White Paper des Forums elektronische Vertrauensdienste

Sichere (elektronische) Dokumente

Neue Rahmenbedingungen durch die europäische eIDAS-Verordnung

DIHK Deutscher Industrie- und Handelskammertag

Inhaltsverzeichnis

Management Summary ... 3

I. Einsatzszenarien ... 5

1. Ein Blick in die Zukunft ... 5
2. Von „Archivierung" bis „Zeugnis" – Einsatzszenarien für das elektronische Siegel ... 6
   - i. Elektronischer Eingangsstempel ... 6
   - ii. E-Mail-Signatur ... 7
   - iii. Elektronische Rechnungen ... 7
   - iv. Zeugnisse ... 7
   - v. Beglaubigungen ... 8
   - vi. Softwareschutz ... 8
   - vii. Behördenbescheide ... 9
   - viii. Kontoauszüge ... 9
   - ix. Steuerbescheinigungen nach §45a EStG ... 9
   - x. Gehaltsnachweise für Kreditanträge ... 10
   - xi. Archivierung ... 10
3. Wer könnte das Siegel nutzen – und wer davon profitieren? ... 11

II. Der Rahmen: eIDAS Verordnung ... 12

III. Elektronische Siegel und elektronische Signatur – die perfekte Ergänzung ... 15

IV. Vertrauensdienste nach eIDAS ... 17

V. Technische Umsetzung und Standards (ETSI/CEN) ... 19

VI. Erfolgsfaktoren ... 21

Management Summary

Elektronische Siegel für juristische Personen fördern effizientes E-Government und intelligente elektronische Workflows. Wenn eine Behörde oder eine Firma ein Dokument elektronisch siegelt, so ist sie als Absender des Dokuments dauerhaft erkennbar und schützt die Daten gleichzeitig vor unbemerkten Veränderungen. Diese Siegel funktionieren also ähnlich wie eine elektronische Signatur, beziehen sich aber immer auf eine juristische und nicht auf eine natürliche Person.

Elektronische Siegel bieten große Chancen für Behörden, Verbände und Unternehmen sowie andere Organisationen. Zum einen ermöglichen die elektronischen Siegel erstmals elektronische Abläufe für Verfahren, die zuvor noch an die Papierform gebunden waren, etwa den Versand von Behördenbescheiden. Zum anderen können sie Prozesse, die bis dato ungesichert und mit hohem Betrugspotenzial durchgeführt wurden, auf eine verlässliche Basis stellen. Hierzu gehören zum Beispiel der elektronische Versand von Bewerbungsunterlagen oder der geschäftliche E-Mail-Verkehr.

Den gesetzlichen Rahmen für die elektronischen Siegel schafft die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, nach dem englischen Titel kurz als „eIDAS-Verordnung" bezeichnet. Wesentlicher Stichtag für die Gültigkeit dieser Verordnung in Deutschland ist der 01.07.2016. Die eIDAS-Verordnung differenziert zwei Siegelniveaus: die fortgeschrittenen und die höherwertigen qualifizierten elektronischen Siegel. Konkrete Einsatzszenarien regelt die eIDAS-Verordnung allerdings nicht, diese bleiben eine Angelegenheit der jeweiligen EU-Mitgliedstaaten.

Als sinnvolle Ergänzungen, nicht als Konkurrenz zueinander, sind elektronische Signaturen und elektronische Siegel anzusehen. Allein die qualifizierten elektronischen Signaturen können nach derzeitiger Rechtslage eine rechtlich geforderte handschriftliche Unterschrift adäquat elektronisch ersetzen. Dieses Formerfordernis erfüllen die (qualifizierten) elektronischen Siegel nicht. Ihnen schreibt die eIDAS-Verordnung aber eine hohe Beweiswertvermutung in Bezug auf die Unversehrtheit und Zurechenbarkeit von Dokumenten zu.

Die technischen Systeme zur Siegelerzeugung werden den Anwendungsbetreibern von einem Vertrauensdiensteanbieter (VDA) gegen Entgelt bereitgestellt. Qualifizierte VDAs werden kontinuierlich in einem sehr aufwändigen Verfahren hinsichtlich der nachgewiesenen Umsetzung aller Sicherheitsvorgaben von unabhängigen Auditoren überprüft. Der Vertrauensstatus ist weltweit über eine Vertrauensliste und ein Gütesiegel nachprüfbar.

Damit die elektronischen Siegel sich erfolgreich im deutschen Behörden- und Geschäftsalltag etablieren, reichen die bereits geschaffenen gesetzlichen, organisatorischen und technischen Voraussetzungen allein nicht aus. Die Vertrauensdiensteanbieter und Anwendungsbetreiber müssen die Handhabung und den Preis der Siegel attraktiv gestalten. Darüber hinaus ist vor allem der deutsche Gesetzgeber gefragt, in Einzelgesetzen konkrete Anwendungsszenarien für die elektronischen Siegel – gerade im öffentlichen Bereich – zu ermöglichen. Dann können die erheblichen Potenziale des elektronischen Siegels vollständig genutzt werden.

I. Einsatzszenarien

1. Ein Blick in die Zukunft

Ein sonniger Samstagmorgen im Mai 2020. Philipp Schneider, 28 Jahre alt, Wirtschaftsingenieur, sitzt zuhause an seinem Schreibtisch in Berlin und hat gute Laune. Gerade hat er online eine interessante Stellenanzeige eines Unternehmens in Marseille entdeckt, die wie angegossen auf sein Profil passt. Südfrankreich, ein Traum! Um ein gutes Bewerbungsschreiben zu verfassen und in lupenreines Französisch zu übersetzen, braucht er jetzt natürlich ein bisschen Zeit. Seine Bewerbungsunterlagen hat er aber zum Glück schnell zusammen: Die Bachelor-Urkunde von der Uni München, das Masterzeugnis von der TU Berlin, das Zwischenzeugnis von seinem aktuellen Arbeitgeber. Alle diese Unterlagen hat er in elektronischer Form auch in Englisch, und das Beste ist: An der Echtheit seiner Zeugnisse kann keiner zweifeln. Denn sowohl seine beiden Unis als auch das Unternehmen, bei dem er derzeit beschäftigt ist, haben ihr elektronisches Siegel auf den Zeugnisdateien angebracht. So kann das Unternehmen in Marseille sicher sein, dass Philipp Schneiders sehr gute Zeugnisse auch tatsächlich seinen Examina und Arbeitsleistungen entsprechen. Denn aufgrund des EU-weiten Standards und eines einheitlichen Erkennungslogos sind die elektronischen Siegel auch in Frankreich bekannt und anerkannt. Dass die Zeugnisse tatsächlich von den Unis München und Berlin und von seinem aktuellen Arbeitgeber ausgestellt wurden, lässt sich von Marseille aus also ebenso einfach per Mausklick verifizieren wie die Tatsache, dass die Zeugnisdaten nicht manipuliert wurden. Sie sind damit deutlich vertrauenswürdiger als eine Kopie auf Papier – gerade auch für einen Empfänger außerhalb Deutschlands.

