eIDAS und der ECM-Markt

Elektronische Identifizierung und Vertrauensdienste
als Chance für die Digitalisierung

www.bitkom.org

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Nils Britze, M.A. | Bereichsleiter Digitale Geschäftsprozesse
T 030 27576-201 | n.britze@bitkom.org

Rebekka Weiß, LL.M. | Leiterin Vertrauen & Sicherheit
T 030 27576-161 | r.weiss@bitkom.org

Verantwortliches Bitkom-Gremium

AK Anwendung elektronischer Vertrauensdienste
AK ECM-Compliance

Besonderer Dank gilt dem Autorenteam, bestehend aus:

- Claudia Göbel, DocuWare GmbH
- Dr. Detlef Hühnlein, ecsec GmbH
- Dr. Siegfried Kaiser, ITOB GmbH
- Enrico Entschew, Bundesdruckerei GmbH
- Jürgen Prummer, d.velop AG
- Markus Schuster, intarsys AG
- Nils Britze, Bitkom e. V.
- Rebekka Weiß, Bitkom e. V.
- Steffen Schwalm, msg systems ag
- Tatami Michalek, secrypt
- Thorsten Brand, Zöller & Partner GmbH

Satz & Layout

Kea Schwandt | Bitkom e.V.

Titelbild

© Tookapic – pexels.com

Copyright

Bitkom, 2019

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom.

eIDAS und der ECM-Markt

Elektronische Identifizierung und Vertrauensdienste
als Chance für die Digitalisierung

Inhaltsverzeichnis

Vorwort 6

Executive Summary 7

1 Einführung 9

2 Die eIDAS-Elemente im Überblick 12

2.1 Identifizierungsdienst 13
2.2 Signatur- und Siegelerstellungsdienst 14
2.3 Bewahrungsdienst 14
2.4 Validierungsdienst 14
2.5 Einschreib- und Zustelldienst 15
2.6 Zeitstempeldienst 16
2.7 Vertrauensdiensteanbieter 16

3 Nutzen von eIDAS für den ECM-Markt 18

3.1 Einsatzszenarien im ECM-Umfeld 18
3.2 Einsatzszenarien in Abteilungen und Branchen 24

4 Zukunftsweisende Initiativen: Vereinheitlichung der Vertrauensdienste 32

5 Anhang 01 – Die eIDAS Werkzeuge im Detail 34

5.1. Elektronische Dokumente – Grundlage für die Digitalisierung 34
5.1.1 Elektronische Signaturen 34
5.1.2 Elektronische Siegel 37
5.1.3 Zeitstempel 39
5.1.4 Elektronische Einschreib- und Zustelldienste 41
5.1.5 Validierungs- und Bewahrungsdienste 42
5.1.6 Zertifikate für Website-Authentifizierung 42

Anhang 02 – Das »eIDAS-Vertrauenssystem« 44

Abkürzungsverzeichnis

Art.	Artikel
ASiC	Associated Signature Containers
AÜG	Arbeitnehmerüberlassungsgesetz
AÜV	Arbeitnehmerüberlassungsvertrag
BGB	Bürgerliches Gesetzbuch
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CAB	Konformitätsbewertungsstelle
CAdES	CMS Advanced Electronic Signatures
CAR	Conformity Assessment Report
CMS	Cryptographic Message Syntax
DAkkS	Deutsche Akkreditierungsstelle
ECM	Enterprise Content Management
EDS	Electronic Delivery Service
EG	Europäische Gemeinschaft
eIDAS	electronic IDentification, Authentication and Trust Services
ENISA	Europäische Agentur für Netz-und Informationssicherheit
ERP	Enterprise Resource Planning
EU	Europäische Union
GUI	Graphical User Interface
HBA	Heilberufsausweis
HSM	Hardware Security Module
ID	Identification
KIS	Krankenhausinformationssystem
NAB	National Accreditation Bodies
NTP	Network Time Protocol
PAdES	PDF Advanced Electronic Signatures

PDF	Portable Document Format
PIN	Persönliche Identifikationsnummer
PresS	Preservation Service
PSD	Payment Services Directive
QES	Qualifizierte elektronische Signatur
PIN	Persönliche Identifikationsnummer
PresS	Preservation Service
PSD	Payment Services Directive
QES	Qualifizierte elektronische Signatur
QESI	Qualifiziertes elektronisches Siegel
SAK	Signaturanwendungskomponente
SigS	Signature Generation & Sealing Service
SMS	Short Message Service
TAN	Transaktionsnummer
TLS	Transport Layer Security
TSA	Time Stamp Authority
ValS	Validation Service
VDA	Vertrauensdiensteanbieter
VDG	Vertrauensdienstegesetz
VDV	Vertrauensdiensteverordnung
XAdES	XML Advanced Electronic Signatures
ZPO	Zivilprozessordnung

Vorwort

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

Dieser Leitfaden bietet detaillierte Beschreibungen der verschiedenen Elemente der eIDAS-Verordnung und erläutert deren Relevanz für den ECM-Markt. Besonders beleuchtet wird die neue mobile Signatur oder Fernsignatur, denn sie eröffnet neue Möglichkeiten für den grenzüberschreitenden Umgang mit Dokumenten in der EU. Anwendungsfälle für die einzelnen Vertrauensdienste und konkrete Anbieterbeispiele zeigen den konkreten Einsatz der Vertrauensdienste und der elektronischen ID.

Besonderer Dank gilt folgenden Mitgliedern der Arbeitskreise ECM-Compliance und Anwendung elektronischer Vertrauensdienste, die mit ihrer Expertise und wertvollen praktischen Erfahrungen ganz maßgeblich zur Entstehung des Leitfadens beigetragen haben.

Executive Summary

Mit dem Inkrafttreten der Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS) für elektronische Transaktionen im Binnenmarkt der Europäischen Union wurde die Basis für eine europaweite, rechtsgültige elektronische Kommunikation und sichere elektronische Identifizierung geschaffen. Mit Hilfe der Vertrauensdienste, wie elektronischen Signaturen, Siegeln, Zeitstempeln, Zustelldiensten und Zertifikaten zur Authentifizierung, können zukünftig Unternehmen, Verwaltungen und Privatpersonen digitale Dokumente wie Angebote, Bestellungen, Verträge u.v.m. innerhalb der Europäischen Union auf einer einheitlichen Rechtsbasis austauschen.

Das effiziente und optimierte Verwalten, Nutzen und Bereitstellen strukturierter und unstrukturierter Informationen ist seit jeher eine wichtige Aufgabe für Unternehmen. Enterprise Content Management (ECM) bietet für diese Herausforderung die passenden Methoden und Werkzeuge. Während viele Großunternehmen ECM in unterschiedlichsten Reifegraden bereits einsetzen, sind kleinen und mittelständigen Unternehmen die Vorteile von ECM noch wenig bekannt. Eine ähnliche Situation zeigt sich bei den zahlreichen Anwendungen und Werkzeugen, die die eIDAS-Verordnung eIDAS-Verordnung ermöglicht. Beide Bereiche sind für die erfolgreiche Digitalisierung von Geschäftsprozessen unerlässlich und greifen bei zahlreichen Anwendungen ineinander. Vereinfachtes Vertragsmanagement, schnellere, digitale Abwicklung von Unterschriftenprozessen, sichere Archivierung und Authentifizierungsprozesse auf sämtlichen Geschäftsebenen sind nur einige der Beispiele, bei denen sich ECM und eIDAS ergänzen.

Dieser Leitfaden bietet detaillierte Beschreibungen der verschiedenen Elemente der eIDAS-Verordnung und erläutert deren Relevanz für den ECM-Markt. Besonders beleuchtet werden die neue mobile Signatur und die Fernsignatur. Beide Instrumente eröffnen neue Möglichkeiten für den grenzüberschreitenden Umgang mit Dokumenten in der Europäischen Union. Das Papier legt in einem ersten Abschnitt die verschiedenen Elemente der eIDAS Instrumente dar und erläutert anschließend die Einsatzszenarien im ECM-Umfeld. Anschließend wird anhand des Vertragswesens und der Gesundheitsbranche aufgezeigt, welche neuen Möglichkeiten sich durch die eIDAS-Verordnung ergeben. Das Papier schließt mit einem Ausblick über Initiativen zur weiteren Vereinheitlichung der Vertrauensdienste.

1 Einführung

1 Einführung

Die EU-Verordnung eIDAS (Electronic Identification, Authentication and Trust Services) stellt Standards für die elektronische Identifizierung und für Vertrauensdienste in der Europäischen Union auf. Mit diesen Diensten lässt sich die Identität von Individuen und Unternehmen sowie die Authentizität von elektronischen Dokumenten überprüfen. Die Verordnung soll dazu beitragen, den sicheren elektronischen Austausch zwischen Unternehmen, Bürgern und Behörden zu erleichtern sowie Online-Services und elektronische Geschäftsbeziehungen innerhalb der EU effizienter zu machen. eIDAS schafft damit einen wesentlichen Baustein für den rechtlichen Rahmen des einheitlichen digitalen EU-Binnenmarkts.

Im Bereich der Vertrauensdienste ist die Verordnung seit dem 30. Juni 2017 rechtsgültig, für die elektronische Identifizierung gilt sie seit dem 18. September 2018. EU-Verordnungen haben den Charakter von »europäischen Gesetzen«, weshalb die Mitgliedsstaaten ihre nationale Gesetzgebung daran anpassen müssen; anders als bei EU-Richtlinien bedarf es aufgrund der unmittelbaren Wirkung von Verordnungen keiner nationalen Umsetzung.

Bisher boten Signaturfunktionen Möglichkeiten, elektronische Unterschriften verschiedener Art und Qualität in einer Enterprise Content Management (ECM)-Umgebung zu nutzen. Eine elektronische Unterschrift kann hierbei technisch unterschiedlich ausgeprägt sein. Ein grafisches Bild einer gescannten Unterschrift kann für den Anwender ebenso eine Unterschrift darstellen wie für andere ein Login mit Passwort oder die Unterzeichnung auf einem Unterschriftenpad.

In Deutschland ist im Bürgerlichen Gesetzbuch, im Vertrauensdienstegesetz (VDG) und in der Vertrauensdiensteverordnung (VDV) geregelt, welche Arten von Unterschriften nicht nur einfach eine Authentifizierungsbehauptung darstellen, sondern auch absichern, dass sie der eigenhändigen Unterschrift gleichkommen. Damit können sie bei jenen Vorgängen, in denen die sogenannte Schriftform gefordert ist, die eigenhändige Unterschrift ersetzen. In Deutschland ist dies bisher nur mit der qualifizierten elektronischen Signatur (QES) möglich[1]. Alle anderen elektronischen Varianten der Authentifizierung können in einer ECM-Umgebung aber ebenfalls von Interesse sein, beispielsweise zum Benutzernachweis im Rahmen von elektronischen Freigabeprozessen. Hier muss nicht immer mit der qualifizierten elektronischen Signatur gearbeitet werden. In der Praxis kommt diesem »normalen« Authentifizierungsprozess sogar eine weitaus größere Bedeutung zu, da für die gängigen Verträge des Alltags kein Schriftformerfordernis besteht. Die Authentifizierung belegt, dass der Benutzer tatsächlich die Person ist, die er zu sein behauptet. Mit Benutzername und Passwort ist sie in jeder ERP-Anwendung gang und gäbe und gilt als ausreichend vertrauenswürdig für Buchungs-, Freigabe- und Genehmigungsverfahren jeder Art.

Es gibt aber auch Anwendungsbereiche, in denen eine qualifizierte elektronische Signatur vorgeschrieben ist. So gibt es z.B. eine gesetzliche Regelung für Unternehmen, die dem Sozialversicherungsrecht unterliegen: Danach sind beim ersetzenden Scannen (nach dem Scannen wird das Original vernichtet) die rechnungswesensrelevanten Dokumente mit der qualifizierten elektro-

1 §126a Absatz 1 BGB bestimmt: Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur versehen.

nischen Signatur derjenigen Person zu versehen, die die Bildprüfung der Scan-Dokumente vorgenommen hat. Auch gibt es beispielweise im kommunalen Umfeld Anweisungen, dass elektronische Freigabeprozesse nur mit einer qualifizierten elektronischen Signatur erfolgen dürfen. Doch selbst nach 20 Jahren Signaturgesetz in Deutschland muss festgestellt werden, dass der Massenmarkt für Signaturen nicht entstanden ist, sieht man von den wenigen Nischen wie Anwaltskanzleien oder dem Sozialversicherungsbereich ab, wo die Nutzung für bestimmte Einsatzfelder vorgeschrieben ist. Doch die eIDAS-Verordnung eIDAS-Verordnung und das darauf basierende deutsche Vertrauensdienstegesetz bieten hier zahlreiche neue Möglichkeiten. Auch der einheitliche europäische Markt macht die eIDAS-Werkzeuge interessant (hierzu im Einzelnen: Annex).

Die ECM-Hersteller können heute bereits Dokumente mit qualifizierter elektronischer Signatur verwalten. Über Eigenentwicklungen oder die Integration von Drittprodukten stellen sie Funktionen wie das Erzeugen und Prüfen von Signaturen oder die Nachsignatur zur Verfügung. Auch können elektronische Vorgänge mit dem Einsatz der qualifizierten elektronischen Signatur umgesetzt werden. Diese Anwendungsfälle werden sich durch eIDAS erweitern, sodass es für ECM-Anwender und ECM-Anbieter interessant sein wird, eIDAS-konforme Objekte zu verwalten oder heute noch papierbasierte Prozesse mit eIDAS-konformen Komponenten umzusetzen. Der deutsche ECM-Markt erwartet daher von der eIDAS-Umsetzung positive Effekte, vor allem durch die neu eingeführte Fernsignatur, die viele wirtschaftliche und behördliche Vorgänge vereinfachen kann. Vorgänge, die heute nur mit Papierunterschrift oder qualifizierter elektronischer Signatur möglich sind, können zukünftig vielleicht mit einem eIDAS-konformen Verfahren umgesetzt werden.

