters ist eine organisatorische Behelfslösung. Diese muss bei der elektronischen Kommunikation genutzt werden, da es durch das SigG rechtlich keine Entsprechung der QES für juristische Personen gibt.

Ein qualifiziertes elektronisches Siegel im Sinne der eIDAS wird zwar als Beweis für die Unversehrtheit und der korrekten Herkunftsangabe der Daten eingesetzt. Es kann jedoch keine persönliche Willenserklärung entsprechend einer handschriftlichen Unterschrift ausdrücken, wie dies bei einer QES der Fall ist.⁹ Dennoch oder gerade weil das qualifizierte elektronische Siegel nicht die persönliche Willenserklärung einer natürlichen Person ausdrückt, bietet sich für dessen Nutzung im behördlichen Umfeld ein umfassendes Handlungspotential. Konkrete Einsatzmöglichkeiten werden später in diesem Artikel vorgestellt.

Serversignatur

Nach Art. 2 der Signaturrechtlinie muss der Signierende die Signaturerstellungsdaten unter seiner alleinigen Kontrolle halten.¹⁰ In der deutschen Umsetzung wird dies durch die Verpflichtung zur Verwendung einer Signaturkarte sichergestellt. Dagegen ergibt sich durch die neuen

Regelungen der eIDAS-Verordnung, dass private Signaturschlüssel nicht mehr ausschließlich auf der Signaturkarte sondern ebenso beim qualifizierten VDA selbst gespeichert und entsprechend verwaltet werden können.^{11, 12}

Die gedrosselten Anforderungen an die Signaturerstellung ermöglichen die Erzeugung von Serversignaturen, auch Remote- oder Fernsignaturen genannt. Bei dieser Variante der Signaturerzeugung sind die Signaturerstellungsdaten beim VDA gespeichert, die Signatur selbst wird direkt auf dem Server erzeugt und anschließend an den Anwender ausgegeben. Dieser Server muss durch ein Hardware-Sicherheitsmodul sicherstellen, dass der private Schlüssel nur für die berechtigte Person abrufbar ist. Von dieser Möglichkeit zur Erzeugung von Serversignaturen und deren Anerkennung als QES erhofft sich die Europäische Union eine erhöhte Verbreitung der Technologie, da es eine Vereinfachung des Verfahrens und damit einen wirtschaftlichen Vorteil bietet. Zusätzlich wird gefordert, dass die Erzeugung und Übertragung über einen sicheren Kommunikationskanal erfolgen und eine entsprechend sichere Systemumgebung eingesetzt wird. Um dies zu gewährleisten, können diese Dienste nur von qualifizierten VDA erbracht werden.¹³

Von besonderer Wichtigkeit bei jeglicher Art von Serversignaturen ist, dass die signierende Person sich über ein sicheres Verfahren identifiziert, bevor sie den privaten Schlüssel abrufen und eine QES erzeugen kann. Durch die eIDAS wird hierfür kein Sicherheitsniveau explizit vorgeschrieben. Kügler (2015, S. 23–25) verweist in seinem Vortrag auf die Formulierung wonach die Signaturerstellungsdaten „mit einem hohen Maß an Vertrauen“ unter der alleinigen Kontrolle des Signierenden stehen müssen.¹⁴

Haftungsregelung

Eine weitere Neuerung ergibt sich bei den Haftungsregelungen bezogen auf Vertrauensdiensteanbieter. Aktuell haftet der Zertifizierungsdiensteanbieter nach Signaturgesetz bzw. Signaturverordnung grundsätzlich für Schäden von Personen, wenn diese dadurch entstehen, dass der Anbieter die Vorschriften des Gesetzes bzw. der Verordnung missachtet. Durch die EU-Verordnung wird es künftig eine Unterscheidung zwischen qualifizierten und nicht-qualifizierten VDA bezüglich der Beweislast geben. Nimmt

⁷ Vgl. Korte, Ulrike; Hühnlein, Detlef (2006), S. 9.

⁸ Vgl. Sosna, Sabina (2014), S. 832.

⁹ Vgl. Verordnung (EU) Nr. 910/2014, Art. 35.

¹⁰ Vgl. Richtlinie 1999/93/EG, Art. 2.

¹¹ Vgl. Verordnung (EU) Nr. 910/2014, Art. 26.

¹² Vgl. Kügler, Dennis (2015b), S. 9.

¹³ Vgl. Verordnung (EU) Nr. 910/2014, Erwägungsgrund 52.