Zwei Wochen später: Philipp Schneider hat seine Bewerbung nach Marseille geschickt und von dort schnell eine Einladung zu einem Telefon-Interview bekommen. Das ist hervorragend verlaufen, Philipp Schneider hat jetzt noch größere Lust auf die Stelle in Südfrankreich. Und bekommt schließlich, ein paar Tage nach dem Telefonat, vom Personalbüro des Unternehmens in Marseille auf elektronischem Wege sein persönliches Jobangebot – versehen mit dem elektronischen Siegel des Unternehmens, damit auch er sich auf die Zusage verlassen kann.

2. Von „Archivierung“ bis „Zeugnis“ – Einsatzszenarien für das elektronische Siegel

Woran erkennt man die Echtheit einer behördlichen Urkunde oder eines Firmenschreibens? Wenn die Dokumente auf Papier vorliegen, dann ergibt sich die Echtheit oft aus dem Briefkopf, aus einem behördlichen Siegel, aus dem Briefumschlag, in dem sie enthalten sind – oder bei Urkunden sogar daraus, dass sie feierlich persönlich überreicht werden. Doch immer mehr Schreiben werden elektronisch ausgetauscht, auch Urkunden bilden da keine Ausnahme. Hier schafft das EU-konforme elektronische Siegel eine komfortable und zuverlässige Möglichkeit, um elektronische Dokumente einem schnellen Echtheits-Check zu unterziehen. Im Ergebnis kann man sich darauf verlassen,

- dass tatsächlich diejenige Organisation (Firma, Behörde, Universität, ...) das Dokument ausgestellt hat, die als Absender genannt ist;
- dass die Daten des Dokumentes hundertprozentig dem Original entsprechen, also nicht im Nachhinein verfälscht worden sind.

Diese doppelte Echtheitsgarantie, verbunden mit einem EU-weit gültigen Rechtsrahmen für elektronische Siegel, erlaubt ganz neue Szenarien für den elektronischen Dokumentenaustausch, die zuvor nicht realisierbar waren. Wann immer per gesetzlicher Anforderung oder per Fomularfeld ein Behördensiegel oder ein Firmenstempel gefordert ist, steht dies jetzt auch elektronisch zur Verfügung und ermöglicht damit medienbruchfreie elektronische Abläufe. Hier einige vorstellbare Anwendungsbeispiele:

i. Elektronischer Eingangsstempel

Viele Unternehmen und Behörden müssen eingehende Post kennzeichnen. Von Sozialversicherungen wird beispielsweise explizit verlangt, erhaltene Faxe qualifiziert elektronisch zu signieren. Hier wäre das Siegel genau das Mittel der Wahl. Es ist zum einem für den Masseneinsatz geeignet, etwa im Rechenzentrum, und spiegelt auch die richtige Authentizität wieder, nämlich die der Sozialversicherung, anstelle der des Sachbearbeiters. Selbstverständlich kann dieser elektronische Eingangsstempel auch für andere Formate, wie zum Beispiel E-Mail, Verwendung finden und dies nicht nur bei Sozialversicherungen, sondern auch bei Behörden, der Justiz und Unternehmen.

ii. E-Mail-Signatur

Jeder kennt die Funktion von „Black Lists“ im E-Mail-Programm, bei denen verdächtige Absenderadressen direkt dem Spam-Filter übergeben werden. Aber wie wäre es zur Abwechslung mal mit einer „White List“? E-Mail-Empfänger könnten serverseitig das Entgegennahmeverhalten steuern, indem sie mit elektronischen Siegeln versehenen E-Mails einen besonderen Vertrauensstatus zuordnen. Wenn also dienstliche und geschäftliche E-Mails vertrauenswürdiger gestaltet werden sollen, wäre dafür ein elektronisches Siegel hervorragend geeignet, vor allem wenn die Einbindung beim Absender und die Überprüfung beim Empfänger automatisiert ablaufen.

iii. Elektronische Rechnungen

Immer mehr Rechnungen gehen elektronisch beim Absender heraus – doch wenn der Empfänger sie zum Vorsteuerabzug geltend machen will, muss er die Echtheit und Korrektheit der Rechnungsdaten belegen können. Früher hat der Gesetzgeber dazu die qualifizierte elektronische Signatur auf Rechnungen vorgeschrieben, die vielen Nutzern für diesen Zweck überdimensioniert vorkam. Mittlerweile sind nur noch etwas vage „innerbetriebliche Kontrollverfahren“ zur Sicherstellung von Authentizität und Integrität der Rechnungsdaten gefordert. Diese Anforderung ließe sich mit elektronischen Siegeln perfekt erfüllen. Die Unternehmen könnten sowohl die Rechnungsdaten selbst als auch die E-Mails, mit denen sie die Rechnungen verschicken, elektronisch siegeln. Rechnungsformate wie ZUGFerd, die auf elektronische Übermittlung und Weiterverarbeitung von Rechnungsdaten setzen, könnten davon sehr profitieren.