Dieser Leitfaden stellt im Folgenden die verschiedenen Elemente der eIDAS-Verordnung vor und erläutert deren Relevanz und Anwendungsfälle für den ECM-Markt. Wie bereits erwähnt, spielt die neue mobile Signatur oder Fernsignatur in der Publikation eine besondere Rolle, weil sie neue Optionen für den grenzüberschreitenden Umgang mit Dokumenten in der EU eröffnet. Die Anwendungsszenarien für das »eIDAS-Ökosystem« zeigen den konkreten Einsatz der Vertrauensdienste, der elektronischen ID und alternativen Identifizierungsverfahren, wie z.B. dem Videoidentverfahren, auf. Den Abschluss bildet ein Blick auf die derzeitigen Angebote für Vertrauensdienste und die elektronische Identifizierung sowie auf Initiativen für deren weitere Vereinheitlichung. In Annex zu diesem Leitfaden werden der eIDAS-Werkzeuge rechtlich und technisch im Detail beleuchtet.

2 Die eIDAS-Elemente im Überblick

2 Die eIDAS-Elemente im Überblick

Die »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«, die gemeinhin als »eIDAS-Verordnung« bekannt ist, verspricht, das Vertrauen und die Effizienz von elektronischen Transaktionen in Europa zu steigern.

Dieser Abschnitt gibt einen groben Überblick über die wesentlichen Teile und Dienste des »eIDAS-Ökosystems«.

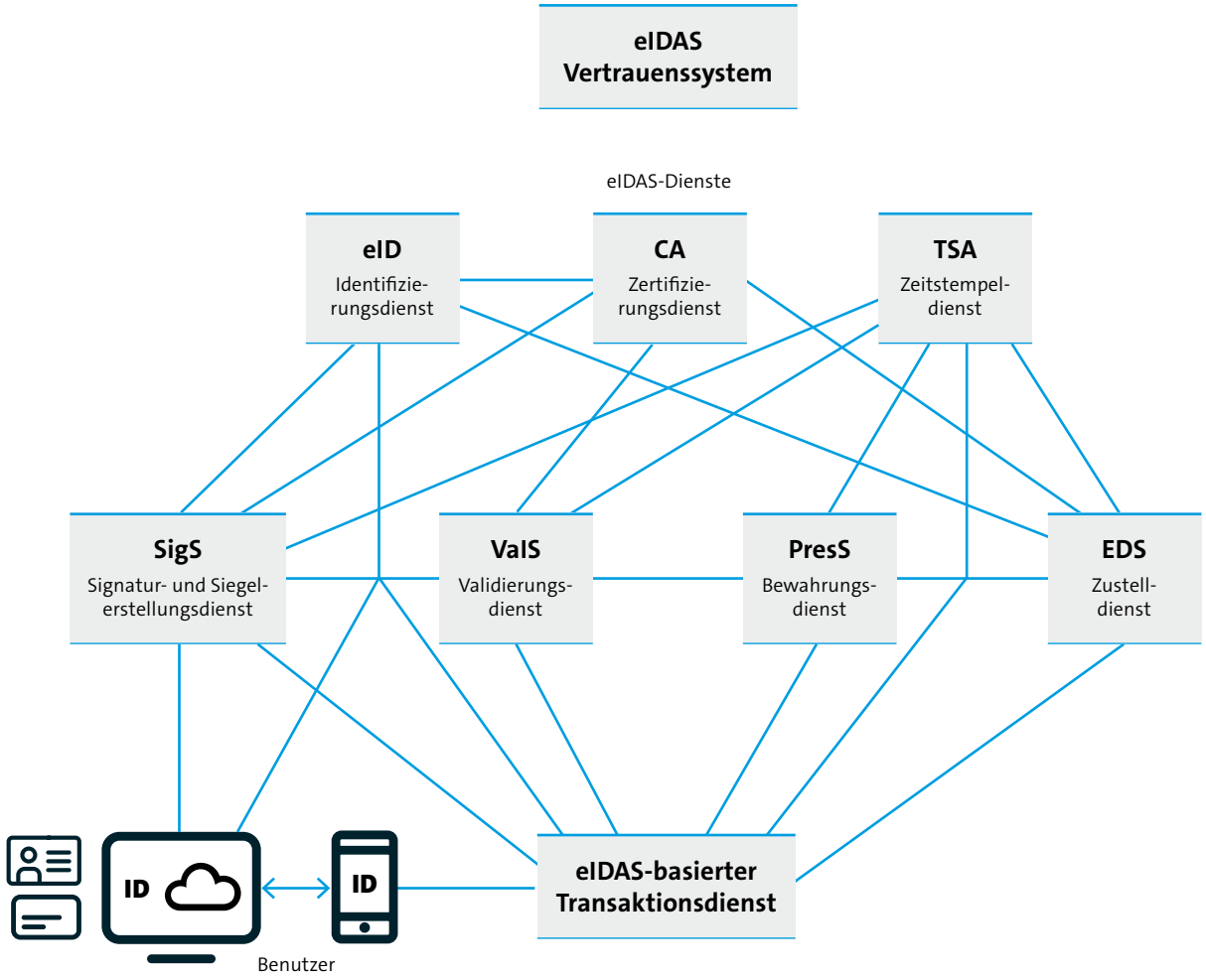

Abbildung 1: ↗https://blog.eid.as/de/eidas-oekosystem

Wie in der Abbildung gezeigt, umfasst dieses Ökosystem insbesondere den »Benutzer«, der elektronische Dokumente[2] in einem »eIDAS-basierten Transaktionsdienst« verarbeitet. Dieser Transaktionsdienst greift wiederum auf eine Reihe von weiteren »eIDAS-Diensten« zu, deren Vertrauenswürdigkeit durch das »eIDAS Vertrauenssystem«[3] sichergestellt wird.

Die »eIDAS-Dienste« umfassen den »Identifizierungsdienst«[4] gemäß Kapitel II der eIDAS-Verordnung und verschiedene »Vertrauensdienste«[5] gemäß Artikel 3 (16) und Kapitel III der eIDAS-Verordnung. Diese umfasst insbesondere den »Signatur- und Siegelerstellungsdienst«[6], den »Bewahrungsdienst«[7], den »Validierungsdienst«[8], den »Zustelldienst« für elektronische Einschreiben[9] und bereits weit verbreitete klassische Vertrauensdienste, wie z.B. »Zeitstempeldienst«[10] und nicht zuletzt den »Zertifizierungsdienst«[11].

2.1 Identifizierungsdienst

Der Identifizierungsdienst (eID-Service) ermöglicht die sichere Identifizierung und Authentifizierung von Benutzern und juristischen Personen. Hierbei können die gemäß Artikel 9 eIDAS-Verordnung eIDAS-Verordnung notifizierten Identifizierungssysteme sowie weitere geeignete Mittel zur Identifizierung und Authentifizierung genutzt werden. Für die Bewertung des Sicherheitsniveaus eines Identifizierungssystems bzw. Identifizierungsmittels sind in Artikel 8 eIDAS-Verordnung die Stufen »niedrig«, »substanziell« und »hoch« definiert. Detaillierte Anforderungen finden sich in der zugehörigen Durchführungsverordnung (EU) 2015/1502. Notifizierte Identifizierungssysteme, die zumindest die Stufe »substanziell« erreichen, werden gemäß Artikel 6 eIDAS-Verordnung von den EU-Mitgliedsstaaten bei grenzüberschreitenden Transaktionen gegenseitig anerkannt.

Durch die am 26.September 2017 erfolgte Veröffentlichung im Amtsblatt der Europäischen Kommission wurde das Notifizierungsverfahren für die Online-Ausweisfunktion des deutschen Personalausweises erfolgreich abgeschlossen. Vorausgegangen war eine Begutachtung durch technische Experten nahezu aller EU-Mitgliedstaaten, wodurch die Erfüllung des höchstmöglichen Vertrauensniveaus (Level of Assurance »high«) bestätigt wurde. Damit wurde die eID-Funktion des Personalausweises und des elektronischen Aufenthaltstitels ab dem 29. September 2018 europaweit zur elektronischen Identifizierung in digitalen Verwaltungsverfahren anerkannt

2 siehe Anhang 1
3 siehe Anhang 2
4 eID-Service
5 Auch Trust Services genannt
6 SigS, Signature Generation & Sealing Service
7 PresS, Preservation Service
8 ValS, Validation Service
9 EDS, Electronic Delivery Service
10 TSA, Time Stamp Authority
11 CA, Certification Authority

und kann seitdem auch von Unternehmen im europäischen Binnenmarkt auf freiwilliger Basis akzeptiert werden.

2.2 Signatur- und Siegelerstellungsdienst

Die Empfänger von digitalen Erklärungen und Dokumenten können sich dank einer elektronischen Signatur oder eines Siegels sicher sein, dass diese tatsächlich von dem jeweiligen Aussteller stammen. Neu ist mit der eIDAS-Verordnung, dass diese Siegel auch von Unternehmen, Behörden oder anderen Organisationen verwendet werden können. Bisher konnten nach dem Signaturgesetz in Deutschland nur natürliche Personen eine qualifizierte elektronische Signatur einsetzen. Darüber hinaus wird der elektronische Rechtsverkehr um das Instrument der Fernsignatur bereichert. Die Szenarien sind vielfältig: Zeugnisse, Bewerbungsunterlagen, Anträge in Verwaltungsverfahren oder E-Mails, die in der Masse an Spam-Nachrichten als sicher identifiziert werden sollen. Zudem können sich mit den elektronischen Siegeln zukünftig auch Geräte im Internet of Things authentifizieren. Der »Signatur- und Siegelerstellungsdienst«[12] ermöglicht die Erzeugung von (qualifizierten) elektronischen Signaturen gemäß Abschnitt 4 und (qualifizierten) elektronischen Siegeln gemäß Abschnitt 5 eIDAS-Verordnung in technischen Formaten, wie z.B. CAdES, XAdES und PAdES.

2.3 Bewahrungsdienst

Die beweiskräftige Aufbewahrung signierter Dokumente über einen langen Zeitraum macht eine Form der Speicherung notwendig, die die Lesbarkeit und den Erhalt der Beweiskraft der Dokumente und Signaturen unabhängig vom Speichermedium sicherstellt. Um die rechtliche Gültigkeit und die Beweiskraft elektronischer Signaturen und Siegel langfristig zu erhalten, müssen geeignete Bewahrungstechniken eingesetzt werden, wie sie in ETSI SR 019 510 beschrieben sind. Die Aufbewahrungstechniken, die von einem »Bewahrungsdienst« (Preservation Service, PresS) gemäß Artikel 34 der eIDAS-Verordnung umgesetzt werden müssen, können sich auf Nachweisdateien (Evidence Records) gemäß RFC 4998 oder RFC 6283 oder die kontinuierliche Konservierung von Signaturen mit Archivzeitstempeln gemäß CAdES oder XAdES stützen.

2.4 Validierungsdienst

Die (qualifizierten) elektronischen Signaturen und Siegel, die mit dem oben erläuterten SigS erzeugt werden, können mit dem »Validierungsdienst« (Validation Service, ValS) geprüft werden. Hierzu nutzt der Validierungsdienst die in den Vertrauenslisten gemäß Artikel 22 eIDAS Verordnung bzw. dem Durchführungsbeschluss DFB (EU) 2015/1506 und ETSI TS 119 162(v2.1.1) enthaltenen Zertifikate als Vertrauensanker und führt eine Signaturprüfung gemäß EN 319 102-1 in Verbindung mit einer geeigneten Signaturprüfungspolitik[13] durch.

12 Signature Generation & Sealing Service, SigS.

13 Signature Validation Policy

2.5 Einschreib- und Zustelldienst

In der papierbasierten Welt kann beim Versand eines Briefs als Einschreiben sicher erkannt werden, dass ein Brief wirklich den Empfänger erreicht hat. Diese Dienstleistung wird durch die Postdienstleister angeboten. In diesem Fall schreibt der Absender seine Nachricht auf Papier, steckt dieses in einen verschlossenen Umschlag, auf dem die Adresse des Empfängers vermerkt ist und verschickt diesen schließlich mit der Post. Die Zurechenbarkeit, die Vertraulichkeit und die Unversehrtheit des Briefs werden weitgehend durch den Absender sichergestellt, während der Postdienstleister vor allem die Gewähr für die Verfügbarkeit und die korrekte Zustellung der Sendung übernimmt.

Gemäß Artikel 44 eIDAS-Verordnung müssen qualifizierte Dienste für die Zustellung elektronischer Einschreiben [...] folgende Anforderungen erfüllen:

a) Sie werden von einem oder mehreren qualifizierten Vertrauensdiensteanbietern erbracht.

b) Sie stellen die **Identifizierung des Absenders** mit einem hohen Maß an Vertrauenswürdigkeit sicher.

c) Sie stellen die **Identifizierung des Empfängers** vor der Zustellung der Daten sicher.

d) Das Absenden und Empfangen der Daten ist durch eine fortgeschrittene **elektronische Signatur** oder ein fortgeschrittenes **elektronisches Siegel** eines qualifizierten Vertrauensdiensteanbieters auf eine Weise gesichert, die die Möglichkeit einer unbemerkten Veränderung der Daten ausschließt.

e) Jede Veränderung der Daten, die zum Absenden oder Empfangen der Daten nötig ist, wird dem Absender und dem Empfänger der Daten deutlich angezeigt.

f) Das Datum und die Zeit des Absendens, Empfangens oder einer Änderung der Daten werden durch einen **qualifizierten elektronischen Zeitstempel** angezeigt.