¹⁴ Vgl. Kügler, Dennis (2015a), S. 23–25.

eine Person Schaden und legt diese dem VDA zu Lasten, so muss nach Artikel 13 folgendermaßen vorgegangen werden:

- Bei einem qualifizierten VDA liegt die Beweislast beim Anbieter selbst. Es wird hier grundsätzlich von Fahrlässigkeit oder Vorsatz ausgegangen. Diese Annahme muss vom VDA widerlegt werden.
- Bei einem nichtqualifizierten VDA liegt die Beweislast bei der Person, die den Schaden anzeigt. Diese natürliche oder juristische Person muss dem nichtqualifizierten VDA ein fahrlässiges oder vorsätzliches Verhalten nachweisen.¹⁵

In der konkreten Umsetzung bedeutet es, dass der qualifizierte VDA stets den Beweis erbringen muss, dass er rechtmäßig im Sinne der Verordnung gehandelt hat. Damit steigt für Anbieter das Risiko aufgrund des angenommenen Vorsatzes bzw. der Fahrlässigkeit, in einem möglichen Gerichtsverfahren zu unterliegen. Um dieses Risiko zu minimieren, müssen die Anbieter großen Wert auf korrekte Durchführung der Dienste und eine umfassende Dokumentation legen. Für den vertrauenden Beteiligten dagegen wird, durch den erhöhten Druck zur fehlerfreien Durchführung der Dienstleistungen, das Vertrauen in die Anbieter gestärkt. Insofern kann die Verschiebung der Beweislast zu Lasten des VDA durchaus zu einer Steigerung der Zuverlässigkeit und damit der Sicherheit von Verdienstleistungen führen.

4 Anwendungsfälle im Records Management der öffentlichen Verwaltung

Ersetzendes Scannen

Auch weiterhin wird ein Teil des Schriftverkehrs über den postalischen Weg und in Papierform erfolgen. Die eIDAS-Verordnung enthält keine Angaben zum Scannen von Papierdokumenten. Folglich wird in diesem Fall das E-Government-Gesetz weiter Anwendung finden. Es besagt, dass das ersetzende Scannen und die anschließende Vernichtung der Originaldokumente bei der Einhaltung bestimmter Bedingungen zulässig sind. Diese Bedingungen werden in Deutschland von der technischen Richtlinie des Bundesamts für Sicherheit in der Informationstechnik (TR-

RESISCAN) vorgegeben. Demnach kann die technische Richtlinie weiterhin angewendet werden. Um den Beweiswert zu erhöhen, ist es laut TR-RESISCAN möglich eine QES an das gescannte Dokument anzubringen. Dies ist momentan sehr umständlich, da in der Praxis jeder signierende Mitarbeiter mit einer Signaturkarte und dem entsprechenden Lesegerät ausgestattet werden muss. Mit Inkrafttreten der eIDAS-Verordnung ist es nun denkbar, dass alle gescannten Dokumente mit einem fortgeschrittenen oder qualifizierten elektronischen Siegel versehen werden. Dieser Arbeitsvorgang ist damit unabhängig von bestimmten Mitarbeitern und die Behörde muss nur ein einziges Zertifikat beantragen, welches dann allen elektronischen Siegeln zugrunde liegt.

Stellvertretersignatur

Durch den Einsatz von Serversignaturen ergibt sich die Möglichkeit zur Vergabe von sogenannten Stellvertretersignaturen als neues Handlungsfeld für Behörden. Die Verwendung einer Stellvertretersignatur gestaltet sich wie folgt: Die zu vertretende Person muss sich bei der jeweiligen Behörde identifizieren und ihr eine Vertretungsvollmacht ausstellen. Daraufhin erzeugt die Behörde mit ihrem privaten Schlüssel ein qualifiziertes elektronisches Siegel und trägt dort ein, dass der Bürger durch das Siegel vertreten wird. Die Behörde bestätigt durch das besiegelte Dokument, dass der Bürger seine Willenserklärung ihr gegenüber deutlich gemacht hat und dass sie zur Besiegelung in Vertretung berechtigt ist. Die Identifizierung kann über ein elektronisches Formular in Verbindung mit einem elektronischen Identifizierungsmittel erfolgen. Wichtig ist die Festlegung klarer Haftungsbeschränkungen, um die Risiken für die anbietende öffentliche Stelle so gering wie möglich zu halten.¹⁶ Das Angebot von Stellvertretersignaturen bedeutet für den Bürger die Möglichkeit ohne eigene technische Infrastruktur und ohne die Inanspruchnahme der Dienste eines VDA, einen elektronischen Herkunftsnachweis zu erbringen. Die Behörde kann dadurch einen neuen Bürgerservice anbieten, der durch geringen Aufwand zu verwirklichen wäre.