iv. Zeugnisse

Ein in festlichem Rahmen überreichtes oder gar eingerahmtes und aufgehängtes Zeugnis mag manchen mit Stolz erfüllen – aber wenn man bei einem neuen Arbeitgeber seine bisherigen Qualifikationen darlegen möchte, kommt es vor allem auf einfache und sichere Übermittlungsmöglichkeiten an. Frisierte Zeugnisse bilden in der täglichen Bewerbungspraxis leider keine Seltenheit. Es gibt sogar Internet-Portale, bei denen man ein Zeugnis seiner Wahl bestellen kann – ohne eigene Leistung, dafür freilich gegen einen gewissen Obolus. Gegen solche Betrügereien hilft ein elektronisches Siegel der Schule, der Universität oder der Firma, die das Zeugnis ausgestellt hat und damit die Echtheit verbürgt. Auch Ausbildungszeugnisse, die die Industrie- und Handelskammern oder die Handwerkskammern ausstellen, könnten in elektronischer Form mit einem Siegel der Kammer abgesichert werden. Auf Sachkundenachweise, die die IHK ausstellt, ließe sich das Verfahren ebenfalls anwenden.

Nicht nur bei Bewerbungsverfahren könnten solche elektronisch gesiegelten Zeugnisse die Vertrauenswürdigkeit erhöhen. Es wäre auch zum Beispiel möglich, Zulassungsverfahren an Hochschulen komplett elektronisch abzuwickeln. Umständliche Parallelverfahren, wie zum Beispiel nach der Online-Einschreibung noch ein Abiturzeugnis beglaubigen zu lassen und in Papier nachzureichen, würden dann der Vergangenheit angehören. Denn die amtliche Beglaubigung ist im elektronisch gesiegelten Zeugnis quasi immer schon integriert.

v. Beglaubigungen

Zu den besonders intensiv nachgefragten Behördendienstleistungen zählt die Beglaubigung von Dokumenten. Es geht darum, von einem schon existierenden amtlichen Dokument, zum Beispiel einem Zeugnis oder einer Geburtsurkunde, eine Abschrift zu erstellen – dies aber nicht mit einer schlichten Kopie, sondern mit dem verbindlichen Nachweis, dass die Zweitschrift auch wirklich mit dem Original übereinstimmt. Solche amtlichen Beglaubigungen können Behörden übernehmen – teilweise für Urkunden, die sie selbst ausgestellt haben, teilweise auch für Urkunden, die von anderen Stellen stammen. Es versteht sich von selbst, dass im digitalen Zeitalter solche Beglaubigungen immer häufiger auch in elektronischer Form nachgefragt werden. Ein maßgeschneiderter Anwendungsfall für das elektronische Amtssiegel – der allerdings voraussetzt, dass das Verwaltungsverfahrensgesetz und das Sozialgesetzbuch dies auch zulassen (siehe Kapitel VI: Erfolgsfaktoren).

vi. Softwareschutz

Der Einsatz vertrauenswürdiger Software ist aufgrund der umfassenden Bedrohungen durch Schad-, Ausspäh- und Erpressungsprogrammen wichtiger denn je. Bereits heute gibt es zum Schutz von Softwareprogrammen Prüfmechanismen, die auf elektronischen Signaturen beruhen, jedoch nur applikationsabhängig verfügbar sind.

Zukünftig können auch Siegel zum Schutz vor bösartiger Manipulation eingesetzt werden. Vor Installation oder Ausführung der Software wird mittels des Siegels der Herausgeber identifiziert und nach erfolgreicher Prüfung kann dann die Software genutzt werden. Zusätzlich können Siegel auch zur Serverauthentifizierung (z. B. Maschine-Maschine-Kommunikation) wie auch zur Device-Authentisierung oder zum asynchronen Integritätsnachweis eingesetzt werden.

vii. Behördenbescheide

Viele Bürger sind in einer Behördenmitteilung schon einmal über den merkwürdigen Satz gestolpert: „Dieses Schreiben wurde maschinell erstellt und ist daher ohne Unterschrift gültig." Diese Formulierung bezieht sich auf § 37 des Verwaltungsverfahrensgesetzes, in dem die (schriftliche, mündliche oder elektronische) Form für Verwaltungsakte definiert wird. Mit elektronischem Siegel könnten sehr viel mehr behördliche Bescheide elektronisch verschickt werden als bisher. Denn zu einer der wichtigsten Maßgaben von Verwaltungsakten gehört es, dass sie die ausstellende Behörde erkennen lassen müssen. So lässt sich für die öffentlichen Verwaltungen insbesondere bei Massenverfahren wie Steuer- oder Rentenbescheiden eine Menge Geld einsparen.

viii. Kontoauszüge

Online-Banking erfreut sich immer größerer Beliebtheit – doch es gibt derzeit einen gravierenden Medienbruch. Eine riesige Menge von Kontoauszügen wird derzeit noch auf Papier ausgestellt, weil die Finanzbehörden sie nur in dieser Form anerkennen. Buchführungspflichtige Kunden könnten ebenso wie Kreditinstitute erheblich davon profitieren, wenn diese Kontoauszüge stattdessen elektronisch übermittelt und zum Beispiel im elektronischen Postfach des Kunden hinterlegt werden könnten. Um die steuerrechtliche Anforderung der Unveränderbarkeit zu gewährleisten, wäre das elektronische Siegel des ausstellenden Kreditinstituts perfekt geeignet.

ix. Steuerbescheinigungen nach §45a EStG

Auch Steuerbescheinigungen über Kapitalerträge müssen dem buchführungspflichtigen Steuerpflichtigen gemäß §45a Einkommensteuergesetz vom Kreditinstitut in Papierform zugestellt werden. Denn die Bescheinigung dient als Nachweis zur Anrechnung der gezahlten Kapitalertragssteuer. Um Missbrauch zu vermeiden, galt bisher nur die Papierform als sicher. Das Elektronische Siegel kann auch in dem Fall der Steuerbescheinigungen die Echtheit der Herkunft und die Unversehrtheit des Ursprungs gewährleisten. Durch eine entsprechende Anpassung des §45 EStG könnten Unternehmen dann entsprechend gesiegelte Steuerbescheinigungen über das ELSTER-Verfahren bei ihrem Finanzamt einreichen und somit auch zur Vereinfachung der Prozesse innerhalb der Finanzverwaltung beitragen.