Vor dem Hintergrund dieser Anforderungen ist es offensichtlich, dass ein Einschreiben-Zustelldienst (Electronic Delivery Service, EDS) eine Vielzahl weiterer eIDAS-Dienste umfasst bzw. nutzen muss. Dazu gehören z.B. die Dienste für die Identifizierung, die Signatur- und Siegelerstellung, die Validierung und für Zeitstempel. Zudem muss er die vom Vertrauensdiensteanbieter (VDA) bereitgestellten Zertifikatstatusinformationen auswerten.

2.6 Zeitstempeldienst

Bei vielen elektronischen Transaktionen ist es nötig, die Existenz bestimmter Daten zu einem bestimmten Zeitpunkt beweisen zu können (z.B. für elektronische Signaturen, bei der Verwaltung elektronischer Rechte, bei elektronischen Verträgen oder für beweiskräftige Aufzeichnungen). Zu diesem Zweck erhält ein Zeitstempeldienst die mit einem Zeitstempel zu versehenden Daten oder einen Hashwert davon. Er liefert dann einen Zeitstempel zurück, der neben dem Hashwert der Daten eine zuverlässige Zeitangabe umfasst und mit einer Signatur des Zeitstempeldienstes versehen ist.

2.7 Vertrauensdiensteanbieter

Ein Vertrauensdiensteanbieter erzeugt elektronische Zertifikate und stellt diese für Benutzer und andere Entitäten[14] aus. Dies kann entweder direkt erfolgen oder vermittelt über einen entsprechenden Dienst, wie z.B. den eIDAS-basierten Transaktionsdienst oder den Signatur- und Siegelerstellungsdienst. In diesem Fall interagiert der Dienst mit dem System der Zertifizierungsstellen und bestimmt zusammen mit dem Vertrauensdiensteanbieter die Identität des Zertifikatsinhabers: Die entsprechenden Identitätsattribute werden geprüft und bestätigt, schließlich werden sie mit dem öffentlichen Schlüssel des Zertifikatsinhabers kombiniert und zur Erstellung des Zertifikates vom Vertrauensdiensteanbieter signiert.

14 Zertifikatsinhaber, Subject.

3 Nutzen von eIDAS für den ECM-Markt

3 Nutzen von eIDAS für den ECM-Markt

Die in der Einführung dargestellten Anwendungsszenarien zeigen die verbesserten Einsatzmöglichkeiten von Signaturverfahren durch die eIDAS-Verordnung. Die qualifizierte elektronische Signatur mit angeschlossenem Kartenleser am vorhandenen PC ist nicht mehr die einzige Möglichkeit, rechtlich gültige elektronische Dokumente zu erstellen. Durch den Einsatz von Fernsignaturen oder digitalen Siegeln werden technische Hürden der Signaturnutzung gesenkt und neue Einsatzmöglichkeiten erschlossen.[15] Hinzu kommt die EU-weite Standardisierung durch die Verordnung, die es großen multinationalen Anwendern erlaubt, den Einsatz über Ländergrenzen hinweg zu planen. Technologie-Hersteller können mit der Technik einen größeren Markt adressieren.

Der Kompetenzbereich Digital Office im Bitkom versteht unter Enterprise Content Management (ECM) klassischerweise die Technologien zur Erfassung, Verwaltung, Speicherung, Bewahrung und Bereitstellung von Content und Dokumenten zur Unterstützung organisatorischer Prozesse. ECM schließt dabei herkömmliche Technologien wie Input Management, Dokumentenmanagement, Collaboration, Web Content Management, Workflow, Business Process Management, Output Management, Storage und elektronische Archivierung ein. Das folgende Kapitel skizziert die Einsatzszenarien in diesem Umfeld.

3.1 Einsatzszenarien im ECM-Umfeld

ECM-Hersteller haben Signaturtechnologien schon lange Zeit im Fokus, da es unterschiedlichste Integrationsmöglichkeiten zu einem ECM-Produkt gibt, z.B.:

- Archivierung von signierten und gestempelten Objekten
- Erstellung von Einzel- und Massensignaturen (Zeitstempel, Signaturen, Siegel)
- Integration in Scan-Komponenten
- Nutzung in Freigabe- oder Workflow-Prozessen
- Signaturprüfung
- Beweiswerterhaltung durch Nachsignatur

Da Dokumente auf verschiedenen Wegen in ein ECM-System gelangen können, ist die Integration von Signaturkomponenten an unterschiedlichen Stellen und im Prozess sinnvoll. Die Scan-Anwendung sollte Signaturen im Rahmen der Papiererfassung erzeugen können. Bei Freigabe- oder Workflow-Prozessen kann die elektronische Unterschrift als Nachweis genutzt werden, wann und durch wen ein bestimmter Schritt erfolgt ist. Aber auch der Archivserver, der für die Langzeitarchivierung der Dokumente zuständig ist, kann auf Teilfunktionen von Signatur-

15 Dadurch muss keine lokale Hardware für den Kartenleser mehr unterstützt werden, sondern es kann zentral auf einen entsprechenden Server-Dienst zugegriffen werden. Interessant ist dabei auch der Einsatz softwarebasierter Zertifikate, eine Lösung, die bereits auch von ECM-Herstellern realisiert wird.

komponenten zurückgreifen, um Integritätsschutzfunktionen durch Berechnung von Inhaltswerten, sogenannte Hashwerte, einzusetzen.

Zusätzlich kommen Dokumente von Dritten hinzu, die bereits eine Signatur besitzen und in einer ECM-Umgebung verwaltet werden sollen. Signaturinformationen sollten ggf. direkt im ECM-Client angezeigt und die Signatur selbst verifiziert werden können. Dies kann, je nach Anforderung, manuell oder automatisch erfolgen. Die Ergebnisse dieser Prüfung sollen in Prüfprotokollen dokumentiert werden.

Dieses heute schon vorhandene Zusammenspiel aus ECM- und Signaturtechnologien wird durch die eIDAS-Verordnung erweitert und erleichtert.

3.1.1 Einsatzszenarien im ECM-Umfeld

Die eIDAS-Verordnung ermöglicht einfachere Verfahren der Signaturerstellung. So können Fernsignaturen und Siegeldienste integriert werden, um Prozesse mit hohen Anforderungen an eine elektronische Unterschrift umzusetzen. Wo bisher zur Erzeugung einer qualifizierten elektronischen Signatur in einem Verfahren eine Infrastruktur bestehend aus Signaturkarte und Kartenlesegerät erforderlich war, kann durch die eIDAS-Verordnung die Fernsignaturtechnologie zum Einsatz kommen. Dadurch muss keine lokale Hardware für den Kartenleser mehr unterstützt werden, sondern es kann zentral auf einen entsprechenden Server-Dienst zugegriffen werden. Dadurch ermöglicht es die eIDAS-Verordnung, Dokumente mobil zu unterschreiben – ohne Karte.

Hierfür bestehen verschiedene Lösungsszenarien. Eine Option ist die Einmalsignatur, wie sie von verschiedenen Vertrauensdiensteanbietern offeriert wird. Diese Lösung bietet sich vor allem für Nutzer an, die selten elektronisch unterschreiben. In diesem Fall erfolgt die Identifizierung der Nutzers beispielsweise über das Videoident-Verfahren[16], bei dem die Person über ein zugelassenes Videoverfahren identifiziert wird, nutzbar auch mit Kameras von Mobilgeräten. Die Unterschrift selbst wird anschließend z.B. durch eine SMS-TAN ausgelöst, ein intuitives Vorgehen, wie es dem Anwender bereits aus dem Onlinebanking bekannt ist. Neben Videoident kommt häufig eine eID für die Identifizierung des Unterschreibenden zur Anwendung. Dies ist für die weitere Nutzung mobiler Unterschriften besonders interessant, weil seit September 2018 die Regelungen für eID-Verfahren der eIDAS in Kraft getreten sind. Die hiermit verbundene Anerkennungspflicht für alle notifizierten eID Systeme für öffentliche Stellen eröffnet dem Anwender die Möglichkeit, weitere eID-Lösungen zu nutzen – neben dem neuen Personalausweis – und so das jeweils bedarfsgerechte Identifizierungswerkzeug einzusetzen.

16 Hinsichtlich des Videoident-Verfahrens bestehen im Bereich des VDG besondere Anforderungen für die deutschen Vertrauensdiensteanbieter gegenüber weiteren Anbietern aus dem EU-Ausland. In diesem Zusammenhang wird auf die Bitkom Stellungnahme zum Videoident-Verfahren als national anerkannte Identifikationsmethode verwiesen: **↗https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Position-zum-Videoidentverfahren-als-national-anerkannte-Identifikationsmethode.html**

Dieses Szenario ist branchenübergreifend nutzbar. Konkrete Anwendungsbeispiele wären:

- online abgeschlossene Verträge
- Adhoc-Verträge und -Dienstleistungen
- Unterschrift von Wartungsprotokollen technischer Anlagen
- Unterschrift behördlicher Bescheide
- Anträge, Angebote usw.

Neben der Einmalsignatur bieten Portallösungen von Vertrauensdiensteanbietern eine weitere Option zur Nutzung mobiler Unterschriften. Sie lassen sich unmittelbar wie transparent in die Unternehmenssoftware, z.B. ein ERP, integrieren. In diesem Fall identifizieren sich die unterschriftsberechtigten Mitarbeiter beim Vertrauensdienstanbieter, der die Identitätsdaten in der eigenen Infrastruktur hinterlegt. Die Signatur selbst kann dann über verschiedene Authentifizierungsmechanismen auch mobil (Token+TAN etc.) ausgelöst werden. Der für Unternehmen wie Behörden herausragende Fakt ist die Möglichkeit, Kunden auf das Portal einzuladen und diesen per Videoident oder eID und SMS-TAN wie im ersten Beispiel aufgezeigt, ebenso die Chance zur Unterzeichnung zu geben. Damit lassen sich vollständige B2G2C-Prozesse vertrauenswürdig wie nachvollziehbar abbilden. Die Anwendungsbeispiele sind ähnlich der Einmalsignatur. Das Szenario hier eignet sich jedoch eher für Anwender mit umfangreicher Interaktion mit Kunden, Behörden und Partnern.

Die Finanzindustrie nutzt eine weitere Option um auf einfache Weise Dokumente elektronisch zu unterschreiben. In diesem Fall fungiert der Mitarbeiter des Kreditinstituts oder bspw. der Außendienstmitarbeiter der Versicherung als Identifizierungsdienstleister des VDA. Das bedeutet, er identifiziert den Kunden mit Hilfe von dessen physischen Personalausweis und übermittelt diese Daten an den VDA. Im Ergebnis erhält der Kunde ein Zertifikat, mit dem er durch eine TAN oder bspw. einen einmaligen Token, der mit Hilfe eines Stifts auf einem Tablet freigeschalten wird, unterschreiben kann. Die Anwendungsfälle reichen von Verträgen über Bestätigungen oder Nachweise bspw. im Versicherungsfall oder Kreditverfahren. Das nachstehende Bild verdeutlicht das Prinzip:

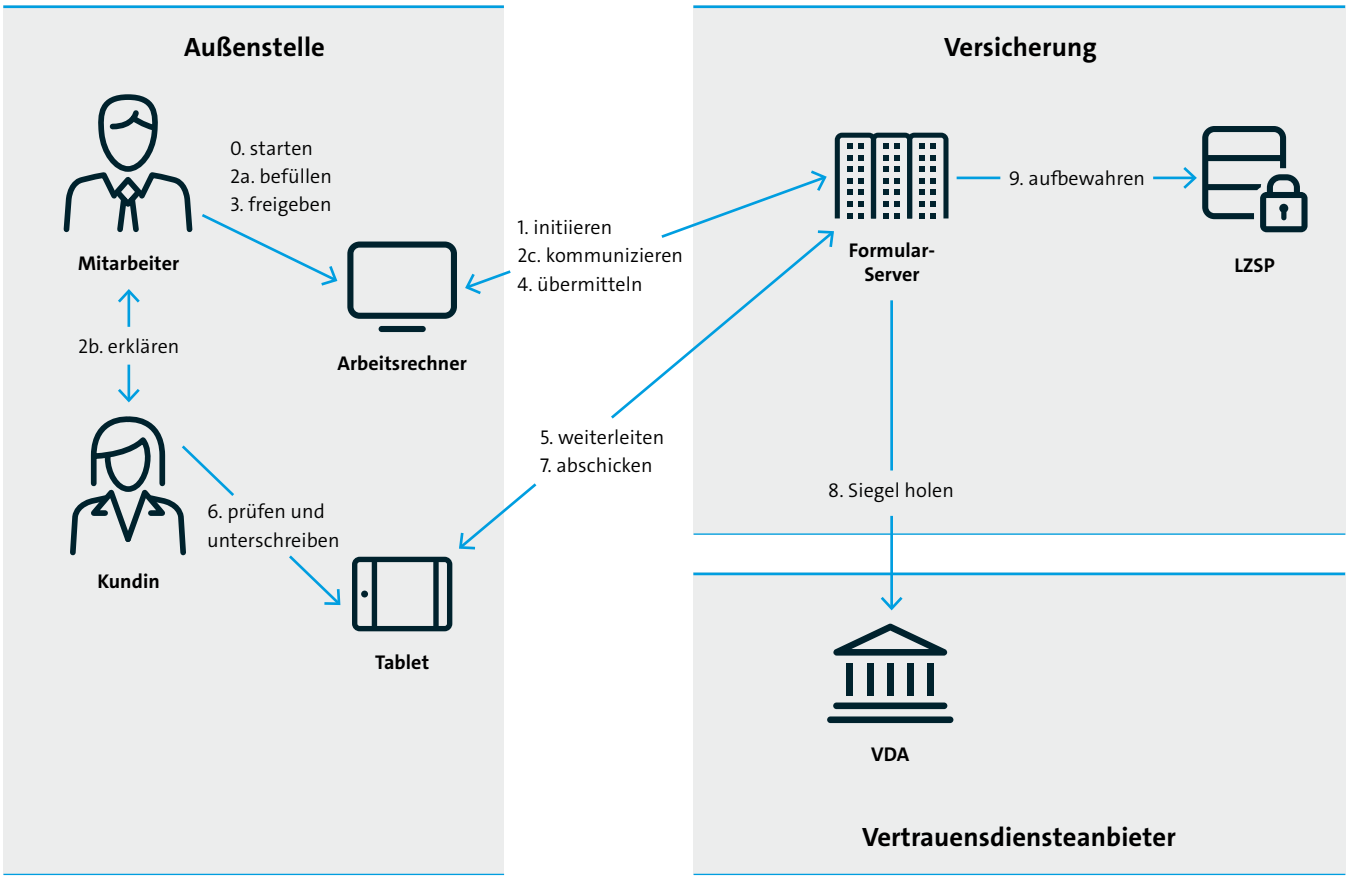

Abbildung 2: Mobile Unterschrift mit Versicherung als Identifizierungsdienstleister, adaptiert von Steffen Schwalm