¹⁵ Gesetz über Rahmenbedingungen für elektronische Signaturen, vgl. § 11 und vgl. Verordnung (EU) Nr. 910/2014, Art. 13.

¹⁶ Vgl. Kügler, Dennis (2015b), S. 14–18 und vgl. Kügler, Dennis (2015a), S. 27.

Mobile Signatur

Eine Variante der Serversignatur ist die Handy-Signatur, welche bereits in Österreich praktiziert wird. Hierbei dienen die Mobilnummer, ein Passwort und ein TAN-Code, welcher an den Signierenden gesendet wird und nur kurze Zeit gültig ist, als Identifizierungsdaten. Die Signaturerzeugung auf dem Server wird direkt über das mobile Gerät angestoßen. Die Ausgabe der mTAN muss dabei über ein unabhängiges System erfolgen, um etwaige Sicherheitslücken zu schließen und Betrug zu verhindern. Konkrete Anwendungsbeispiele finden sich in der österreichischen Verwaltung. Dort können Bürger zahlreiche E-Government-Angebote, wie z.B. eine Meldebestätigung oder einen Strafregisterauszug über die mobile Signatur nutzen. Der Entfall des Behördengangs und die für den Bürger praktische Erledigung von unterwegs hat dort zu einer erhöhten Verbreitung der mobilen Signatur und einer Lösung des typischen Henne-Ei-Problems der Signaturanwendungen geführt.¹⁷

5 SWOT-Analyse

Die Neuerungen, die sich bei den Prozessabläufen und den entsprechenden Rahmenbedingungen für die öffentliche Verwaltung ergeben, wurden in einer umfassenden SWOT-Analyse untersucht. Die wichtigsten Ergebnisse in Bezug auf elektronische Signaturen und Siegel werden im Folgenden wiedergegeben.

Stärken

Als eine große Stärke ist die Einführung eines EU-weiten Rechtsverständnisses in Bezug auf Vertrauensdienste zu nennen. Die unterschiedlichen nationalen Gesetzgebungen werden unter einem allgemeingültigen EU-Gesetz vereinheitlicht. Für Behörden bedeutet dies eine gesteigerte Rechtssicherheit bei der Verwendung solcher Dienste. Zudem werden die rechtlichen Vorgaben durch europaweite Standards spezifiziert, sodass die Harmonisierung auf der technischen Umsetzungsebene fortgeführt wird.

Durch eIDAS ist es möglich Signaturen mit deutlich geringerem Aufwand zu erzeugen. Statt lokale Signaturen mithilfe einer Signaturkarte zu erstellen, können nun Serversignaturen und mobile Signaturen genutzt werden. In diesem Zusammenhang ist die Einführung von Organisati-

onszertifikaten und damit die Möglichkeit elektronische Siegel zu erzeugen, ebenfalls als Stärke zu werten. Die Erzeugung und Validierung von elektronischen Siegeln können Behörden von qualifizierten VDA durchführen lassen. Diese sind zu regelmäßigen Konformitätsprüfungen verpflichtet und werden entsprechend mit dem EU-Vertrauensiegel gekennzeichnet. Für den Anwender bietet das einen eindeutigen und klaren Hinweis darauf, dass der Anbieter die erforderlichen Sicherheitsbedingungen erfüllt.

Schwächen

Zwar ist die Möglichkeit zur Erstellung von Serversignaturen grundsätzlich als eine Stärke zu werten. Die Tatsache, dass die Signaturerstellungsdaten nicht mehr unter der alleinigen Kontrolle des Signierenden auf einer Signaturkarte gespeichert sind, bringt jedoch eine Abschwächung beim Identifizierungsvorgang mit sich. Der Identifizierungsfaktor Besitz fällt weg, wenn die Signaturerstellungsdaten auf einem Server des VDA liegen. Dabei ist es zusätzlich von Nachteil, dass kein festgelegtes Sicherheitsniveau für die Identifizierung zur Erzeugung von Serversignaturen vorliegt.

Auch bei den Zertifikaten, die QES und qualifizierten elektronischen Siegeln zugrunde liegen, gibt es Schwächen. So werden in der eIDAS-Verordnung keinerlei Angaben zu deren Gültigkeitsdauer gemacht. In diesem Fall greifen die bereits vorhandenen nationalen Vorgaben. Die Möglichkeit zur Festlegung einer EU-weit einheitlichen Gültigkeit ist versäumt worden. Weiterhin fehlt den Organisationszertifikaten ein Berechtigungsnachweis. Hier wäre es sinnvoll gewesen ein Attribut vorzuschreiben, welches die natürlichen Personen benennt, die berechtigt sind das qualifizierte elektronische Siegel im Namen der Institution zu vergeben.