x. Gehaltsnachweise für Kreditanträge

Ähnlich wie bei Zeugnissen muss sich ein Kreditinstitut bei Gehaltsnachweisen, die im Rahmen eines Kreditantrags vorgelegt werden, auf die Echtheit der Angaben des Kreditnehmers verlassen können. Leider besteht dabei für einige potenzielle Kreditnehmer die Versuchung, ihre Gehaltsnachweise zu beschönigen. Wenn Gehaltsnachweise beispielsweise als einfaches PDF vom Arbeitgeber zur Verfügung gestellt werden, bedarf es keiner außerordentlichen Expertise, um Änderungen an dem Dokument vorzunehmen. Um niemanden in Versuchung zu führen, wären elektronisch gesiegelte Gehaltsnachweise das ideale Instrument – für das Kreditinstitut, aber auch für den Angestellten, der einen verlässlichen Nachweis über seine Einkommenssituation erhält.

xi. Archivierung

Papierarchive brauchen eine Menge Platz und sind aufwändig zu verwalten. Immer mehr Papierdokumente, für die eine Aufbewahrungspflicht besteht, werden daher in elektronische Archive überführt – also eingescannt und nach einem bestimmten System abgelegt. Die Krux dabei: Wer garantiert für den Beweiswerterhalt? Wer steht dafür gerade, dass die Daten beim Scannen komplett und inhaltlich unverändert erfasst werden und auch auf Dauer vor Manipulationen geschützt sind? Die elektronischen Siegel können helfen, diese Sicherheitskriterien zu gewährleisten. Hier greift neben der Absenderechtheit vor allem die Integritätsschutz-Funktion der elektronischen Siegel, weil die gesiegelten Archivdaten nicht mehr unbemerkt verändert werden können.

Schon heute praktizieren viele Unternehmen und Behörden dieses „ersetzende Scannen" und sichern die Integrität der elektronisch transformierten Daten mit der qualifizierten Signatur oder mit anderen Integritätssicherungsmaßnahmen gemäß der TR-RESISCAN des Bundesamts für Sicherheit in der Informationstechnik (BSI) ab. Hier bietet das elektronische Siegel zukünftig eine komfortable Lösung, insbesondere beim dezentralen Scannen.

3. Wer könnte das Siegel nutzen – und wer davon profitieren?

Anhand der möglichen Anwendungsszenarien lässt sich klar ersehen, welche Organisationen ein elektronisches Siegel führen könnten: Allen voran kommen hier die „siegelführenden Stellen" (mit Ausnahme der Notare) in Frage, also Ämter und Behörden. Potenzielle Anwender wären dann also die zahlreichen kommunalen Behörden wie Standesämter und Ausländerbehörden, außerdem Landesbehörden einschließlich der Finanzämter, Bundesbehörden, Polizei, Gerichte, Schulen, Hochschulen, Kirchen und nicht zuletzt die Organisation der Industrie- und Handelskammern, die ja auch mit hoheitlichen Aufgaben betraut ist. Sie könnten dank elektronischer Siegel manchen Papiervorgang durch einen effizienten elektronischen Workflow ersetzen.

Über den behördlichen Einsatz hinaus kann man das elektronische Siegel aber auch als elektronisches Pendant zum Firmenstempel sehen. Als Anwender kämen dann alle privaten Wirtschaftsunternehmen und Organisationen in Betracht, die für elektronische Nachrichten die Absender- und Dokumentenechtheit garantieren wollen oder die sich im Internet sicher und verlässlich zu erkennen geben wollen. Hier gilt es ein echtes Manko zu füllen – denn für Unternehmen gibt es momentan kein einheitliches, allgemein anerkanntes Verfahren, um im Internet sicher ihre Identität nachzuweisen. Hier wäre das elektronische Siegel also so etwas wie ein „Personalausweis für Unternehmen" im Internet – angesichts von immer mehr Identitätsdiebstahl in der virtuellen Welt sicher eine interessante Sache.

II. Der Rahmen: eIDAS Verordnung

Der Impuls für die elektronischen Siegel kommt von der Europäischen Union. Unternehmen, Bürger und die öffentliche Verwaltung sollen innerhalb der EU sicher und vertrauenswürdig elektronisch kommunizieren können – das ist das Ziel der „Verordnung für elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt" der EU vom 17.09.2014 (in englischer Sprache „Regulation on electronic Identification and trust Services", daher die Abkürzung eIDAS-Verordnung).

Bis zum Inkrafttreten der eIDAS-Verordnung, das ist die nüchterne Bilanz, gab es innerhalb der EU keine einheitlichen Systeme für sichere elektronische Transaktionen und elektronische Identitätsmerkmale – und das, obwohl der Binnenmarkt auf einheitliche, rechtlich anerkannte Kommunikationswege im Online-Verkehr angewiesen ist und 13 Millionen EU-Bürger in einem anderen EU-Land arbeiten. Ziel der eIDAS-Verordnung war es daher, einen digitalen Binnenmarkt zu realisieren. Die wichtigsten Bausteine dafür:

- Einheitliche Regeln für die Anerkennung der verschiedenen elektronischen Identifizierungssysteme in Europa.
- Abgestimmte Formate für Signaturen, Siegel, Zeitstempel, Website-Zertifikate, E-Mail-Zustelldienste und Archivdienste.
- Einheitliche Vorgaben für die entsprechenden Vertrauensdiensteanbieter (VDA).
- Gegenseitige Anerkennung der elektronischen Identifizierungsmittel und der VDA-Leistungen.
- Festlegung eines Rechtsrahmens für betroffene Dienste.

Ein gutes Zeichen für den Binnenmarkt: Vertrauenswürdige EU-Online-Services dürfen sich mit diesem Siegel schmücken. Internetnutzer können an dem Logo erkennen, dass der Dienst vertrauenswürdig ist.