Eine andere Möglichkeit besteht darin, das Signaturzertifikat nach erfolgreicher Identifizierung in einem HSM in der eigenen Infrastruktur des Anwenders abzulegen und mit einer sicheren Authentifizierung auch mobil auszulösen. Die europäischen Sicherheitsstandards hierzu liegen noch nicht final vor, sodass die derzeit am Markt befindlichen Lösungen möglicherweise noch Anpassungen unterliegen. Andererseits ist die Lösungsvariante insofern interessant, als dass die Zertifikate in der eigenen IT-Umgebung liegen und ein mobiler Zugriff nur auf die eigene Infrastruktur erfolgt und nicht ein Zugang zu einem externen Anbieter wie dem VDA in den o.g. Beispielen notwendig wird. Für besonders sicherheitsrelevante Behörden und Unternehmen so z.B. im Kontext kritische Infrastrukturen, ist dies ein möglicher Weg für mobile, nutzerfreundliche Unterzeichnung von Dokumenten und damit vollständig digitale Transaktionen.

Sofern die qualifizierte elektronische Signatur nicht gesetzlich explizit gefordert ist, lassen sich mobile Szenarien auch mit fortgeschrittenen Signaturen abbilden. In diesem Fall ist nur eine sichere Authentifizierung notwendig. Dies wird bspw. in den zuvor genannten in die Unternehmens-IT integrierten Portallösungen häufig genutzt. Besonders für elektronische Verträge ist nicht in jedem Fall die QES notwendig, sofern sich beide Vertragspartner hierauf einigen und es gesetzlich nicht anders bestimmt ist. Allerdings entfallen die Erleichterungen in der Anerkennung der elektronischen Dokumente vor Gericht, wie dies bei der QES der Fall ist.

Alternativ bietet sich die Nutzung des qualifizierten elektronischen Siegels (QESI). Da dieses sich auf ganze Organisationen bezieht ist auch nur die Identifizierung der Organisation selbst notwendig, nicht des einzelnen Mitarbeiters. In Deutschland wird das Siegel derzeit auf Karte angeboten – aufgrund des Organisationsbezugs jedoch unkritisch. Es muss nur die Karte inklusive Kartenleser in einem sicheren Bereich installiert und vom Siegelverantwortlichen freigeschaltet werden. Im Ergebnis kann jeder berechtigte Nutzer über eine sichere Authentifizierung das Siegel nutzen – was auf einfache Weise auch mobil möglich ist. Der Beweiswert des Siegels – der eindeutige Nachweis von Authentizität und Integrität ist in der eIDAS-Verordnung selbst definiert. Es lässt sich in Deutschland derzeit zwar nicht als Ersatz der Schriftform nutzen, andererseits können so alle anderen Dokumente auf vertrauenswürdige wie nachweisbare Art und Weise bestätigt bzw. gezeichnet werden. So ließen sich bspw. Bescheide, Zeugnisse, Angebote oder auch Verträge bei denen die Schriftform kein Ausschlusskriterium ist, elektronisch siegeln und damit vollständig digital lösen, ohne Nachteile in der Nachweisfähigkeit und Dokumentation. Insbesondere die flächendeckende Nutzung der E-Akte in Behörden wie auch die Abbildung vollständig digitaler behördenübergreifender Prozesse resp. zu Unternehmen und Bürger wird mit dem qualifizierte elektronische Siegel erheblich erleichtert.

3.1.2 Papierbasierte Prozesse

Wo zum Beispiel rechtliche Vorgaben eine Unterschrift erfordern, wird häufig noch auf die Papierform zurückgegriffen. Für das ECM-System bleibt nur das Scannen ggf. mit reduziertem Beweiswert. Abhängig von den rechtlichen Grundlagen muss das Original sogar zusätzlich aufbewahrt werden.

Hier können die eIDAS-Dienste zu einfacheren Lösungen mit reduzierter technischer Komplexität führen. Die Verordnung bietet die Chance, bisher papierbasierte Abläufe einfacher durch digitale Prozesse zu ersetzen. Dadurch lässt sich das heutige Scannen von Papier vermeiden und es entstehen mehr elektronische Objekte.

Beispiele für heute papierlastige Dokumentarten sind beispielweise Verträge, Zeugnisse, Beglaubigungen, Behörden- oder Gebührenbescheide, Leistungsbewilligungen oder Genehmigungen aller Art, Kontoauszüge, Steuerbescheinigungen oder Gehaltsnachweise.

Voraussetzung für den Einsatz des qualifizierten Siegels ist allerdings, dass die rechtlichen Rahmenbedingungen an die eIDAS-Verordnung angepasst werden. Dann können Softwarehersteller von Fachanwendungen, aber auch ECM-Hersteller, entsprechende Lösungen anbieten. Und selbst wenn der fachliche Prozess nicht von den ECM-Herstellern abgedeckt wird, können die neuen elektronischen Objekte in einem ECM-System langzeitarchiviert werden.

3.1.3 Cloud-Dienste

Cloud-Dienste sind kein besonderes Merkmal von ECM-Anbietern, kommen aber auch bei diesen zum Einsatz.[17] Hier können Vertrauensdienste zur Erzeugung von Signaturen, Siegeln und Zeitstempeln, aber auch zur Zustellung elektronischer Einschreiben, zur Validierung und Langzeitbewahrung elektronisch signierter oder gesiegelter Dokumente deutlich einfacher integriert und genutzt werden als Signaturkarten zur Erzeugung qualifizierter elektronischer Signaturen mit Kartenleser am PC. Somit profitieren auch hier die ECM-Hersteller und können entsprechende Mehrwertdienste einfacher anbieten. Insbesondere das Potenzial der kurzfristigen Reaktion auf Lastspitzen ist nicht zu vernachlässigen. Die europaweite Standardisierung der eIDAS-Dienste ist gerade bei Cloud-Lösungen, die international angeboten werden, ein weiterer wichtiger Vorteil, um rechtliche Komplexität zu senken und technische Lösungen zu standardisieren.

3.1.4 Nachweis der Unveränderbarkeit

Eine Kerneigenschaft von ECM-Systemen ist die Sicherstellung der Unveränderbarkeit. Neben dem Einsatz von einmalbeschreibbaren Speichersystemen und entsprechenden Systemfunktionen kommen auch Verfahren zum Einsatz, mit denen die Unveränderbarkeit eines Objektes nachgewiesen werden kann, z.B. durch den Einsatz von Hash-Werten, die beweisen, dass sich ein Objekt nicht verändert hat.

Auch die qualifizierte elektronische Signatur leistet das, allerdings mit vergleichsweise hoher technischer Komplexität. Die personenbezogene Einzelsignatur passt daher nicht besonders gut zu einem massenhaften Nachweisverfahren zur Sicherstellung der Unveränderbarkeit.

Hier können jetzt elektronische Siegel helfen, wie sie in der eIDAS-Verordnung vorgesehen sind. Sie sind nicht personenbezogen und können serverbasiert eingesetzt werden, ggf. auch in Kombination mit Zeitstempel-Diensten (nicht neu durch eIDAS), wenn der Zeitpunkt einer Aktion von besonderer Bedeutung ist.

3.1.5 Interne Freigabeverfahren

Auch wenn die eIDAS-Verordnung eine einfachere technische Integration von rechtlich definierten Unterschriftsverfahren erlaubt, ist bei ihrem Einsatz die Verhältnismäßigkeit zu beachten. Wo keine qualifizierte elektronische Signatur oder ein Siegeldienst erforderlich ist, können auch andere technische Verfahren für den Nachweis der Identität zum Einsatz kommen. Häufig reichen hier Login-Informationen oder Authentifizierungs-Daten aus.

17 Eine ausführliche Darstellung von ECM-Lösungen in der Cloud finden Sie auch in den folgenden Leitfäden: **↗https://www.bitkom.org/noindex/Publikationen/2018/Leitfaeden/Digital-Office/180710-Bitkom-LF-DSGVO.pdf** und **↗https://www.bitkom.org/Bitkom/Publikationen/Geschaeftliche-E-Mails-effizient-in-der-Cloud-managen.html**

Ist z.B. eine interne Rechnungsfreigabe durch einen Klick auf den Genehmigungs-Button und eine dazugehörige Protokollierung ausreichend, werden Anwender keine eIDAS-Dienste einsetzen. Die Authentifizierung (der Benutzer ist tatsächlich derjenige, der er behauptet zu sein) mit Benutzername und Passwort in jeder ERP-Anwendung ist hier gang und gäbe und offensichtlich ausreichend vertrauenswürdig für interne Buchungs-, Freigabe- und Genehmigungsverfahren. Fordern hingehen rechtliche, behördliche oder betriebliche Anforderungen den Einsatz von QES, dann können die eIDAS-Dienste eine Vereinfachung darstellen.

3.1.6 Immer noch erforderlich: Beweiswerterhaltung durch Nachsignatur

Elektronisch signierte Dokumente – ob mit oder ohne eIDAS – können in einem ECM-System elektronisch archiviert werden. Neben der Erfüllung der Ordnungsmäßigkeitsanforderungen, wie Unveränderbarkeit und Nachvollziehbarkeit ist hier auch weiterhin die Anforderung an eine Nachsignatur (Beweiswerterhaltung) vorhanden, wenn sich der Beweiswert der signierten Objekte reduziert. Dies ändert sich auch durch die eIDAS-Dienste nicht. ECM-Anbieter müssen also weiterhin entsprechende Dienste zur Nachsignatur anbieten oder integrieren.

3.2 Einsatzszenarien in Abteilungen und Branchen

Die folgenden Kapitel gehen auf konkrete Einsatzmöglichkeiten in der organisatorischen Praxis ein. Demnach werden die Digitalisierungspotenziale der eIDAS-Dienste durch das Vertrags- und Personalmanagement diskutiert und abschließend im Gesundheitswesen aufgezeigt.

3.2.1 Vertragsmanagement

Vertragsmanagement digitalisieren mit eIDAS
Das Management von Verträgen ist ein unternehmenskritischer Prozess und bringt zahlreiche Herausforderungen mit sich. Es gilt, verschiedene Abteilungen mit unterschiedlicher Aufgabenstellung entlang des gesamten Vertragslebenszyklus zu organisieren. Dabei ist insbesondere eine hohe Transparenz der erfolgsentscheidende Faktor.

Schon bevor die eigentliche Laufzeit beginnt, müssen diverse Abteilungen in den Vertragsvorgang involviert werden: Informationen werden zusammengetragen, Verträge und mitgeltende Unterlagen sind zu erstellen und an den konkreten Vertragsgegenstand anzupassen, es erfolgen interne Abstimmungen sowie Verhandlungen mit dem externen Vertragspartner. Freigabe- sowie Unterschriftenprozesse leiten den Übergang in die aktive Vertragslaufzeit ein. Ohne ein digitales Vertragsmanagement sind Excel-Listen häufig das Mittel der Wahl, um Tätigkeiten und Fristen zu einem Vertrag nachzuverfolgen. Nicht selten werden diese Listen ebenso wie die Ablage der Verträge abteilungsbezogen, wenn nicht sogar redundant organisiert. Das Ergebnis sind aufwändige Recherchen, veraltete Informationsstände und eine ungeeignete Datenbasis für unternehmensweite Analysen des Vertragsbestands. Das Risiko durch verpasste Fristen ist hoch, die Chancen aus möglichen Kostensenkungspotenzialen gering.

Wird das Vertragsmanagement digitalisiert, hat bestenfalls jede berechtigte Abteilung überall und jederzeit schnellen sowie transparenten Zugriff auf bestehende Verträge. Umfangreiche Übersichten mit komfortablen Auswertungsfunktionen heben die relevanten Informationen aus dem Vertragsbestand hervor und erlauben ein sicheres Fristenmanagement.