Chancen

Durch die EU-weite Vereinheitlichung und die vereinfachte Handhabung von Signaturen ist es absehbar, dass sich diese weiter verbreiten und vermehrt von Behörden und Bürgern verwendet werden. Gerade da sich die Nutzung in Deutschland noch nicht flächendeckend durchgesetzt hat, bietet sich hier ein hohes Potential diesen Markt auszubauen. Grundsätzlich wird nicht nur die Kommunikation zwischen Behörde und deutschem Bürger vereinfacht und beschleunigt, sondern auch die Kommunikation auf internationaler Ebene. Durch die verpflichtende grenzübergrei-

¹⁷ Vgl. Viola, Gerald (2012).

fende Anerkennung von Vertrauensdiensten ist es möglich EU-weite beweissichere Kommunikation zu betreiben. Im Gegensatz zum Papierdokument bietet dies eine Zeit- und Kosteneinsparung.

Es ist zudem zu erwarten, dass eine erhöhte Sicherheit durch standardisierte Signaturformate und die regelmäßige Überprüfung der qualifizierten VDA erreicht wird. Die einheitlichen Standards bezüglich der Formate und der Umsetzung der Vertrauensdienste bieten eine erhöhte EU-weite Interoperabilität. Sie ermöglicht eine intensivere Zusammenarbeit und einen reibungslosen Datenaustausch über Landesgrenzen hinweg.

Durch die einheitlichen Anforderungen, die an VDA gestellt werden, ist es für eine Behörde problemlos möglich die Dienste eines VDA aus einem anderen EU-Land zu nutzen. Dies bringt eine erhöhte Flexibilität mit sich. Es ist anzunehmen, dass sich die Marktlage durch die EU-weite Anerkennung von VDA zugunsten des Endanwenders und somit für Behörden verschieben wird. Dieser wird von günstigeren Konditionen bei der Inanspruchnahme von Vertrauensdiensten profitieren können.

Risiken

Speziell durch die Einführung des elektronischen Siegels und den teilweise zu vagen Regelungen diesbezüglich, ergibt sich Handlungsbedarf, um drohende Risiken abzuwenden. Das Siegel kann von mehreren Mitarbeitern vergeben werden. Diese sind jedoch nicht offiziell im Organisationszertifikat genannt, wie bereits bei den Schwächen dargelegt. Daher ist es für eine Behörde von größter Wichtigkeit, die Berechtigungen für die Siegelvergabe genau zu dokumentieren und dafür Sorge zu tragen, dass es Unbefugten nicht gelingt dennoch ein Siegel im Namen der Behörde zu erzeugen.

Zwar wird die Zertifizierung der qualifizierten VDA basierend auf den festgelegten Standards vorgenommen. Sie wird jedoch nicht EU-übergreifend, sondern national abgewickelt. Es ist daher nicht auszuschließen, dass Abweichungen bei den Ansprüchen an die VDA und deren Vertrauensdiensten auftreten. In Deutschland wurden die Regelungen zur elektronischen Signatur bisher sehr streng gehandhabt, was z. B. die Verpflichtung zur Verwendung einer Signaturkarte zeigt. Doch auch wenn in anderen EU-Ländern – im Rahmen der Durchführungsrechtsakte – möglicherweise geringere Anforderungen für eine Zertifizierung als qualifizierter VDA genügen, haben die Vertrauensdienste dennoch den entsprechenden Beweiswert nach eIDAS, und jede öffentliche Stelle ist verpflichtet diese anzuerkennen. Dadurch können Sicherheitsmängel bei

den entsprechenden Vertrauensdiensten entstehen, die das Betrugsrisiko erhöhen.

6 Fazit

Das erklärte Ziel der eIDAS-Verordnung ist es den digitalen europäischen Binnenmarkt zu stärken. Durch den einheitlichen Rechtsrahmen und die EU-weite Verwendung von Vertrauensdiensten und elektronischen Identifizierungsmitteln sind gute Voraussetzungen gegeben, um dieses Ziel zu erreichen. Grundsätzlich lässt sich für die öffentliche Verwaltung in Deutschland eine positive Bilanz aus der Betrachtung ziehen. Die neuen Regelungen vereinfachen Prozesse in vielen Fällen und erweitern die Möglichkeit zur beweissicheren, nationalen sowie internationalen Kommunikation.

Dennoch bleiben einige Fragen offen. Für deren Klärung muss die Veröffentlichung der entsprechenden Standards abgewartet werden. Das Ziel muss sein für den Anwender eine uneingeschränkte Rechtssicherheit zu schaffen. Nur so kann das Vertrauen der Bürger und Behörden in Vertrauensdienste und elektronische Identifizierungsmittel gewonnen werden. Das ist eine grundsätzliche Voraussetzung für den Einsatz der genannten Techniken im Behördenumfeld.

Dem Ziel eines digitalen europäischen Kommunikationsraums ist man durch die verbindliche eIDAS-Verordnung einen entscheidenden Schritt näher gekommen. Die vereinfachte Handhabung der Vertrauensdienste lässt einen Bedeutungsgewinn von elektronischen Signaturen und deren erhöhte Verbreitung unter den Bürgern erwarten. Neben der internationalen wird sich dadurch auch die innerdeutsche Kommunikation zwischen Bürgern und Behörden weiter in den digitalen Raum verschieben. Durch die eIDAS-Verordnung wird somit der Gedanke eines sicheren und vertrauenswürdigen Records Managements weitergeführt und zu dessen Umsetzung beigetragen.

Literatur

- Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) (16.05.2001): http://www.gesetze-im-inter.net.de/bundesrecht/sigg_2001/gesamt.pdf [14.12.2015].
- Hoffmann, Christian (2014). Warum die eID-Funktion des neuen Personalausweises (noch) keinen Erfolg hat. <http://www.government2020.de/blog/?p=1420> [14.12.2015].
- Jandt, Silke (2015). Beweissicherheit im elektronischen Rechtsverkehr: Folgen der europäischen Harmonisierung. In: Neue juristische Wochenschrift 17.1206–1211. ISSN 1613-4621.

- Korte, Ulrike; Hühnlein, Detlef (2006): Grundlagen der elektronischen Signatur. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/esig_pdf.pdf?__blob=publicationFile [14.12.2015].
- Kügler, Dennis (2015a). Remote Signatures und mögliche Angriffe. In: 25. Smartcard-Workshop. Tagungsband. Darmstadt, 4./5.02.2015: Fraunhofer-Verlag, S. 22–28. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/SmartCard_Workshop/Workshop_2015_Kuegler.pdf?__blob=publicationFile [14.12.2015].
- Kügler, Dennis (2015b). Remote Signatures und mögliche Angriffe. Vortrag. 25. Smartcard-Workshop. Darmstadt, 04.02.2015.
- Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (1999/93/EG). <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31999L0093&from=DE> [14.12.2015].
- Roßnagel, Alexander (2015). Der Anwendungsvorrang der eIDAS-Verordnung: Welche Regelungen des deutschen Rechts sind weiterhin für elektronische Signaturen anwendbar?. In: Multimedia und Recht 18, Nr.6. 359–364. ISSN 1434-596X.
- Roßnagel, Alexander; Altenhain, Karsten (2013). Beck'scher Kommentar zum Recht der Telemediendienste: Telemediengesetz, Jugendmedienschutz-Staatsvertrag (Auszug), Signaturgesetz, Signaturverordnung, Vorschriften zum elektronischen Rechts- und Geschäftsverkehr. München: Beck. ISBN 978-3-406-63211-2.
- Sosna, Sabina (2014): EU-weite elektronische Identifizierung und Nutzung von Vertrauensdiensten: eIDAS-Verordnung. – ein Überblick über die wichtigsten Inhalte und deren Konsequenzen für Unternehmen. In: Computer und Recht, 30, Nr.12. 825–832. ISSN 0179-1990.
- 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 (28.08.2014). <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&qid=1425317383295&from=DE> [14.12.2015].
- Viola, Gerald (2012): Mit dem Handy im Internet Anträge und Formulare unterschreiben: kostenlose eSignatur in Österreich. In: eGovernment Computing. <http://www.egovernment-computing.de/mit-dem-handy-im-internet-antraege-undformulare-unterschreiben-a-358782> [14.12.2015].

Theresa Vogt
 BearingPoint
 Kurfürstendamm 207–208
 10719 Berlin
theresa.vogt@bearingpoint.com

Theresa Vogt ist als Business Analyst beim Beratungsunternehmen BearingPoint tätig. Zu ihren fachlichen Schwerpunkten zählen elektronische Signaturen, beweiserhaltende Langzeitspeicherung und digitale Archivierung. Sie hat ihr Masterstudium im Fach Informationswissenschaften an der Fachhochschule Potsdam mit einer Arbeit zum Thema „Auswirkungen der eIDAS-Verordnung auf das Records Management der öffentlichen Verwaltung in Deutschland“ abgeschlossen. Ihr Bachelorstudium im Fach Bibliothekswesen absolvierte sie von 2010 bis 2013 an der Fachhochschule Köln.