Die eIDAS-Verordnung beschränkt sich nicht darauf, bestehende Systeme zu vereinheitlichen. Mit dem elektronischen Siegel schafft sie für den deutschen Markt auch ein neues Produkt, das früher überhaupt nicht definiert war. Was hat man sich nun unter diesem elektronischen Siegel genau vorzustellen? Die eIDAS-Verordnung macht dazu folgende Aussagen:

- Elektronische Siegel sind Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit zu prüfen (Art. 3 Abs. 25 eIDAS-Verordnung).

  Das bedeutet: Das Siegel verschmilzt mit den elektronischen Daten, die gesiegelt werden, zu einer Einheit – ähnlich wie Siegellack, der auf einer Urkunde aufgetragen wird.

- Es sind zwei Niveaus von elektronischen Siegeln zu unterscheiden (Art. 3 Abs. 26 und 27 eIDAS-Verordnung): Fortgeschrittene elektronische Siegel und – höherwertige – qualifizierte elektronische Siegel.

  Das bedeutet: Je nach Sicherheitsanforderung ist das passende Siegelniveau auszuwählen. Das qualifizierte Siegel ist möglicherweise etwas aufwändiger, dafür sicherer.

- Fortgeschrittene elektronische Siegel erfüllen folgende Anforderungen:
  - Sie sind eindeutig dem Siegelersteller (also einer Behörde oder Firma) zugeordnet.
  - Sie ermöglichen die Identifizierung des Siegelerstellers.
  - Sie werden unter Verwendung von elektronischen Siegelerstellungsdaten erstellt, die der Siegelersteller mit einem hohen Maß an Vertrauen unter seiner Kontrolle halten kann.
  - Sie sind mit den Daten, auf die sie sich beziehen, so verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

  Das bedeutet: Anhand des Siegels kann man eindeutig erkennen, welche Behörde oder Firma dahintersteckt. Das Siegel ist also für jedermann öffentlich überprüfbar – aber selbstverständlich soll nur die Behörde oder Firma selbst das Siegel aktiv anbringen können. Gleichzeitig dient das Siegel als Fälschungsschutz für Urkunden oder Dokumente.

- Qualifizierte elektronische Siegel erfüllen folgende Anforderungen:

  - Es gelten dieselben Anforderungen wie beim fortgeschrittenen Siegel und zusätzlich:
  - Sie werden von einer qualifizierten elektronischen Siegelerstellungseinheit erstellt.
  - Sie beruhen auf einem qualifizierten Zertifikat für elektronische Siegel.

  Das bedeutet: Zusätzlich zu allen Merkmalen, die für fortgeschrittene Siegel gelten, dürfen beim qualifizierten Siegel nur besonders sichere Produkte und Prozesse zum Einsatz kommen, die eigens von einer zuständigen Überwachungsbehörde kontrolliert werden. Dafür können qualifizierte Siegel als besonders vertrauenswürdig gelten.

Keine Frage, die Aussagen der eIDAS-Verordnung bleiben noch etwas abstrakt und sind nach und nach mit Leben zu füllen. Ihre Wirkung wird sie aber auf jeden Fall entfalten. Denn die Tragweite ergibt sich durch den Charakter der Verordnung: Sie ist unmittelbar geltendes Recht in allen EU-Staaten, im Gegensatz zu einer Richtlinie gibt es so gut wie keine Umsetzungsspielräume. Der wichtigste Stichtag zum Inkrafttreten der eIDAS-Verordnung ist der 01.07.2016, und es greift der sogenannte Anwendungsvorrang: Gerichte und Behörden müssen das EU-Recht anwenden, wenn dieses mit dem deutschen Recht kollidiert. Das deutsche Signaturgesetz und die Signaturverordnung gelten übergangsweise nur insofern weiter, wie die EU-Verordnung nicht ausdrücklich etwas anderes bestimmt. Im angekündigten Vertrauensdienste-Gesetz passt der Gesetzgeber die deutsche Rechtslage an die eIDAS-Verordnung an.

III. Elektronische Siegel und elektronische Signatur – die perfekte Ergänzung

Nicht nur Experten erkennen schnell die vielen Parallelen zwischen elektronischen Siegeln und elektronischen Signaturen: Beide Produkte sichern die Echtheit des Absenders und die Integrität der übertragenen Daten und stützen sich dafür auf ganz ähnliche technische Abläufe. Außerdem setzen beide Verfahren auf geprüfte Vertrauensdiensteanbieter als Beglaubigungsinstanzen, welche die vertrauenswürdigen Zertifikate für Siegel bzw. Signaturersteller ausstellen. Trotz dieser wichtigen Gemeinsamkeiten existieren aber auch grundlegende Unterschiede zwischen organisationsbezogenen elektronischen Siegeln einerseits und an Menschen gebundenen elektronischen Signaturen andererseits:

- Die elektronische Signatur ersetzt die handschriftliche Unterschrift eines Menschen. Das elektronische Siegel bildet das Pendant zum Behördensiegel oder zum Firmenstempel.

- Die elektronische Signatur beruht immer auf einem Zertifikat, das einen Menschen identifiziert. Beim elektronischen Siegel verweist das Zertifikat dagegen auf eine Organisation.

- Die elektronische Signatur macht elektronische Daten zu einer persönlichen Willenserklärung. Man weiß genau, wer dahinter steckt, man hat einen persönlichen Ansprechpartner. Dementsprechend eignet sich die Signatur für individuelle Erklärungen, Anträge oder Formulare. Elektronische Siegel stellen hingegen sicher, dass die Daten von einer bestimmten Institution stammen (oder aber sie belegen einfach die Echtheit eines Dokuments, das eine Informationsfunktion erfüllt – siehe die oben genannten Anwendungsbeispiele).

Diese wichtigen Abgrenzungen zwischen elektronischen Siegeln und elektronischen Signaturen werden auch in der eIDAS-Verordnung deutlich, wenngleich diese nur einen Rahmen für die sichere elektronische Kommunikation schafft und nicht in die nationalen Formvorschriften eingreift (Artikel 2 Absatz 3). Es bleibt also allein in der Entscheidungskompetenz des jeweiligen Mitgliedsstaates, ob ein bestimmter Verwaltungsvorgang oder eine Rechtshandlung schriftlich, elektronisch oder mündlich vorgenommen werden kann.