Das integrierte Vorgangsmanagement erlaubt es, Prozesse unternehmensweit verbindlich zu standardisieren und zwar mithilfe von Phasenmodellen von der Anbahnung bis hin zur Kündigung und Archivierung von Verträgen. Dabei lassen sich auch Verknüpfungen zu vor- oder nachgelagerten Teilprozessen wie Ausschreibungsverfahren oder Projektakten realisieren. Innerhalb der definierten Vertragsphasen unterstützen Aufgabentemplates den Anwender bei der effektiven Organisation seiner Tätigkeiten.

Interne Konversationen (Chat) sowie externe Konversationen (E-Mail) werden direkt innerhalb des Vertragsvorgangs dargestellt und bieten damit die Möglichkeit, auch nach Jahren noch den Grund für bestimmte Entscheidungen nachzuvollziehen. Nicht zuletzt wird jede Aktivität innerhalb des Vertragsvorgangs detailliert in einem Verlaufsprotokoll dokumentiert.

Digitalisierung des Vertragsmanagements

Damit die o.g. Vorteile für ein digitales Vertragsmanagement genutzt werden können, müssen Verträge, die dem Schriftformerfordernis unterliegen unterschrieben oder mit qualifizierter elektronischer Signatur versehen werden. Die qualifizierte Signatur kann durch verschieden sichere Signaturerstellungseinheiten, wie die Smartcard, oder Fernsignaturdienste erfolgen.

eIDAS und Vertragsmanagement mit einem ECM-System

Verträge werden in den meisten Fällen von mindestens zwei oder mehreren Vertragspartnern unterzeichnet, damit benötigt jeder von ihnen ein Signaturzertifikat, das von den unterschiedlichsten Signaturerstellungseinheiten zur Verfügung gestellt werden kann. Seit Inkrafttreten der eIDAS-Verordnung gibt es die Möglichkeit einer Fernsignatur. Dabei wird das Zertifikat von einem Vertrauensdiensteanbieter zur Verfügung gestellt. Bei dieser Art von Bereitstellung des Zertifikates kann die Signatur an jedem Gerät (Desktop, Tablet, Smartphone usw.) ausgelöst werden. Ebenfalls bietet dies den Vorteil, dass die Authentifizierung und Bereitstellung des Zertifikates innerhalb weniger Minuten erfolgen kann, sofern die Teilnehmer noch kein Zertifikat besitzen.

ECM-Systeme bieten den Vorteil, dass in deren Lösungen für Vertragsmanagement oder Workflow-Systeme eine Integration des kompletten Signaturprozesses inklusive der Registrierung abgebildet werden kann.

In dem Folgenden beschriebenen Prozess ist ein möglicher Prozessablauf mit einem ECM-System, einer Signatur-Middleware und einem Vertrauensdiensteanbieter abgebildet.

Exemplarischer Ablauf:

1. Der Anwender wählt den benötigten Vertrag aus und wählt die Option zum Signieren des Dokumentes aus.

2. Es wird geprüft, ob der Anwender bereits ein Zertifikat besitzt oder sich erst noch registrieren muss.

3. Besitzt der Anwender bereits ein Zertifikat, wird das Dokument zur Signatur angezeigt.

4. Der Anwender kann nun ein Signaturfeld in dem jeweiligen Dokument markieren, sofern das Signaturfeld nicht fest vorgegeben ist.

5. Anschließend muss der Anwender sein Passwort zur Signatur eingeben. Der Anwendername wird automatisiert übergeben.

6. Die Signaturmiddleware errechnet den Hashwert des Dokuments und übergibt diesen an den jeweiligen Vertrauensdiensteanbieter.

7. Der Vertrauensdiensteanbieter sendet eine mobile TAN (mTAN) an das Smartphone des Anwenders.

8. Der Anwender gibt die mTAN in das Browserfenster des Anbieters ein.

9. Der Hashwert wird signiert und an die Middleware übergeben.

10. Die Middleware integriert die Signatur in die PDF ggf. inklusive einer Unterschriftengrafik, falls der Anwender die Unterschrift zuvor nicht über einen Stift oder per Finger erzeugt hat.

11. Das Dokument wird dem Anwender inklusive Signaturinformationen dargestellt und archiviert.

3.2.2 Personalmanagement

Das Gesetz zur Regelung der Arbeitnehmerüberlassung (AÜG) regelt die Rechtsbeziehungen zwischen Verleiher und Entleiher von Arbeitskräften und verlangt für den Vertrag zwischen diesen die Schriftform gemäß § 12 Abs. 1 Satz 1 AÜG.

Der Abschluss des Arbeitnehmerüberlassungsvertrages (AÜV) in elektronischer Form ist demzufolge nur mit einer qualifizierten elektronischen Signatur möglich (§ 126 a BGB). Diese Gesetzesänderung zur Zeitarbeit erfordert seit dem 01.04.2017 eine prozesseffiziente Lösung zur AÜV-Unterzeichnung bei Verleiher und Entleiher.

In Deutschland hätte dies vor der Umsetzung der eIDAS-Verordnung bedeutet, dass alle Teilnehmer an diesem Verfahren über eine Smartcard mit Kartenleser und Signaturanwendungskomponente hätten verfügen müssen. Unabhängig davon, wie viele Arbeitnehmerüberlassungsverträge der jeweilige Vertragspartner je Tag, Woche, Monat oder Jahr zu signieren hat.

Ein wesentlicher Vorteil des reinen digitalen Verfahrens liegt in der schnellen, einfachen Kommunikation zwischen den Vertragsparteien. So kann ein solcher Vertrag in wenigen Minuten gemäß den gesetzlichen Anforderungen geschlossen werden. Dies ist insbesondere bei kurzfristigen Engpässen von Bedeutung. In Papierform ist es unmöglich auf vertraglicher Basis noch am gleichen Tag Personal zu erhalten bzw. zu vermitteln.

Dieser Vorteil der digitalen Kommunikation geht jedoch verloren, wenn eine der beiden Parteien nicht über ein qualifiziertes Zertifikat verfügt. Nach dem Signaturgesetz hätten beide Parteien über eine Signaturkarte verfügen müssen. Deren Lieferzeit betrug jedoch mindestens fünf Wochentage und verlangt meist den Gang zur Post, um sich hier via Post-Ident-Verfahren identifizieren zu lassen.

Dank der eIDAS kann hier nun die Fernsignatur eingesetzt werden. Bei diesem Verfahren wird nicht nur die Distribution einer Smartcard eingespart, es ist auch eine Identifikation via Videoident möglich. So kann ein Vertragspartner ein qualifiziertes Zertifikat in weniger als 10 Minuten erhalten und dieses Verwenden. Durch die unterschiedlichen Angebote der Vertrauensdiensteanbieter für Fernsignaturen werden hier auch wirtschaftliche Alternativen zum Erwerb des Zertifikates angeboten. So können Großkonzerne die benötigen Zertifikate ihrer Vertragspartner sponsern um für diese noch eine weitere Motivation für die Digitalisierung zu schaffen.

Webbasierte Vendor-Management-Systeme

Einen besonderen Vorteil bietet diese Lösung insbesondere den Anbietern. Bei diesen entfällt nicht nur der Vertragsaustausch über E-Mail, sondern sie vermeiden auch Anwendungsfehler beim Anwender. Verfügen diese Systeme über eine webbasierte Signaturanwendungskomponente, so können sie darauf achten, dass die richtigen und gültigen Zertifikate zum Einsatz kommen und auch an der richtigen Stelle z.B. sichtbar in einem PDF-Dokument signiert wird.

Ein weiterer Vorteil der webbasierten Vendor-Management-Systeme liegt in der Transparenz des Workflows. Der jeweilige Status wird allen Beteiligten online mitgeteilt. Somit kann schnell reagiert und gehandelt werden.

Anforderung an die Signaturanwendungskomponente

Soll eine Signaturanwendungskomponente (SAK) in einem webbasierten Vendor-Management-System zum Einsatz kommen, so muss auch diese webbasiert sein. Nur so können alle Vorteile der modernen Digitalisierung voll genutzt werden.

Insbesondere ist darauf zu achten, dass die webbasierte Signaturanwendungskomponente beide Verfahren, lokale Signaturkarten und Fernsignaturdienste, über eine Anwendung und API unterstützt. So kann der Entleiher mit Signaturkarte und der Verleiher mit Fernsignaturdienst innerhalb einer Anwendung mit der gleichen grafischen Benutzeroberfläche (GUI) einen Vertrag qualifiziert signieren.

So wie es bei Signaturkarten mehrere Anbieter gab und gibt, so sollten diese Anwendungen auch mehrere Fernsignaturdiensteanbieter unterstützen.

Im Weiteren sollte im Sinne des Datenschutzes darauf geachtet werden, dass die Dokumente die eigentliche Plattform nicht verlassen. Diese kann über eine sogenannte Hash-Signatur erfolgen. Bei dieser wird lediglich der Hashwert des Vertrages an die verwendete lokale Signaturkarte oder den zentralen Fernsignaturdienst gesendet.

Bereits heute haben Anbieter von webbasierten Vendor-Management-Systemen solche Lösungen im Einsatz.

Vorteile auf einen Blick

- Digitale rechtsgültige Arbeitnehmerüberlassungsverträge
- AÜG-Rechtssicherheit
- Kostenreduzierung durch elektronischen Workflow
- Prozesseffizienz: Schnelle Unterzeichnung von AÜV
- Wegfall von Porto-, Papier-, Druck- und Archivierungskosten
- Zeitgleiche Verfügbarkeit aller Dokumente in den Fachabteilungen

3.2.3 Gesundheitswesen

Im deutschen Gesundheitswesen werden jährlich noch circa fünf Milliarden Dokumente auf Papier erstellt. Die Umstellung auf digitale Prozesse bietet ein bedeutendes Einsparpotenzial und eine deutliche Effizienzsteigerung.

Medizinische Einrichtungen können mit elektronischen Signaturen, E-Siegeln und Zeitstempeln sowohl die Entstehung von Papier vermeiden als auch bereits vorhandene Papierdokumente scannen und digitalisieren. Zusätzlich sichern diese Werkzeuge bei der digitalen Archivierung der Dokumente einen hohen Beweiswert.

Galt dieses Themenfeld in der Vergangenheit als unübersichtlich und nicht standardisiert, so hat mit der eIDAS-Verordnung eine EU-weite Vereinheitlichung technischer und rechtlicher Regelungen für elektronische Signaturen, Siegel und Zeitstempel stattgefunden. Neue Verfahren, wie E-Siegel für juristische Personen und die Signatur per Smartphone statt Signaturkarte erhöhen Komfort und Nutzerakzeptanz.

Die elektronische Signatur für natürliche Personen

Die elektronische Signatur ersetzt handschriftliche Unterschriften natürlicher Personen, beispielsweise auf Arztbriefen, Befunden und Laboranforderungen, und entspricht der strengen Schriftform.

Mit einer Signaturkarte kann jede Ärztin und jeder Arzt asynchron, das heißt am Ende des Arbeitstages oder später, in der digitalen Unterschriftenmappe durch einmaliges Stecken seiner Signaturkarte, und einmalige PIN-Eingabe entweder einzelne Dokumente oder Dokumentenstapel rechtssicher unterschreiben. Als Signaturkarte kann beispielsweise der Heilberufsausweis (HBA) gelten.

Alternativ ermöglicht die eIDAS-Verordnung, diesen Vorgang per Fernsignatur mit dem Smartphone, also ohne Signaturkarte, abzuwickeln. So ist es künftig denkbar, dass medizinische Dokumente mittels Smartphone unterschrieben werden. Der private Signaturschlüssel (das qualifizierte Zertifikat) wird dabei zentral beim Vertrauensdiensteanbieter in einer sicheren Signaturerstellungseinheit in Form eines Hardware Security Module (HSM) gespeichert. Ausgelöst wird die Fernsignatur durch eine Zwei-Faktor-Authentifizierung über zwei getrennte physische Kanäle, die sich im Falle der Arztbriefsignatur wie folgt umsetzen ließe:

1. Der Arzt öffnet das zu signierende Dokument, z.B. in seinem ECM-System oder einer Signatursoftware, authentifiziert sich mittels Benutzername und Passwort und betätigt den »Signieren«-Button.

2. Daraufhin erhält der Vertrauensdiensteanbieter eine Signaturanfrage und startet die Authentifizierung, z.B. mittels TAN-SMS.

3. Der Arzt gibt die TAN an seinem Arbeitsbildschirm ein. Der Vertrauensdiensteanbieter überprüft die Eingabe, erzeugt die Signatur und übermittelt sie an den Arzt.

Das elektronische Siegel für juristische Personen
Das elektronische Siegel gemäß eIDAS-Verordnung ist ein EU-weit anerkanntes Signaturwerkzeug für juristische Personen und schützt Dokumente wie Entlassbriefe in der Außenwirkung. Das E-Siegel weist den Ursprung (Authentizität) und die Unversehrtheit (Integrität) elektronischer Dokumente sicher nach. Es ist der digitale Stempel für Einrichtungen des Gesundheitswesens.

Mit einem Siegelserver wird das E-Siegel zentral eingesetzt und sämtlichen dokumentenführenden Prozessen, z.B. zur Direktverarbeitung aus dem ECM oder Krankenhausinformationssystem (KIS), zur Verfügung gestellt. Über ein Rechtemanagement wird festgelegt, dass nur siegelberechtigte Mitarbeiter und Prozesse das E-Siegel auslösen können.