Juristisch ausgedrückt bedeutet das, dass materiell-rechtliche und verfahrensrechtliche Formerfordernisse der Mitgliedstaaten ihre Gültigkeit behalten. Einfacher formuliert, schreibt die eIDAS-Verordnung den Nationalstaaten also nicht vor, ob zum Beispiel eine Gewerbeanmeldung schriftlich eingereicht werden muss oder nicht. Sobald ein Nationalstaat allerdings die Entscheidung für die Schriftform getroffen hat, sieht die eIDAS-Verordnung in Artikel 25 Absatz 2 vor, dass dann auch die qualifizierte elektronische Signatur als Ersatz für die handschriftliche Unterschrift anerkannt werden muss.

Welche Aussagen macht die eIDAS-Verordnung aber nun zur Anerkennung elektronischer Siegel? Die gleiche Rechtswirkung wie eine handschriftliche Unterschrift spricht sie jedenfalls einzig und allein der qualifizierten elektronischen Signatur zu, das gesetzliche Schriftformerfordernis erfüllt das (qualifizierte) elektronische Siegel also nicht. Die eIDAS-Verordnung stuft die elektronischen Siegel hingegen als (reines) Beweisinstrument ein – dies freilich auf einem sehr hohen Niveau: Sie schreibt fest, dass für ein qualifiziertes elektronisches Siegel die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten gilt, mit denen das qualifizierte elektronische Siegel verbunden ist.

Fazit: Das elektronische Siegel wird die qualifizierte elektronische Signatur nicht überflüssig machen oder ersetzen. Vielmehr ergänzen sich beide Verfahren perfekt. Juristische Personen können nicht selbst handeln, sondern immer nur die sie repräsentierenden natürlichen Personen. Einem elektronischen Siegel kann man im Nachhinein nicht mehr ansehen, welche natürliche Person das Siegel im konkreten Fall angebracht hat. Diese Sicherheit gewährleistet nur die qualifizierte elektronische Signatur. Die im deutschen Gesetz definierten Einsatzbereiche für die qualifizierte Signatur (vgl. § 126 a Abs. 1 BGB, § 130a ZPO, § 3 a Abs. 2 Satz 2 VwVfG) stehen also bis auf weiteres in bestem Einklang mit der eIDAS-Verordnung und können ohne weiteres fortbestehen. Die elektronischen Siegel werden sich dagegen in der Praxis bewähren, um Massenvorgänge in Organisationen mit einem Echtheitsstempel zu versehen. Sicherlich wäre es hilfreich, wenn im deutschen Recht dazu noch gezielte Anwendungsbereiche definiert würden. Am gewaltigen Einsatzpotenzial für elektronische Siegel dürfte angesichts der eingangs beschriebenen Einsatzszenarien jedenfalls kein Zweifel bestehen.

IV. Vertrauensdienste nach eIDAS

Die eIDAS-Verordnung behandelt verschiedene elektronische Vertrauensdienste:

- elektronische Signaturen,
- elektronische Siegel,
- elektronische Zeitstempel,
- Zertifikate für die Website-Authentifizierung,
- Dienste für die Zustellung elektronischer Einschreiben,
- Archivierungsdienste, auch für elektronische Signaturen, Siegel oder Zertifikate.

Damit die Vertrauensdienste ihren Namen auch verdienen, müssen sie natürlich rechtlich und technisch sicher gestaltet sein. Aus diesem Grund kommt den Vertrauensdiensteanbietern (VDAs) in der eIDAS-Verordnung eine zentrale Rolle zu. Darunter versteht die eIDAS-Verordnung diejenigen Anbieter, die Erstellungs-, Überprüfungs- und Validierungdienste vorhalten.

Hierbei wird hinsichtlich des Sicherheitsniveaus zwischen nichtqualifizierten und qualifizierten VDAs unterschieden. Ein qualifiziertes Zertifikat kann nur durch einen qualifizierten Anbieter ausgestellt werden.

Diesen Status erhält der Vertrauensdiensteanbieter, wenn er vor Betriebsaufnahme erfolgreich eine genau geregelte Konformitätsprüfung zur Übereinstimmung mit den Vorgaben der eIDAS absolviert hat. In diesem Fall stellt ihm eine staatlich akkreditierte Konformitätsbewertungsstelle ein Testat aus, welches der VDA der nationalen Aufsichtsbehörde übergibt und damit seine Betriebsaufnahme beantragt. Diese Aufsichtsbehörde wird im jeweiligen Mitgliedsstaat benannt und ist gesetzlich verpflichtet, innerhalb eines bestimmten Zeitraums zu reagieren. Diese Tätigkeit übernimmt in Deutschland voraussichtlich die Bundesnetzagentur mit folgenden konkreten Aufgaben:

- Sie prüft die Berichte der Konformitätsbewertungsstelle.
- Sie erfüllt die gemäß eIDAS vorgesehenen Meldepflichten.
- Sie veröffentlicht, bei positivem Ergebnis, die Daten des VDA in der offiziellen Vertrauensliste.

Die Vertrauensliste ist ein zentrales Instrument, um qualifizierte Siegel zu validieren. Wenn man ein elektronisches Siegel oder eine elektronisch gesiegelte Datei überprüfen will, wird die Vertrauensliste angesteuert, um zu überprüfen, welchen Status der zertifikatsausstellende VDA erfüllt und wie vertrauenswürdig er ist. Der Status des in der Vertrauensliste hinterlegten VDAs entscheidet über den Status des Siegelzertifikats des Endnutzers. Verletzt ein Vertrauensdiensteanbieter die allgemeinen Sicherheitsanforderungen, haftet er für alle „unmittelbaren Schäden", es sei denn, dass er nachweisen kann, dass er nicht fahrlässig gehandelt hat.

Alle zwei Jahre muss sich ein VDA auf eigene Kosten einer Wiederholungsprüfung bei seiner gewählten Konformitätsbewertungsstelle unterziehen. Das Ergebnis ist wiederum der Aufsichtsbehörde vorzulegen, die nach entsprechender Prüfung darüber entscheidet, ob der VDA weiterhin das oben beschriebene eIDAS-Gütesiegel tragen darf oder nicht.