Biometrische Unterschrift in der Patientenaufnahme
Auch die Patientenunterschrift, z.B. auf Wahlbehandlungsverträgen, kann sicher digital abgebildet werden. Die Unterschrift erfolgt dabei wie gewohnt mit einem Stift direkt auf dem Tablet statt auf Papier. Personenindividuelle Unterschriftsmerkmale (biometrische Daten: z.B. Schreibdruck, Schreibgeschwindigkeit, Schreibbeschleunigung) werden mittels Stift und Tablet erfasst und unter Berücksichtigung des Datenschutzes in das PDF-Dokument eingebettet.

Für die Umsetzung komplexer Unterschriftsprozesse kann die biometrische Unterschrift auch mit einer qualifizierten elektronischen Signatur kombiniert werden (Kombi-Signatur).

Dauerhafter Beweiswert mit Zeitstempeln im E-Archiv

Elektronische Patientenakten werden häufig für viele Jahre archiviert. Für die Erhaltung des Beweiswertes über lange Zeiträume hinweg bietet sich der Einsatz von Zeitstempeln gemäß eIDAS-Verordnung an. Dabei werden für die archivierten Datensätze hierarchisch strukturierte Prüfsummen (Hash-Bäume) erzeugt und z.B. einmal täglich mit einem Zeitstempel versehen. Basis hierfür ist der internationale LTANS/ERS-Standard sowie die Technische Richtlinie TR-ESOR des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Auf diese Weise wird der inhaltliche Zustand der Dokumente dauerhaft und nachvollziehbar abgesichert.

4 Zukunftsweisende Initiativen: Vereinheitlichung der Vertrauensdienste

4 Zukunftsweisende Initiativen: Vereinheitlichung der Vertrauens-dienste

Zu einem florierenden ECM-Markt gehört die Verwaltung der digitalen Identität als Markt. Inzwischen gibt es verschiedene Initiativen für eine weitere Vereinheitlichung und Vereinfachung der Vertrauensdienste, auch »Log-in« oder »Datenallianzen« genannt.

Wenn ein Nutzer sich für viele Dienste und Portale, die er über das Internet verwendet, nur einmal statt unzähliger Male anmelden müsste, wäre dies ein großer Schritt hin zu mehr Bedienfreundlichkeit. Für den ECM-Markt wäre dies besonders wichtig, denn damit ließen sich Prozesse rechtssicher digital und über Systemgrenzen hinaus abwickeln.

Folgende Initiativen und Log-In Allianzen haben sich bisher herausgebildet[18]:

Verimi
netID Foundation
SkIDentity
YES
ID4me

18 Die folgende Aufstellung von Log-in-Allianzen erhebt keinen Anspruch auf Vollständigkeit.

5 Anhang

5 Anhang 01
Die eIDAS Werkzeuge im Detail

5.1 Elektronische Dokumente – Grundlage für die Digitalisierung

Definition
Die eIDAS-Verordnung eIDAS-Verordnung versteht unter elektronischen Dokumenten jeden in elektronischer Form gespeicherten Inhalt, insbesondere Text-, Ton-, Bild- und audiovisuelle Aufzeichnungen (Artikel 3, Nr. 35). Um grenzüberschreitende digitale Transaktionen zu ermöglichen, ist es erforderlich, dass diesen Dokumenten europaweit ihre Rechtswirkung, z.B. eine Bestellung auszulösen, nicht deshalb abgesprochen werden kann, weil sie in elektronischer Form, z.B. als E-Mail vorliegen (Artikel 46 eIDAS-Verordnung).

Technische Umsetzung
Für die Gestaltung elektronischer Dokumente sind keine Rahmenbedingungen definiert worden. Sie lassen sich daher mit geringem Aufwand durch jeden erzeugen.

Rechtliche Relevanz
Trotz ihrer Einfachheit entfalten elektronische Dokumente nun auf Basis von Art. 46 eIDAS-Verordnung in der gesamten EU eine Rechtswirkung, die sich aus dem Inhalt des Dokuments ergibt. Sie kann auch gegen den Willen eines anderen durchgesetzt werden, weil elektronische Dokumente in allen Mitgliedsstaaten als Beweismittel vor Gericht zugelassen sind. Dennoch kann es für eine Partei schwierig sein, ihr Recht auf Grundlage eines einfachen elektronischen Dokuments, wie etwa einer Bestell-E-Mail oder einer elektronisch vorliegenden Rechnung, durchzusetzen, denn möglicherweise lassen sich weder die Unversehrtheit der Datei, noch ihr Urheber oder ihr Entstehungs- oder Zugangszeitpunkt zweifelsfrei feststellen.

Daher haben das Europäische Parlament und der Rat mit elektronischen Signaturen, Siegeln, Zeitstempeln und Zustelldiensten Instrumente geschaffen, mit denen diese Mängel beseitigt werden können.

5.1.1 Elektronische Signaturen

Definition
Elektronische Signaturen dienen dazu, elektronische Daten einer natürlichen Person zuzuordnen und den Nachweis zu erbringen, dass diese Daten nach der Signatur nicht mehr verändert wurden. Zu diesem Zweck muss die natürliche Person über ein eigenes Zertifikat mit entsprechendem persönlichen Schlüssel verfügen. Dieses Zertifikat ist so zu schützen, dass der persönliche Schlüssel nur von dieser Person verwendet werden kann.

Zur Speicherung des persönlichen Schlüssels bedarf es für die QES einer zertifizierten sicheren Signaturerstellungseinheit. Daneben können aber auch fortgeschrittene Signaturen eingesetzt werden, z. B. können Behörden auf dieser Basis Zugänge eröffnen. Fortgeschrittene Signa-

turen können außerdem dort eingesetzt werden, wo beispielsweise. Vertragsabwicklungen digitalisiert werden sollen, ohne dass eine gesetzliche Schriftformerfordernis die QES notwendig ist (vgl. § 126a BGB). Fortgeschrittene Signaturen müssen nicht auf einer qualifizierten Signaturerstellungseinheit gespeichert werden.

Die privaten Schlüssel, auch von qualifizierten Zertifikaten, müssen sich nicht mehr im persönlichen Besitz des Schlüsselinhabers befinden (persönliche Smartcard) wie dies noch im Signaturgesetz vorgesehen war. Sie können auch auf einem Hardware Security Module (HSM), welches von einem Vertrauensdiensteanbieter kontrolliert wird, gespeichert sein.[19]

Signaturen, die auf Basis von qualifizierten Zertifikaten erstellt werden, kommen gemäß der eIDAS-Verordnung eIDAS-Verordnung einer händischen Unterschrift gleich (Artikel 25 Abs. 2 eIDAS Verordnung).

Technische Umsetzung
Für den Fall, dass sich der private Schlüssel beim Zertifikatsinhaber befindet, wird die bereits bekannte Technologie mittels einer zertifizierten Smartcard verwendet. Um mit einer solchen Smartcard zu kommunizieren ist ein entsprechender Kartenleser zu verwenden. Dieser wird über die Signaturanwendungskomponente angesprochen. Wird ein Fernsignaturdienst verwendet, so ist über den VDA vor der Verwendung des privaten Schlüssels eine starke Authentisierung des Schlüsselinhabers durchzuführen. Dies erfolgt bei den heutigen Diensten meist über ein mobiles TAN-Verfahren.

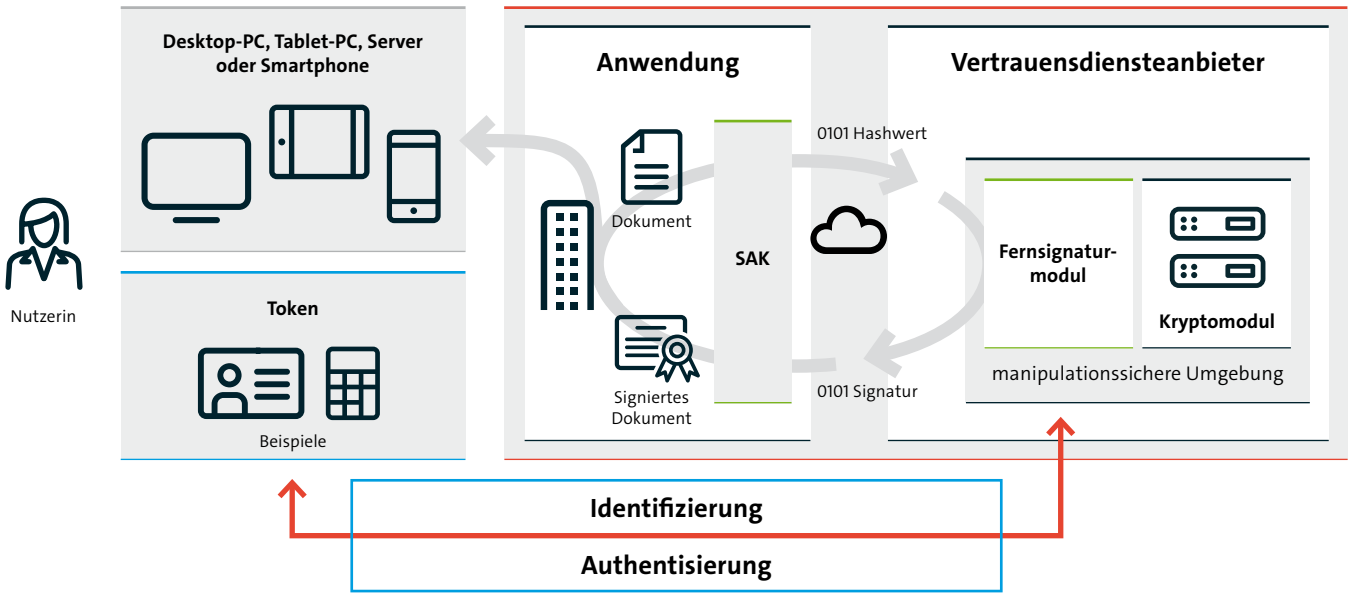

Abbildung 3: Zusammenspiel von VDA und Nutzer für Fernsignatur und -siegel, adaptiert nach intarsys AG

19 Anhang II: Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten.

Die Nutzung eines Fernsignaturdienstes kann durch die Übermittlung des zu signierenden Dokumentes oder dessen Hashwertes an den VDA erfolgen. In der obigen Abbildung wird die Hashwert-Signatur dargestellt. Hierbei wird nicht das Dokument zum Vertrauensdiensteanbieter übermittelt, sondern nur dessen Hashwert. So können auch sensible Dokumente mit einer Fernsignatur signiert werden.

Signaturen sollten auf Basis des Regelwerkes von ETSI in folgenden Formaten gespeichert werden:

- **CAdES**[20] ist eine Erweiterung der Cryptographic Message Syntax (CMS) für eine elektronische Signatur aller Dokumententypen.
- **PAdES**[21] ist eine Menge von Einschränkungen sowie Erweiterungen für PDF-Dateien, um diese für interne elektronische Signaturen anzupassen.
- **XAdES**[22] ist eine Zusammenstellung von Erweiterungen für die W3C-Empfehlung XML-DSig, durch den die Verwendung erweiterter elektronischer Signaturen in XML-Dateien möglich gemacht wird.
- **ASiC**[23] spezifiziert eine Container-Struktur, um signierte Daten gemeinsam mit elektronischen Signaturen in einem Container zu speichern.

Rechtliche Relevanz
Gemäß Artikel 25 Abs. 2 eIDAS-Verordnung eIDAS-Verordnung kommen Signaturen, die auf Basis von qualifizierten Zertifikaten erstellt werden, einer händischen Unterschrift gleich. Weitere Beweisvorschriften trifft die eIDAS-Verordnung eIDAS-Verordnung für qualifizierte Signaturen nicht. Dies mag in der Tatsache begründet sein, dass die qualifizierte elektronische Signatur bereits über die alte Signaturrichtlinie der EU in die jeweilige nationale Gesetzgebung eingeflossen ist.

Mit dem Inkrafttreten des eIDAS-Durchführungsgesetzes am 29.07.2017 wurde zum einen das Signaturgesetz durch das Vertrauensdienstegesetz ersetzt und auch zahlreiche weitere Gesetze geändert. So wurde z.B. der § 126 a BGB genauso geändert wie auch § 371 b ZPO. In den Gesetzen wurde »qualifizierte elektronische Signatur nach dem Signaturgesetz« durch »qualifizierte elektronische Signatur« ersetzt.

Somit erfüllt eine qualifizierte elektronische Signatur nach der eIDAS-Verordnung eIDAS-Verordnung alle Formvorschriften, die auch vorher auf Basis des Signaturgesetzes erfüllt wurden.

20 CMS Advanced Electronic Signatures.

21 PDF Advanced Electronic Signatures.

22 XML Advanced Electronic Signatures.

23 Associated Signature Containers.

5.1.2 Elektronische Siegel

Definition

Elektronische Siegel dienen dazu, den Ursprung und die Unversehrtheit der Daten sicherzustellen. Der Ursprung dieser Daten bezieht sich dabei auf eine juristische Person wie Unternehmen und Behörden. Zu diesem Zweck muss die juristische Person über ein eigenes Zertifikat mit entsprechendem persönlichen Schlüssel verfügen. Dieses Zertifikat ist so zu schützen, dass der persönliche Schlüssel nur von der juristischen Person verwendet werden kann. Im Gegensatz zur elektronischen Signatur ist jedoch diese Sicherung nicht vorgegeben. So können auch interne IT-Sicherungsmaßnahmen die Verwendung des Siegelzertifikats ohne Authentisierung gegenüber der sicheren Signaturerstellungseinheit gewährleisten. Auch wird nicht dargestellt, welche natürliche Person das Siegel »ausgelöst« hat. Damit ist das elektronische Siegel ähnlich wie Siegellack, der auf einer Urkunde aufgetragen wird.

Zur Speicherung des persönlichen Schlüssels benötigt man für ein qualifiziertes Siegel eine zertifizierte sichere Signaturerstellungseinheit. Das kann eine Smartcard wie auch ein Hardware Security Module (HSM) sein. Dabei kann das HSM auch von einem VDA betrieben werden und damit ein »Fernsiegeldienst« angeboten werden. In diesem Fall ist zwar die Nutzung durch die juristische Person sicherzustellen, jedoch keine starke Authentisierung des jeweiligen Nutzers notwendig.

Das elektronische Siegel wird durch eine nachweislich verantwortliche (vertretungsberechtigte) Person der Unternehmung oder Behörde beantragt und auch an diese »ausgeliefert«. Die vertretungsberechtigte Person ist für die Verwendung und ggf. auch für die Sperrung des Siegels verantwortlich.

Neben den qualifizierten Siegeln gibt es auch fortgeschrittene Siegel, diese sind z.B. für die ländergrenzenübergreifenden Behördenkommunikation ausreichend. Sie müssen nicht auf einer qualifizierten Signaturerstellungseinheit gespeichert werden.

Technische Umsetzung

Als sichere Signaturerstellungseinheit sind für elektronische Siegel dieselben zugelassen wie für elektronische Signaturen. Je nach VDA können die Anwender zwischen einer Siegelkarte am Arbeitsplatz oder Server sowie einem HSM, auch als Fernsiegel verfügbar, entscheiden.

Elektronische Siegel sollten auf Basis des Regelwerks von ETSI in folgenden Formaten gespeichert werden:

- **CAdES**[24] ist eine Erweiterung der Cryptographic Message Syntax (CMS) für eine elektronische Signatur aller Dokumententypen.

24 CMS Advanced Electronic Signatures.

- **PAdES**[25] ist eine Menge von Einschränkungen sowie Erweiterungen für PDF-Dateien, um diese für interne elektronische Signaturen anzupassen.

- **XAdES**[26] ist eine Zusammenstellung von Erweiterungen für die W3C-Empfehlung XML-DSig, durch den die Verwendung erweiterter elektronischer Signaturen in XML-Dateien möglich gemacht wird.

- **ASiC**[27] spezifiziert eine Container-Struktur, um signierte Daten gemeinsam mit elektronischen Siegeln in einem Container zu speichern.

Damit unterscheiden sich elektronische Siegel vom Signaturformat von elektronischen Signaturen nicht. Jedoch lassen sich elektronische Siegel durch die Zertifikatsinformationen von elektronischen Signaturen unterscheiden. Dies ist vor allem dann wichtig, wenn Siegel und Signaturen in großen Mengen serverbasiert validiert werden sollen und Formvorschriften bei diesem Prozess beachtet werden müssen.

Rechtliche Relevanz
Gemäß Artikel 35 Absatz 2 eIDAS-Verordnung eIDAS-Verordnung gilt nur für qualifizierte elektronische Siegel die Vermutung der Unversehrtheit der Daten und der Richtigkeit des Herkunftsnachweises dieser Daten. Damit schafft die EU eine Beweisvorschrift für qualifizierte elektronische Siegel, ohne dass diese in der jeweiligen nationalen Gesetzgebung aufgenommen werden muss.

Da die eIDAS-Verordnung eIDAS-Verordnung sich jedoch nicht in nationale Formvorschriften einmischt, müssen elektronische Siegel ggf. in die nationalen Gesetzgebung aufgenommen werden. Dies ist mit dem Inkrafttreten des eIDAS-Durchführungsgesetzes am 29.07.2017 teilweise geschehen. So wird nun in § 19 Absatz 5 Satz 2 der Vergabeverordnung Verteidigung und Sicherheit sowie in § 28 Absatz 3 Satz 2 der Konzessionsvergabeverordnung das elektronische Siegel aufgeführt. Von einer solchen Änderung waren insgesamt vier Verordnungen betroffen. Sicherlich ist es wünschenswert, dass diese Möglichkeit noch in wesentlich mehr Gesetzen und Verordnungen Berücksichtigung finden.

Bereits berücksichtigt wurde das elektronische Siegel in der BSI TR RESISCAN als Integrationssicherung für das ersetzende Scannen.

Auch in Kombination mit einer qualifizierten elektronischen Signatur kann das qualifizierte elektronische Siegel auch heute bereits mehrwertbringend eingesetzt werden. So kann über das qualifizierte elektronische Siegel bewiesen werden, dass der Unterzeichner mit der qualifizierten elektronischen Signatur im Namen des Unternehmens gehandelt hat. So würde es z.B. die

25 PDF Advanced Electronic Signatures.

26 XML Advanced Electronic Signatures.

27 Associated Signature Containers.

Antwort auf die Frage liefern, ob der unterschreibende Richter auch zum Zeitpunkt seiner Unterschrift Richter am entsprechenden Gericht war.

5.1.3 Zeitstempel

Definition
Elektronische Zeitstempel dienen dazu, elektronische Daten einer eindeutigen, ggf. gesetzeskonformen, Zeit zuzuordnen und den Nachweis zu erbringen, dass diese Daten nach dem Aufbringen des Zeitstempels nicht mehr verändert wurden. Zu diesem Zweck betreibt der Vertrauensdiensteanbieter einen Zeitstempelserver, der aus drei Komponenten besteht:

- Einer Uhr (NTP Server), die nachweislich die korrekte Uhrzeit liefert und deren Betrieb nicht manipuliert werden kann.
- Einem KeyStore (HSM oder Kartenrack), mit einem Zertifikat mit dem die abgefragte Uhrzeit »signiert« werden kann. Die »Qualität« dieses Zertifikates bestimmt die »Qualität« des Zeitstempeldienstes.
- Einem Timestamp-Server, der Uhrzeit und Signatur entsprechend den Standards mit den »gelieferten« Daten verbindet.

Zur Speicherung des persönlichen Schlüssels des Zeitstempelzertifikates wird eine zertifizierte sichere Signaturerstellungseinheit benötigt. Diese kann eine Smartcard wie auch ein Hardware Security Module (HSM) sein.

Timestamp-Server liefern das Ergebnis üblicherweise im Zeitstempelprotokoll RFC 3161, welches dann durch eine Signaturanwendungskomponente über zwei Wege als Zeitstempel verwendet wird:

- Als eigenständiger Zeitstempel zum Dokument-Beleg dafür, dass die Daten zu dieser Zeit so vorgelegen haben.
- Als in der Signatur oder Siegel eingebetteter Zeitstempel. Dies ist ein Beleg dafür, dass die vorliegenden Daten vom entsprechenden Nutzer zu diesem Zeitpunkt signiert wurden.

Technische Umsetzung
Als »Uhr« werden zertifizierte NTP-Server eingesetzt, die manipulationsfrei arbeiten. Hierfür verfügen Sie zum einen über einen Zugriffsschutz und zum anderen vergleichen sie die selber generierte Zeit mit mindestens einer weiteren Referenzzeit. Hierzu wird häufig der Zeitzeichensender DCF77 verwendet.

Wichtig für die universelle Verwendung eines Zeitstempels mit Ortszeit ist die Ergänzung um die Angabe des Offsets zu UTC als numerische Angabe oder per Name wie MEZ bzw. MEST gemäß

ISO 8601. Nur so kann ein vollständiger Vergleich von Zeitstempeln realisiert und das Berechnen von Zeitdifferenzen zwischen zwei Zeitstempeln ermöglicht werden.

Für den persönlichen Schlüssel des Zeitstempelzertifikats sind dieselben sichere Signaturerstellungseinheiten zugelassen, wie für elektronische Signaturen.

Zeitstempel sollten auf Basis des Regelwerkes von ETSI in folgenden Formaten gespeichert werden:

- **CAdES-T** ist eine Erweiterung der Cryptographic Message Syntax (CMS) und fügt vertrauenswürdige Zeitstempel ein.
- **PAdES** ist eine Menge von Einschränkungen sowie Erweiterungen für PDF-Dateien, um diese für interne elektronische Zeitstempel anzupassen.
- **XAdES-T** ist eine Zusammenstellung von Erweiterungen für die W3C-Empfehlung XML-DSig, durch den die Verwendung elektronischer Zeitstempel in XML-Dateien möglich gemacht wird.
- **ASiC** spezifiziert eine Container-Struktur, um Daten gemeinsam mit elektronischen Zeitstempeln in einem Container zu speichern.

Zeitstempel finden insbesondere bei der technischen Umsetzung von Prüf- und Bewahrungsdiensten eine Verwendung.

So wird die Antwort nach der Gültigkeit eines Zertifikates vom Vertrauensdiensteanbieter mit einem Zeitstempel versehen, der die Zeit der Anfrage beinhaltet (OCSO-Response). Aber auch zur Beweiswerterhaltung von Signaturen werden Zeitstempel verwendet. So wird damit dokumentiert, dass schwächer gewordene Parameter und Algorithmen rechtzeitig gesichert wurden (RFC 4998-Evidence Record Syntax).

Rechtliche Relevanz
Gemäß Artikel 41 Absatz 2 eIDAS-Verordnung gilt für qualifizierte elektronische Zeitstempel die Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben sind, sowie der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten, ohne dass diese in die jeweiligen nationalen Gesetzgebung aufgenommen werden muss.

Damit enthält ein qualifizierter elektronischer Zeitstempel auch außerhalb des ehemaligen Signaturgesetzes eine juristische Bedeutung.

Da die eIDAS-Verordnung eIDAS-Verordnung sich jedoch nicht in nationale Formvorschriften einmischt, müssen elektronische Zeitstempel ggf. in die nationale Gesetzgebung aufgenommen werden. Dies ist mit dem Inkrafttreten des Gesetzes zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz) am 29.07.2017, nicht geschehen.

Bereits Berücksichtigt wurde der elektronische Zeitstempel in der BSI TR RESISCAN als Integrationssicherung für das ersetzende Scannen.

5.1.4 Elektronische Einschreib- und Zustelldienste

Definition
Hier handelt es sich um einen elektronischen Dienst, der in der Regel gegen Entgelt erbracht wird. Dieser ermöglicht die Übermittlung von Daten zwischen Dritten mit elektronischen Mitteln und erbringt einen Nachweis über die Handhabung der übermittelten Daten. Dazu zählt der Nachweis über Absendung und Empfang der Daten, und der Nachweis darüber, wie die die übertragenen Daten vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung geschützt sind. In Deutschland regelt das De-Mail-Gesetz seit 2011 Dienste für den sicheren, vertraulichen und nachweisbaren elektronischen Geschäftsverkehr. Mit den Versandoptionen Versandbestätigung und Eingangsbestätigung erfüllt eine De-Mail die Voraussetzungen für einen Dienst zur Zustellung elektronischer Einschreiben.

Für die versandten Nachrichten legt die eIDAS-Verordnung eine besondere Rechtswirkung fest (Artikel 43 Abs. 2): Es besteht die Vermutung der Unversehrtheit der Daten, der Absendung dieser Daten durch den identifizierten Absender und des Empfangs der Daten durch den identifizierten Empfänger. Weiterhin besteht die Vermutung der Korrektheit des Datum und der Uhrzeit der Absendung und des Empfangs, wie sie von dem qualifizierten Dienst angegeben werden. Anbieter bekommen den Qualifikationsstatus von der zuständigen Behörde verliehen, nachdem sie die Konformität zu den entsprechenden Anforderungen aus der Verordnung nachgewiesen haben.

Technische Umsetzung
Die technischen Anforderungen sind vielschichtig geregelt. In Deutschland ist vor allem das De-Mail-Gesetz seit 2011 für Dienste für den sicheren, vertraulichen und nachweisbaren elektronischen Geschäftsverkehr einschlägig. Wie die De-Mail-Diensteanbieter die Anforderungen an qualifizierte Dienste zur Zustellung elektronischer Einschreiben nach eIDAS-Verordnung erfüllen, ist im Dokument zur technischen Umsetzung bei De-Mail vom BSI detailliert aufgeführt.[28]

Rechtliche Relevanz
Die rechtliche Relevant und auch die Rechtwirkung eines qualifizierten Diensts für elektronische Einschreiben umfasst mehrere rechtlich relevante Vermutungen, wie sich aus Artikel 43 Absatz 2 eIDAS-Verordnung eIDAS-Verordnung ergeben:

Es besteht die Vermutung der Unversehrtheit der Daten, der Absendung dieser Daten durch den identifizierten Absender und des Empfangs der Daten durch den identifizierten Empfänger, sowie der Korrektheit des Datums und der Uhrzeit der Absendung und des Empfangs, wie sie von dem qualifizierten Dienst für die Zustellung elektronischer Einschreiben angegeben werden.