Bei erfolgreicher Umsetzung der eIDAS-Vorgaben existieren in jedem Mitgliedsstaat vergleichbare Infrastrukturen und Rahmenbedingungen zur nachweislichen Umsetzung der Sicherheitsvorgaben zur Schaffung eines europäischen Vertrauensraumes.

V. Technische Umsetzung und Standards (ETSI/CEN)

Die Europäische Kommission hat parallel zur Schaffung der rechtlichen Vorgaben mittels der eIDAS-Verordnung die internationale Standardisierung für elektronische Identifizierung, Authentifizierung und Signaturen sowie zugehöriger Vertrauensdienste in die Wege geleitet.

Mit diesen Standardisierungsaufgaben sind die beiden folgenden europäischen Standardisierungsorganisationen betraut:

- Das Europäische Komitee für Normung (Comité Europèen de Normalisation / CEN). Dieses Komitee arbeitet mit dem Deutschen Institut für Normung (DIN) zusammen.
- Das Europäische Institut für Telekommunkationsnormen (European Telecommunication Standards Institute / ETSI).

Per EU-Mandate/460 wurden CEN und ETSI gemeinsam beauftragt, die bestehenden Interoperabilitätsnormen grundsätzlich neu zu strukturieren und umfassend zu überarbeiten.

Zu Beginn des Jahres 2016 wurden die wesentlichen Normen zur europaweiten Implementierung elektronischer Siegel verabschiedet. Hervorzuheben ist dabei die EN 319 411-2 für ein vereinheitlichtes Sicherheitsniveau qualifizierter Vertrauensdienste.

Prinzipiell unterscheidet sich technisch ein qualifiziertes Siegelzertifikat nicht von einem qualifizierten Signaturzertifikat. Beides sind standardisierte X.509-Zertifikate, die nur in Details voneinander abweichen. Daher sind für die Anwendung von Siegelzertifikaten nur wenige Anpassungen erforderlich.

Das Siegelzertifikat enthält neben der Angabe des Namens der juristischen Person weitere Informationen, um eine juristische Person zu einem zuvor erfolgten Identifizierungsprozess des VDA zuzuordnen. Ein qualifiziertes Siegelzertifikat ist durch einen berechtigten Vertreter der juristischen Person zu beantragen, die näheren Details zum Beantragungsprozess sind derzeit in Bearbeitung.

Zur eigentlichen Siegelerzeugung können zwei unterschiedliche Ansätze verfolgt werden.

1. Üblicherweise befinden sich das Siegelzertifikat und die zugehörige Siegelerstellungseinheit in Dateiform oder auf einem hardwarebasierten Träger, wie zum Beispiel einer Chipkarte, bei der juristischen Person, der das Siegel gehört. Die dort autorisierten Mitarbeiter haben das Siegel unter Kontrolle und setzen es ein, wenn ein Siegel benötigt wird.

   Der Standard EN 419212 liefert eine Programmierschnittstelle (API) für qualifizierte Signaturerstellungseinheiten, die auch für die Anforderungen an qualifizierte Siegelerstellungseinheiten übertragbar sind. Die neueste Überarbeitung der API im Jahr 2016 stellt bereits Implementierungsregeln für elektronische Siegel bereit: Dabei wurde auf den verpflichtenden Identifikationsnachweis durch natürliche Personen per PIN/Passwort bzw. Biometrie verzichtet und für juristische Personen angepasst.

2. Darüber hinaus ist es auch möglich, einen fernausgelösten Service zum Siegeln zu nutzen. Hierfür verbleibt das Siegelschlüsselpaar auf einem Hardware Sicherheitsmodul (HSM) beim VDA und wird von diesem verwaltet. Um ein elektronisches Siegel anzubringen, authentisiert sich ein Vertreter der juristischen Person gegenüber dem Service des VDAs und autorisiert den Siegelprozess mittels des dort gesicherten privaten Siegelschlüssels der Organisation. Vorteile dieser Lösung sind ein höheres Maß an Komfort, Verfügbarkeit und Praktikabilität. Allerdings ist diese Lösung ausschließlich im qualifizierten Kontext nutzbar.

   Für beide Ansätze der Siegelerstellung werden demnächst standardisierte Sicherheitsanforderungen in Form von Protection Profiles vorliegen, die wie die oben beschriebenen Aktivitäten für die Signaturerstellungseinheiten im Rahmen von CEN TC 224 unter Leitung des DIN erstellt werden.

VI. Erfolgsfaktoren

Um elektronische Siegel in der deutschen Behörden- und Unternehmenswelt zu etablieren, sind die Voraussetzungen gegeben. Dank eIDAS-Verordnung und den Vorbereitungen der Vertrauensdiensteanbieter stehen der Verbreitung der neuen organisationsbezogenen Zertifikate keine Hindernisse im Weg. Die Attraktivität dieses neuen Produkts für deutsche Anwender ergibt sich dadurch aber noch nicht von selbst: Niemand wird die elektronischen Siegel einsetzen, weil sie neu sind und Potenzial haben – vielmehr muss sich daraus ein konkreter Nutzen für die entsprechenden Stellen ergeben. Die Vorteile, die die Organisationen in Form von Workflow-Verbesserungen, Einsparungen, Reputationsgewinn aus den elektronischen Siegeln ziehen, müssen also den Aufwand für die Anschaffung und Implementierung der elektronischen Siegel kompensieren oder noch besser übersteigen.

Damit diese Rechnung aufgeht, müssen die elektronischen Siegel zunächst einmal so anwenderfreundlich wie möglich gestaltet werden. Hier sind die Anbieter elektronischer Siegel und Siegelanwendungskomponenten gefragt:

- **Das Antragsverfahren**
  für ein elektronisches Siegel muss möglichst unkompliziert gehalten werden. Hier kommt es darauf an, die eIDAS-Vorgaben für die Identitätsnachweise und Identitätsüberprüfungen so kundenfreundlich wie möglich umzusetzen. Das beliebige Absenken des Sicherheitsniveaus stellt dabei freilich keine Option dar: Auch für die Beantragung einer physischen Siegel-Petschaft bei einem Siegelhersteller muss eine Behörde schließlich ihre Legitimation nachweisen. Andernfalls würde die hohe Vertrauenswürdigkeit der Siegel leiden.

- **Die praktische Anwendung**
  des Siegels sollte möglichst einfach sein. In der täglichen Praxis soll ein normaler Sachbearbeiter das Siegel intuitiv ansteuern und anbringen können. Für Massenanwendungen ist ein automatisierter Siegelabruf vorzusehen, bei dem im Rahmen eines kontrollierten Prozesses viele Dokumente in kurzer Zeit elektronisch gesiegelt werden können. Ebenso einfach muss ein Empfänger ein gesiegeltes Dokument lesen und auf die Sicherheitsmerkmale „Echtheit des Absenders" und „Echtheit des Dokumenteninhalts" überprüfen können.

- **Der Preis**
  darf nicht prohibitiv hoch ausfallen, wenngleich die hohen Sicherheitsanforderungen an die Vertrauensdiensteanbieter zu berücksichtigen sind.

Noch wichtiger für die Akzeptanz der elektronischen Siegel wird es sein, attraktive Anwendungsmöglichkeiten zu etablieren. Leuchttürme sind gefragt, strahlende Beispiele, die den Sinn und Nutzen elektronischer Siegel anschaulich vermitteln. Die Industrie- und Handelskammern könnten beispielsweise die Abschlusszeugnisse, die sie Jahr für Jahr nach erfolgreicher Berufsausbildung für viele Hundertausend Prüflinge ausstellen, auch elektronisch gesiegelt zur Verfügung stellen und damit eine enorme Breitenwirkung entfalten. Die Banken könnten ihren buchführungspflichten Kunden elektronisch gesiegelte Kontoauszüge und Steuerbescheinigungen zukommen lassen und damit selbst Druckkosten und eine Menge Porto für den Papierversand sparen.

Nicht alles, was an Einsatzmöglichkeiten für elektronische Siegel denkbar wäre, ist heute allerdings auch schon rechtlich zulässig. Aus diesem Grund muss auch der deutsche Gesetzgeber seinen Beitrag leisten. Hier geht es nicht nur um einen symbolischen „Ritterschlag", sondern auch darum, die elektronischen Siegel in Einzelgesetzen und -verordnungen für konkrete Verwaltungsakte als geeignet, zulässig oder vielleicht sogar verbindlich zu erklären. Dafür bieten sich zum Beispiel an:

- E-Government-Gesetz des Bundes (§ 2, § 6, § 7): Behörden sollten verpflichtet werden, elektronische Dokumente auch mit elektronischem Siegel (nicht nur mit qualifizierter elektronischer Signatur) entgegennehmen zu können.

- E-Government-Gesetz des Bundes (§ 6, § 7): Zur Absicherung der elektronischen Aktenführung und der Vernichtung von Papieroriginalen bei der Einführung elektronischer Archive könnte als geeignete technisch-organisatorische Maßnahme das qualifizierte elektronische Siegel genannt werden.

- Verwaltungsverfahrensgesetz (§ 33): Schon in der jetzigen Form schreibt das Gesetz vor, dass jede Behörde von Urkunden, die sie selbst gefertigt hat, elektronische Dokumente und elektronische Beglaubigungen ausfertigen können soll. Was läge hier näher als die Maßgabe, eine solche Abschrift/Beglaubigung auch mit einem qualifizierten elektronischen Siegel abzusichern?

- Verwaltungsverfahrensgesetz (§ 37): Ausdrücklich ist schon jetzt festgeschrieben, dass auch ein elektronischer Verwaltungsakt die erlassende Behörde erkennen lassen muss. Genau diese Anforderung erfüllt das elektronische Siegel perfekt und sollte darum folgerichtig hier auch Erwähnung finden.

- Einkommensteuergesetz (§ 45a): Bescheinigungen über Kapitalerträge müssen das verantwortliche Kreditinstitut erkennen lassen. Dazu wird aktuell ein Verfahren mit maschinellem Ausdruck und Absenderkennzeichnung vorgeschrieben. Auch hier sollte die elektronische Ausstellung mit elektronischer Siegelung ermöglicht werden.

- Viertes Sozialgesetzbuch (§ 110): Im Zusammenhang mit der Aufbewahrungspflicht für Sozialversicherungsträger ist für die elektronische Form der Aufbewahrung ausdrücklich auch die Absicherung mit Hilfe elektronischer Siegel vorzusehen.

- Zehntes Sozialgesetzbuch (§ 25, § 33): Elektronische Auszüge oder Abschriften aus Akten, für die eine Akteneinsicht zu gewähren ist, können ebenfalls mit elektronischem Siegel abgesichert werden.

Die zunehmende Digitalisierung ist dringend angewiesen auf sichere Identitäten. Es ist darum enorm wichtig, dass auch die elektronische Identität von Organisationen sicher und offiziell überprüfbar wird. Wieder einmal zeigt sich in diesem Konzept die Unentbehrlichkeit von Vertrauensdiensteanbietern, die als verlässliche Beglaubigungsinstanz fungieren und die einzelnen Kommunikationspartner davon entlasten, ihre Identitäten gegenseitig prüfen zu müssen. Aber die Erfahrung zeigt: Nicht am grünen Tisch wird über den Erfolg neuer Technologien entschieden, sondern im praktischen Leben. Von daher muss alles dafür getan werden, auch überzeugende Lösungen mit den elektronischen Siegeln zu realisieren.

Verfasser:
Annette Floren, DE-CODA GmbH
Enrico Entschew, Bundesdruckerei GmbH
Arno Fiedler, Nimbus Technologieberatung GmbH

Erstellt mit Unterstützung durch:
Dr. Gisela Meister, Giesecke & Devrient GmbH,
Dr. Katrin Sobania, Deutscher Industrie- und Handelskammertag e. V.

Version 1.0 Stand: Juni 2016

DIHK
Deutscher
Industrie- und Handelskammertag