28 BSI (2016): Erfüllung der Anforderungen an qualifizierte Dienste für die Zustellung elektronischer Einschreiben nach eIDAS-Verordnung durch De-Mail-Dienste. Link: ↗**https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/eIDAS/Anforderungen_eIDAS_De-Mail.pdf?__blob=publicationFile&v=6**

5.1.5 Validierungs- und Bewahrungsdienste

Definition
Die Validierungs- und Bewahrungsdienste ermöglichen es, die Vertrauenswürdigkeit von qualifizierten elektronischen Signaturen und qualifizierten elektronischen Siegeln über den Zeitraum ihrer technologischen Geltung hinaus zu verlängern. Sie sind elektronische Dienste, die in der Regel gegen Entgelt erbracht werden. Validierungs- und Bewahrungsdienste ermöglichen die Bewahrung von elektronischen Signaturen, Siegeln oder Zertifikaten, die diese Dienste betreffen. Der Dienst selbst kann nur von qualifizierten Vertrauensdiensteanbietern erbracht werden. Betreiben Behörden oder Unternehmen selbst einen Bewahrungsdienst so bezieht sich dieser auf einen geschlossenen Benutzerkreis und liegt somit nicht im Geltungsbereich der eIDAS-Verordnung. Der Bewahrungsdienst betrifft z.B. die oben genannte Fernsignatur.

Technische Umsetzung
Der Bewahrungsdienst betrifft z.B. die oben genannte Fernsignatur. Der private Signaturschlüssel wird durch einen Vertrauensdiensteanbieter auf einem zertifizierten Hardware Security Module (HSM) gespeichert und kann dann z.B. via Smartphone genutzt werden. Mit der Technischen Richtlinie BSI-TR 03125 »Beweiswerterhaltung kryptographisch signierter Dokumente« hat das Bundesamt für Sicherheit in der Informationstechnik auch bereits einen Leitfaden zur vertrauenswürdigen Speicherung von Dokumenten zur rechtswirksamen Beweiswerterhaltung erarbeitet.[29]

Rechtliche Relevanz
Durch die langzeitsichere Archivierung von Dokumenten kann die Beweiswerterhaltung sichergestellt werden.

5.1.6 Zertifikate für Website-Authentifizierung

Definition
Zertifikate für die Website-Authentifizierung (verkürzt: Webseiten-Zertifikate) dienen der Absicherung der Identität von Webseiten und der Realisierung einer verschlüsselten Kommunikation zwischen dem Client-Rechner und dem Server, welcher die Webseite hosted (Webserver). Webseiten-Zertifikate verknüpfen die Webseite mit der Identität einer natürlichen oder juristischen Person, der die Webseite gehört. Sie entsprechend technisch einem TLS-Zertifikat.[30]

Webseiten-Zertifikate werden durch einen VDA erstellt, überprüft und validiert. Webseiten-Zertifikate sind »qualifizierte Zertifikate für die Website-Authentifizierung« im Sinne von Artikel 3 Satz 1 Nr. 38 eIDAS-Verordnung, wenn sie von einem qualifizierten VDA ausgestellt wurden. Damit gehen alle Anforderungen einher, die ein qualifizierter VDA erfüllen muss, um qualifizierte Zertifikate erstellen zu dürfen. Die Mindestinhalte eines solchen Zertifikats werden im Anhang IV der eIDAS-Verordnung definiert.

29 BSI (2018): BSI Technische Richtlinie 03125: Beweiswerterhaltung kryptographisch signierter Dokumente. Link: ↗https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html

30 Transport Layer Security-Zertifikat.

Technische Umsetzung
Das wesentliche Element für eine verschlüsselte Webseite ist ein Schlüsselpaar mit zugehörigem TLS-Zertifikat. Mit Hilfe des TLS-Zertifikats werden zwei Funktionen realisiert, die Transportsicherung und die Identitätsbestätigung. Sowohl das Schlüsselpaar als auch das Zertifikat sind auf dem Webserver hinterlegt. Es kommt i.d.R. keine HSM-Technologie zur sicheren Speicherung des privaten Schlüssels zum Einsatz.

Das Profil eines Webseitenzertifikats wird in der Norm ETSI EN 319 412-4 definiert. Die Prüfanforderungen entsprechen weitestgehend denen, die an ein EV[31]-Zertifikat gestellt werden.

Rechtliche Relevanz
Die eIDAS-Verordnung schreibt einem qualifizierten Webseiten-Zertifikat keine unmittelbare Rechtswirkung zu. Gleichzeitig kann aber zunächst bei jedem qualifizierten Webseiten-Zertifikat von der Richtigkeit der Identität der Webseiten-Domain als auch des Besitzers des Webseiten-Zertifikats ausgegangen werden, da die der Zertifikatsausstellung zugrundliegenden Prüfprozesse sehr umfangreich sind.

Qualifizierte Webseiten-Zertifikate werden zunehmend durch die EU und ihren Institutionen in digitalen Geschäftsprozessen vorgeschrieben. Das bisher wichtigste Anwendungsgebiet ist die Absicherung der Identität elektronischer Dienste und der Kommunikation zwischen Banken, Zahlungsdienstleistern und FinTechs im Rahmen der EU-Zahlungsdienstleistungsrichtlinie PSD2.

31 Extended Validated.

Anhang 02
Das »eIDAS-Vertrauenssystem«

Das »eIDAS-Vertrauenssystem« besteht aus verschiedenen Organisationen, die vor dem Hintergrund wohldefinierter rechtlicher und regulatorischer Rahmenbedingungen miteinander interagieren, um das Vertrauen im »eIDAS-Ökosystem« aufrecht zu erhalten.

Insgesamt werden durch das »eIDAS-Vertrauenssystem« letztlich signierte XML-basierte Listen mit Vertrauensankern (Vertrauenslisten) für die verschiedenen Vertrauensdienste im eIDAS-Ökosystem verwaltet, mit denen schließlich die qualifizierten Zertifikate, Signaturen und Siegel der Nutzer und Vertrauensdienste, sowie die Zeitstempel und beispielsweise Zustellbestätigungen der entsprechenden Anbieter von jedermann geprüft werden können.

Die grundsätzlichen Anforderungen an diese Vertrauenslisten sind im Durchführungsbeschluss (EU)2015/1505 spezifiziert, der wiederum auf den bei ETSI entwickelten Standard TS 119 162 (v2.1.1) verweist.

Wie in der Abbildung dargestellt, umfasst das »eIDAS-Vertrauenssystem«

- die Europäische Kommission[32],
- die Europäische Kooperation für Akkreditierung[33],
- die EU-Mitgliedstaaten[34],
- die nationalen Akkreditierungsstellen (National Accreditation Bodies, NAB), die von den Mitgliedstaaten und der EA gemäß der Verordnung (EG) Nr. 765/2008 ernannt werden, wie z.B. die Deutsche Akkreditierungsstelle (DAkkS) in Deutschland,
- die von den Mitgliedstaaten benannten Aufsichtsbehörden gemäß Artikel 17 eIDAS-Verordnung, wie z.B. die Bundesnetzagentur (BNetzA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland,
- die Europäische Agentur für Netz-und Informationssicherheit (ENISA), die gemäß Artikel 19 Absatz 3 eIDAS-Verordnung von den nationalen Aufsichtsbehörden einen Jahresbericht mit gemeldeten Sicherheitsvorfällen erhält,
- die Konformitätsbewertungsstellen (Conformity Assessment Bodies, CAB) nach Artikel 3 Nr 18 eIDAS-Verordnung, die von den nationalen Akkreditierungsstellen gemäß der EU-Verordnung (EG)765/2008 für eIDAS-spezifische Konformitätsbewertungen akkreditiert worden sind,

32 European Commission, EC.

33 European Accrediation, EA.

34 Member State, MS.

- die (qualifizierten) Vertrauensdiensteanbieter gemäß (2014/910 / EU) Art. 3 Nr. 19 und 20 eIDAS-Verordnung, die einen oder mehrere eIDAS-Dienste bereitstellen.

Gemäß Artikel 22 Absatz 3 der eIDAS-Verordnung übermitteln die Mitgliedsstaaten »der Kommission unverzüglich Informationen über die für die Erstellung, Führung und Veröffentlichung der nationalen Vertrauenslisten verantwortlichen Stellen, den Ort der Veröffentlichung der Listen, die zur Unterzeichnung oder Besiegelung der Vertrauenslisten verwendeten Zertifikate und alle etwaigen Änderungen dieser Informationen.« Die deutsche Vertrauensliste wird von der Bundesnetzagentur in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik verwaltet.

Wie in Artikel 22 Absatz 4 der eIDAS-Verordnung festgelegt, veröffentlicht die Europäische Kommission ihrerseits eine eigene, signierte oder gesiegelte Vertrauensliste, die auf die verschiedenen Vertrauenslisten aller Mitgliedsstaaten verweist.

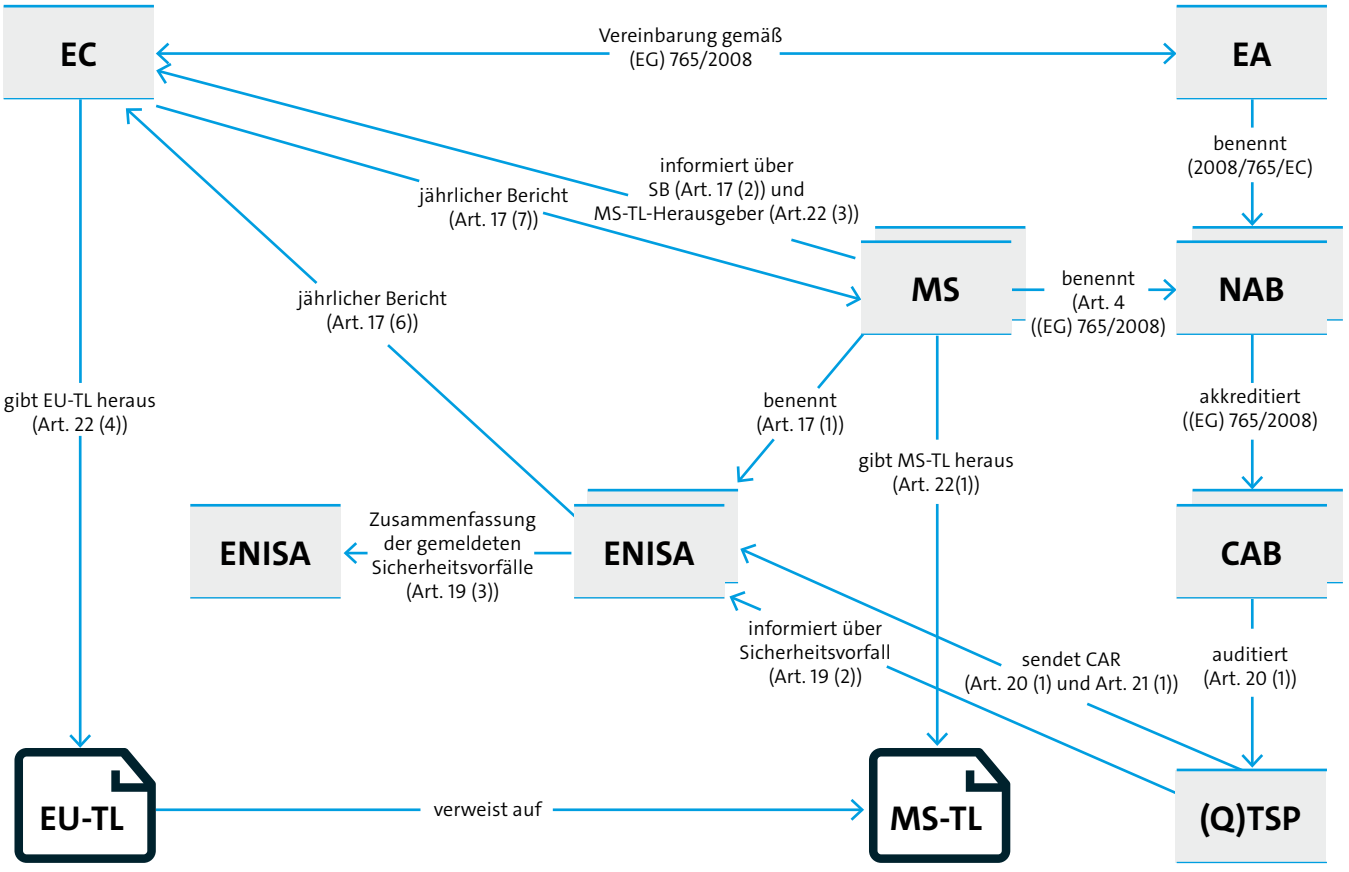

Abbildung 4: Das eIDAS-Vertrauenssystem, adaptiert nach Dr. Detlef Hühnlein

Um in die MS-TL aufgenommen zu werden, muss ein Vertrauensdiensteanbieter eine Konformitätsbewertungsstelle (CAB) beauftragen, die Konformität des vom TSP angebotenen Vertrauensdienstes mit der eIDAS-Verordnung zu überprüfen. Das Ergebnis wird in Form eines »Konformitätsbewertungsberichts«[35] festgehalten, der zusammen mit einer entsprechenden Mitteilung gemäß Artikel 21 eIDASVerordnung an die zuständige Aufsichtsbehörde geschickt wird. Die Aufsichtsbehörde prüft den CAR und fügt, sofern alles in Ordnung ist, die entsprechenden Informationen und Vertrauensanker, die zum neuen Vertrauensdienst gehören in die MS-TL ein.

Durch das ausgeklügelte »eIDAS-Vertrauenssystem« ist sichergestellt, dass die von Vertrauensdiensteanbietern in ganz Europa bereitgestellten Dienste tatsächlich Ihrem Namen gerecht werden und so sicher, zuverlässig und vertrauenswürdig sind, dass sie als Grundlage für rechtsverbindliche elektronische Transaktionen genutzt werden können.

35 Conformity Assessment Report, CAR.

Bitkom vertritt mehr als 2.600 Unternehmen der digitalen Wirtschaft, davon gut 1.800 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom