BUNDESDRUCKEREI

WHITEPAPER

Durchgängig digital.

mit Fernsignatur und elektronischem Siegel

Geschäftsprozesse optimieren, Kosten senken,
Kundenzufriedenheit erhöhen

Sichere
Organisation

Management Summary

Handschriftlich unterschriebene Dokumente sind eines der größten Hemmnisse für durchgängig elektronische Workflows. Dabei gibt es mit der digitalen Signatur eine technisch ausgereifte und rechtssichere Alternative. Deren Verbreitungsgrad ist jedoch sehr gering. So kommen – laut einer aktuellen Studie der Bundesdruckerei – digitale Signaturen in nur 16 Prozent der deutschen Unternehmen zum Einsatz.

Das wird sich in Zukunft schnell ändern. Impulsgeber ist die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS), die geltendes Recht in allen 28 EU-Mitgliedsstaaten ist. Sie will erreichen, dass Unternehmen, Bürger und Behörden untereinander Geschäfte und E-Government-Leistungen komfortabel, medienbruchfrei und zu geringen Kosten tätigen können.

Um dieses Ziel zu erreichen, schafft die EU-Verordnung mit der Fernsignatur ein vereinfachtes Verfahren für die elektronische Unterschrift und mit dem elektronischen Siegel ein neues Werkzeug um die Herkunft eines Dokuments rechtssicher zu belegen.

Die Fernsignatur ermöglicht es, eine elektronische Unterschrift – ohne Signaturkarte und Kartenlesegerät – auch aus der Ferne auszulösen, zum Beispiel über mobile Endgeräte wie Tablets und Smartphones. Bei der Fernsignatur-Lösung mit sign-me geschieht dies durch die Eingabe von Benutzername und Passwort sowie einer zugestellten SMS-TAN.

Die Einsatzgebiete der Fernsignatur erstrecken sich auf die unterschiedlichsten Branchen und Bereiche – vom Vertragsmanagement über Online-Kredite und digitale Versicherungsdienstleistungen bis hin zur E-Vergabe öffentlicher Aufträge und zur Förderung der elektronischen Patientenakte.

Ergänzt werden digitale Signaturen durch **elektronische Siegel,** die den Firmenstempel und das Behördensiegel ins digitale Zeitalter überführen. Elektronische Siegel beziehen sich auf juristische Personen, also auf eine Organisation. Sie dienen als Herkunftsnachweis und zum Schutz der Daten.

Aktuelle Siegel-Lösungen basieren auf einer Siegelkarte, die mit vorhandenen Signatur-Infrastrukturen aus Hardware- und Softwarekomponenten eingesetzt werden kann.

Typische Anwendungsszenarien sind die rechtssichere elektronische Archivierung und Rechnungsverarbeitung, die Absicherung der elektronischen Kommunikation sowie das digitale Ausstellen von Kontoauszügen, Urkunden oder Steuer- und Rentenbescheiden.

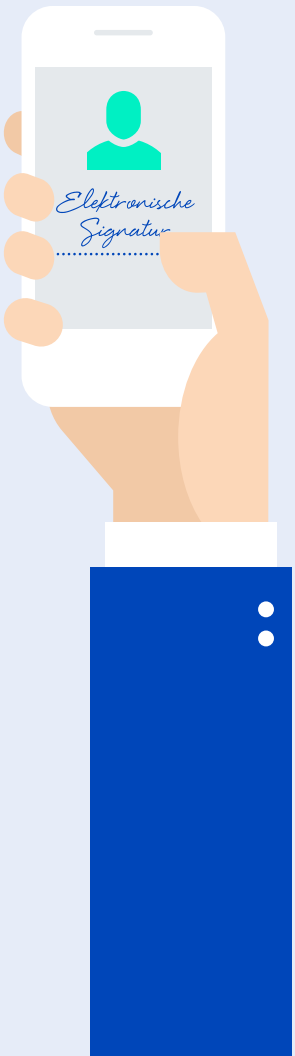
Die Effizienzgewinne können nach Angaben der estnischen Regierung, die flächendeckend digitale Signaturen für E-Government-Dienste einsetzt, bis zu zwei Prozent des jährlichen Bruttoinlandsprodukts betragen. In Deutschland wären das umgerechnet 60 Milliarden Euro.

Deutschland im Jahr 2018

Ab jetzt zählt jede Minute. Die Lage ist ernst. Nachdem der Patient stabilisiert wurde, beginnt die Fahrt im Rettungswagen. Die Notfalldokumentation erstellt der behandelnde Arzt sofort auf seinem Tablet-PC. Dazu gehören auch zentrale Informationen für die Weiterbehandlung – wie die Erstdiagnose und verabreichte Medikamente. Per Mausklick übermittelt der Notarzt das Dokument elektronisch an die Klinik. Beim Eintreffen des Patienten sind die Kollegen der Notaufnahme bestens vorbereitet. Die Behandlung beginnt ohne Verzögerung und mit optimaler Informationsversorgung. Währenddessen leistet der Notarzt die gesetzlich geforderte Unterschrift bequem digital mit Tablet und Smartphone.

Ortswechsel. Im Büro von Frau Cyan. Die Geschäftsführerin der Hedracel AG ist zufrieden. Gerade hat sie den langerhofften Großauftrag für Batteriekomponenten gewonnen. In Zeiten papiergebundener Vertragsabläufe müssten nun viel Zeit und Ressourcen investiert werden. Heute lässt sich der Vertragsprozess komplett medienbruchfrei abbilden. Die rechtsgültige digitale Signatur kann von beiden Geschäftsführern einfach und schnell elektronisch ausgelöst und anschließend archiviert werden. Ein Prozess, der früher mindestens eine Woche in Anspruch genommen hat, ist nun in weniger als 20 Minuten erledigt.

Max – online auf der Couch. Die Erfüllung seines Wunschtraums, der Kauf eines Mountainbikes, steht kurz vor der Verwirklichung. Für einen Teil des Geldes benötigt er einen Ratenkredit. Früher wäre das ein umständlicher Vorgang gewesen: PostIdent-Dokument ausfüllen, Kreditantrag ausdrucken und unterschreiben, dann alles zur Post bringen und auf die schriftliche Zusage warten. Nun braucht Max dafür nur wenige Minuten. Auf der Website des Kreditinstituts füllt er den Antrag aus und erlaubt der Bank den einmaligen Blick auf seine Kontoumsätze. Innerhalb von 30 Sekunden erhält er den positiven Bescheid. Direkt im Anschluss legitimiert er sich bei einem Identifizierungsdienstleister und unterzeichnet den Vertrag mit seiner elektronischen Unterschrift. Schon in 24 Stunden wird er über den Kreditbetrag verfügen können.



Lisa – am PC auf Jobsuche. Eine interessante Tätigkeit bei einem Maschinenbauunternehmenim europäischen Ausland weckt Lisas Interesse. Für den Bewerbungsprozess werden beglaubigte Versionen der Zeugnisse und Urkunden gefordert. Was früher ein langwieriger Prozess war, mit Besuchen beim Bürgerbüro und im Universitätssekretariat, ist für Lisa schnell erledigt. Denn sowohl ihre Diplomurkunde als auch die Zeugnisse ihrer bisherigen Arbeitgeber liegen digital mit einem elektronischen Siegel versehen vor. Aufgrund des EU-weiten Geltungsbereichs elektronischer Siegel und der einfachen Verifizierung per Mausklick, akzeptiert das Maschinenbauunternehmen Lisas Unterlagen.

Sie halten die vier Szenarien für Zukunftsmusik? In diesem Whitepaper wollen wir Sie vom Gegenteil überzeugen. Unsere These:

Fernsignatur und elektronisches Siegel werden zu den zentralen Werkzeugen der digitalen Transformation.

1. ELEKTRONISCHE SIGNATUREN ALS DIGITALISIERUNGSBESCHLEUNIGER

Durch die digitale Transformation können Organisationen effizienter werden und Kosten sparen. Getrieben wird dieser Trend zur Digitalisierung auch durch gestiegene Kundenanforderungen. Erwartet wird, dass Produkte und Dienstleistungen komplett elektronisch erhältlich sind.

Dem wachsenden Wunsch nach elektronischen Dokumenten widerspricht die Realität in vielen Organisationen. Woran liegt das? Eine zentrale Antwort lautet: an rechtlich vorgeschriebenen oder unternehmensintern festgelegten handschriftlichen Unterschriften. So fand der IT-Fachverband AIIM (Association for Information and Image Management) in einer weltweiten Studie heraus, dass 50 Prozent der Unternehmen Dokumente nur wegen der benötigten Unterschrift ausdrucken.[1]

Einen Ausweg aus dieser ineffizienten Unterschriftenpraxis bietet der Einsatz digitaler Signaturen. Denn nur durch elektronisches Unterschreiben lassen sich Geschäftsprozesse konsequent medienbruchfrei gestalten.

Daten und Fakten

75 %

der Unternehmen geben an, dass die Hälfte ihrer Prozesse oder mehr papierbasiert ablaufen.
QUELLE: Bitkom, Unternehmen reduzieren ihren Papierverbrauch, April 2017

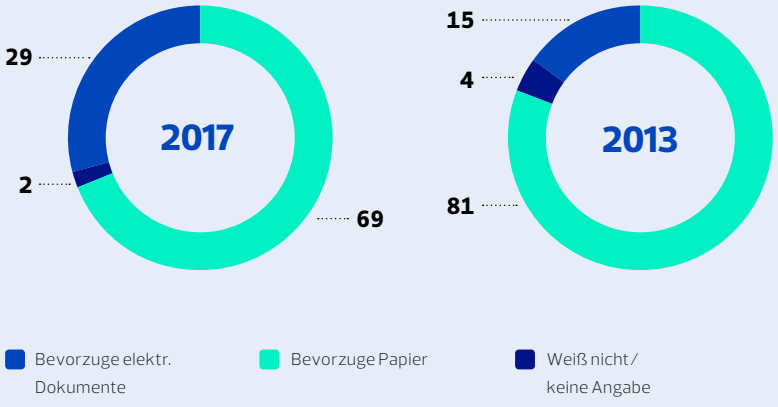
Daten und Fakten

25 %

der Internetnutzer können sich bereits vorstellen, online einen Kredit aufzunehmen oder eine Versicherung abzuschließen.
QUELLE: Bitkom, Digital Banking, Juni 2016

Wunsch nach elektronischen Dokumenten wächst[2]

Ein Drittel der Bundesbürger möchte persönliche Dokumente wie Verträge und Rechnungen lieber digital zugeschickt bekommen (29 Prozent). Das bedeutet gegenüber 2013 (15 Prozent) eine Verdoppelung.



Frage: Bekommen Sie persönliche Dokumente wie Rechnungen oder Verträge lieber als Brief oder digital als E-Mail zugeschickt? Angaben in Prozent

1 AIIM White Paper, E-Signatures in Europe, 2016

2 Bitkom, Wunsch nach elektronischen Dokumenten wächst, März 2017

Daten und Fakten

Nur in

16 %

der Unternehmen existieren die Voraussetzungen für das digitale Unterschreiben.

QUELLE: Bundesdruckerei, IT-Sicherheit in deutschen Unternehmen, Juni 2017

Von allen Signaturtypen besitzt die sogenannte Qualifizierte Elektronische Signatur (QES) das höchste Sicherheitsniveau. Sie entspricht der gesetzlich geforderten Schriftform und ist der handschriftlichen Unterschrift, bis auf wenige gesetzlich definierte Ausnahmen, in der Rechtswirkung gleichgestellt. Oder anders formuliert:

Dokumente mit Qualifizierter Elektronischer Signatur ersetzen als elektronische Form die per Gesetz geforderte Schriftform auf Papier.

Noch ist der Verbreitungsgrad digitaler Signatur-Lösungen eher gering, wie die Bundesdruckerei in einer aktuellen Studie feststellte. Doch wird sich dies in der Zukunft ändern.

IN EIGENER SACHE

Die Bundesdruckerei hat Ende Juni ihre neue Studie **„Digitalisierung und IT Sicherheit in deutschen Unternehmen“** vorgestellt. Befragt wurden schwerpunktmäßig kleine und mittelständische Unternehmen. Die Studie kann hier kostenlos heruntergeladen werden: **www.bundesdruckerei.de**

GUT ZU WISSEN

Digitale Signatur-Lösungen bieten in der Praxis eine Vielzahl von Vorteilen.

Elektronisch unterschreiben:

- erzielt erhebliche Einsparungseffekte beim Versand (Papier, Briefumschläge, Porto) und Archivierung (Ordner, Regale, Räumlichkeiten)
- optimiert Geschäftsprozesse durch die konsequente Vermeidung von Medienbrüchen
- erhöht die Kundenzufriedenheit durch schnellere Reaktionen auf Kundenanfragen sowie die komplett digitale Abwicklung bisher papierintensiver Workflows, wie bei Kredit- und Versicherungsabschlüssen
- ermöglicht neue und komfortable E-Government-Dienstleistungen
- steigert die Wettbewerbsfähigkeit von Unternehmen, indem neue Produkte und Dienstleistungen über das Internet angeboten werden können

2. NEUE VERFAHREN UND WERKZEUGE FÜR DIE ELEKTRONISCHE KOMMUNIKATION

Daten und Fakten

415
Mrd. Euro
betragen die jährlichen Wachstumsimpulse durch den digitalen Binnenmarkt.
QUELLE: EU-Kommission

Der Impuls für eine breite und europaweite Nutzung elektronischer Signaturen kommt von der Europäischen Union. Seit September 2014 gilt im gesamten EURaum die Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, kurz eIDAS. Sie ist geltendes Recht in allen 28 Mitgliedsstaaten.

Die eIDAS-Verordnung ermöglicht eine sichere und vertrauenswürdige elektronische Kommunikation auf allen Ebenen und EU-weit. Um dies zu erreichen, schafft eIDAS eine doppelte Sicherheit.

Erstens: Sicherheit im Sinne von Integrität und Authentizität. Technische Schutzmaßnahmen auf hohem Niveau sorgen dafür, dass elektronische Dokumente fälschungssicher sind und der Absender eindeutig identifizierbar ist.

Zweitens: Sicherheit im Sinne von Rechtssicherheit. Denn die eIDAS-Verordnung regelt auch die Rechtswirksamkeit der Kommunikationswerkzeuge, darunter ebenso die digitale Unterschrift, und verleiht den elektronischen Dokumenten vor Gericht einen starken Beweiswert – alles mit gesamteuropäischer Geltung.

Bundeswirtschaftsministerin Brigitte Zypries[3]:

„Ein elektronisch signierter Kaufvertrag muss auch im EU-Ausland so behandelt werden, als wäre er handschriftlich unterzeichnet. Das ist ein wichtiger Schritt hin zu einem starken digitalen Binnenmarkt. Wir entlasten die Menschen und die Unternehmen damit von Bürokratie, denn viele Behördengänge und Briefe können künftig durch elektronische Kommunikation ersetzt werden."

Zentrale Instrumente zur Umsetzung der eIDAS-Verordnung sind die sogenannten Vertrauensdienste. Unter diesem Begriff sind verschiedene Verfahren für die digitale Kommunikation zusammengefasst, darunter auch die elektronische Signatur und das elektronische Siegel.

3 Bundesministerium für Wirtschaft und Energie, Pressemitteilung „Zypries: Digitale Unterschrift spart Kosten und ist sicher"

GUT ZU WISSEN

Der rechtliche Rahmen

Die eIDAS-Verordnung ist seit Inkrafttreten am 17. September 2014 geltendes Recht in allen EU-Mitgliedsstaaten und muss nicht, wie eine Richtlinie, erst noch in nationales Recht umgesetzt werden. Die bisher bestehende EG-Signaturrichtlinie ist aufgehoben. Aktuell befindet sich die EU-Verordnung in der praktischen Umsetzung; entsprechende Produkte und Dienstleistungen dürfen bereits seit Juli 2016 angeboten werden.

Nationaler Ergänzungs- und Konkretisierungsbedarf ist in Deutschland durch das Gesetz zur Durchführung der eIDAS-Verordnung (eIDAS-Durchführungsgesetz) geregelt. Das Herzstück dieses Artikelgesetzes, das Vertrauensdienstegesetz (VDG), enthält alle notwendigen Vorschriften für den Einsatz digitaler Signaturen und löst das bestehende deutsche Signaturgesetz ab.

2.1 Die Fernsignatur

Die Qualifizierte Elektronische Signatur erhält von eIDAS die gleiche Rechtswirkung zugesprochen wie eine handschriftliche Unterschrift. Entscheidend für den EU-weiten Einsatz: Eine Qualifizierte Elektronische Signatur, die in einem Mitgliedsstaat ausgestellt wurde, muss in allen anderen Mitgliedsstaaten als QES anerkannt werden.

Bei der praktischen Umsetzung der digitalen Signatur sorgt die EU-Verordnung für eine europaweite Harmonisierung und Standardisierung der technischen Formate. Weiterhin fördert eIDAS ein vereinfachtes Verfahren für die Signaturerstellung, die Fernsignatur.

eIDAS-Verordnung, Erwägungsgrund (52):

„Die Erstellung elektronischer Fernsignaturen [...] soll aufgrund der vielfältigen damit verbundenen wirtschaftlichen Vorteile ausgebaut werden."

So lassen sich elektronische Unterschriften jetzt auch aus der Ferne auslösen, zum Beispiel über mobile Endgeräte wie Smartphones und Tablets. Dabei werden die für die Signaturerstellung notwendigen Bestandteile (Zertifikat und Schlüsselkomponenten) auf hochsicheren Servern eines externen Dienstleisters vorgehalten. Dies erlaubt Anwendern den Verzicht auf Signaturkarte, Kartenlesegerät und Signatursoftware.

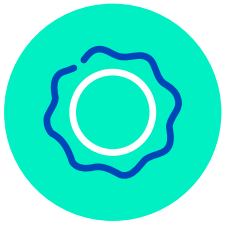
Fazit: Die Fernsignatur steigert die Nutzerfreundlichkeit der elektronischen Unterschrift, etabliert Signaturprozesse in mobilen Umgebungen – inklusive Webbrowser und Apps – und schafft damit komplett neue Signaturanwendungsszenarien.

GUT ZU WISSEN

Die elektronische Unterschrift mit Signaturkarte

Neben der Fernsignatur können bestehende Verfahren zum digitalen Signieren weiter zum Einsatz kommen. Als Verfahren mit ausgereifter Technologie und einem eindeutigen rechtlichen Rahmen präsentiert sich dabei die Signaturkarte. Diese gilt als sichere Signaturerstellungseinheit im Sinne der eIDAS-Verordnung. Die rechtsverbindliche elektronische Unterschrift wird auf der Karte – in Kombination mit einem Lesegerät, Signatur-Software und der Signatur-PIN – erstellt. Erhältlich sind Signaturkarten bei qualifizierten Vertrauensdiensteanbietern, die besonders hohe Sicherheitsniveaus vorweisen müssen. Die Bundesdruckerei verfügt mit ihrem Tochterunternehmen D-TRUST über einen eigenen qualifizierten Vertrauensdiensteanbieter. Mehr Infos unter: **www.bundesdruckerei.de**

2.2 Das elektronische Siegel



Während mit elektronischen Signaturen eine Willenserklärung abgegeben wird, dienen elektronische Siegel einer Institution als Herkunftsnachweis.

Das elektronische Siegel überführt damit das Behördensiegel und den Firmenstempel ins digitale Zeitalter. Es bezieht sich immer auf eine juristische Person, ist also auf eine Organisation ausgestellt.

Wenn Unternehmen und öffentliche Verwaltungen ein Dokument elektronisch siegeln, identifizieren sie sich eindeutig als Absender und schützen die Daten gleichzeitig vor unbemerkten Veränderungen.

Das elektronische Siegel bietet eine doppelte Echtheitsgarantie. Wer gesiegelte Dokumente erhält, kann sich darauf verlassen, dass tatsächlich diejenige Organisation das Dokument ausgestellt hat, die als Absender genannt ist, und dass die Daten des Dokuments vollständig dem Original entsprechen, also nicht nachträglich verändert wurden.

Elektronische Signaturen und Siegel ergänzen sich perfekt

Elektronische Signaturen

- Natürliche Personen (Einzelpersonen)
- Identitätsfeststellung
- Integritätsschutz
- Willenserklärung

Elektronische Siegel

- Juristische Personen (Organisationen)
- Herkunftsnachweis
- Dokumentenechtheit

Fazit: Das elektronische Siegel ermöglicht erstmals digitale Abläufe für Verfahren, die bisher an die Papierform gebunden waren. Die Absender- und Dokumentenechtheit erlaubt es, Steuer- und Rentenbescheide oder Zeugnisse und andere beglaubigte Dokumente elektronisch auszustellen und zu verschicken. Weiterhin kann das Siegel Geschäftsabläufe, die gegen Betrug geschützt werden müssen, auf eine verlässliche Basis stellen. Dazu gehören zum Beispiel die rechtssichere Dokumentenarchivierung oder der elektronische Versand von Kontoauszügen.

3. ERSTE eIDAS-KONFORME FERNSIGNATUR „MADE IN GERMANY“

sign-me

Als erstes Unternehmen in Deutschland hat die Bundesdruckerei mit sign-me eine Lösung für die eIDAS-konforme Fernsignatur vorgestellt. Diese ist vom TÜViT zertifiziert und in die nationale eIDAS-Vertrauensliste der Bundesnetzagentur aufgenommen worden[4].

Mit sign-me lassen sich Dokumente vertrauenswürdig und rechtsverbindlich online unterschreiben. Der webbasierte Service beinhaltet alle notwendigen Softwarekomponenten, um den gesamten Signatur-Workflow abzudecken. Dabei wird der Anwender über die intuitive Benutzeroberfläche Schritt für Schritt durch den Signaturprozess geführt.

Die Signaturplattform sign-me kann über eine Webschnittstelle in Archiv- und Dokumentenmanagementsysteme eingebunden werden. Die Lösung sign-me unterstützt alle drei Signaturniveaus – einfach, fortgeschritten und qualifiziert. Je nach Signaturniveau löst der Unterzeichner die elektronische Unterschrift auf verschiedene Weise aus – von der alleinigen Eingabe von Benutzername und Passwort bis hin zur Zwei-Faktor-Authentifizierung.

4 Der Eintrag von sign-me in die deutsche Vertrauensliste ist einsehbar unter: https://webgate.ec.europa.eu/tlbrowser/#/tl/DE/4/95

Daten und Fakten

90 %

reduzieren sich die Kosten durch den Einsatz von Fernsignaturen.
QUELLE: Infografik der EU-Kommission

GUT ZU WISSEN

Wie funktioniert die Fernsignatur mit sign-me technisch?

Der gesamte Signaturprozess findet in der hochsicheren Umgebung von D-TRUST statt. Das Tochterunternehmen der Bundesdruckerei übernimmt dabei das Hosting der Signaturplattform sign-me. An die Webplattform können sowohl PDF/ADateien als auch Dokumenten-Hash-Werte übergeben werden. Wenn ein PDF/ADokument hochgeladen wird, erzeugt die Anwendung mittels eines mathematischen Algorithmus aus dem Dokument eine eindeutige Folge aus Zahlen und Buchstaben, den sogenannten Hash-Wert. Die Hash-Signatur kommt vor allen Dingen dann zum Einsatz, wenn Dokumente aus Sicherheitsgründen nicht das IT-Umfeld der Organisation verlassen dürfen. In diesem Fall wird der Hash-Wert bereits im Organisationsumfeld erzeugt und dann an sign-me übergeben.

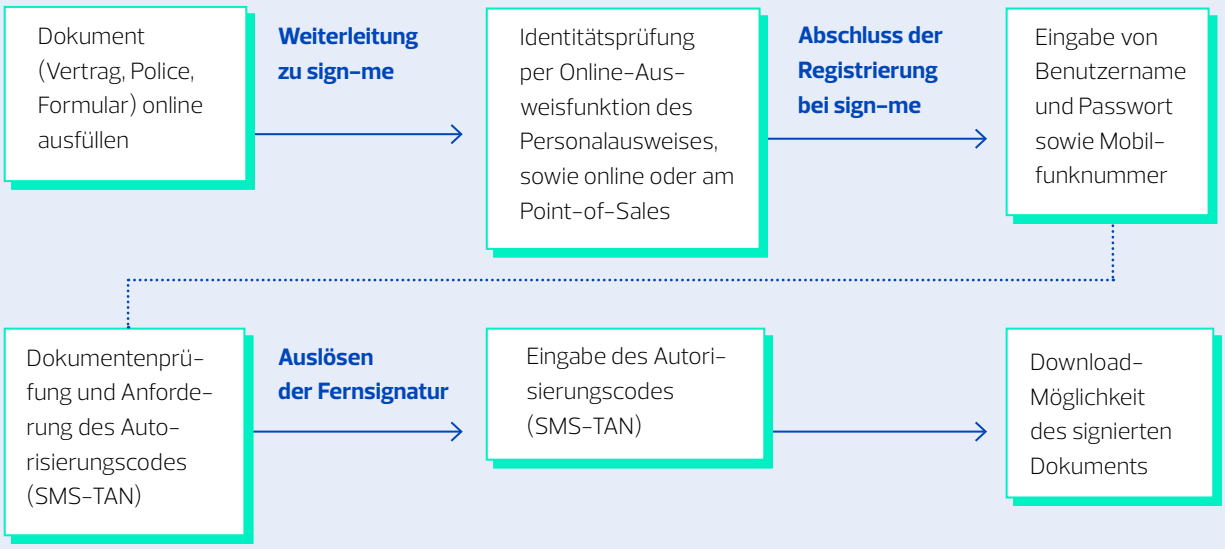
Beim höchsten Niveau der Identifikation, erstellt D-TRUST ein qualifiziertes Zertifikat mit den Identitätsinformationen des Unterzeichners sowie ein Schlüsselpaar, bestehend aus öffentlichem und privatem Schlüssel. Letzterer dient zum Verschlüsseln des Hash-Werts, der zusammen mit dem Zertifikat und dem öffentlichen Schlüssel zur digitalen Signatur verbunden wird. Der Empfänger kann mithilfe des öffentlichen Schlüssels die digitale Unterschrift verifizieren und mit dem gelieferten Zertifikat die Urheberschaft eindeutig identifizieren.

3.1 Die Fernsignatur im Workflow

Der Ablauf einer fernausgelösten elektronischen Unterschrift mit sign-me ist nachfolgend aus Sicht des Unterzeichners skizziert – und zwar am Beispiel eines Online-Kredits. Dabei wird eine qualifizierte elektronische Fernsignatur eingesetzt.

1. Der Interessent übermittelt seine für die Kreditvergabe benötigten Daten über die Website der Bank.
2. Von dort wird er zur sign-me Plattform weitergeleitet. Hier wird seine Identität überprüft. Dafür stehen moderne und sichere Verfahren zur Verfügung, darunter die Online-Ausweisfunktion des Personalausweises (ab Ende 2017), die Online-Identifizierung und die Identifizierung am Point-of-Sales.
3. Ist die Identitätsprüfung erfolgreich abgeschlossen, wählt der Kunde Usernamen und Passwort und teilt seine Mobilnummer mit; danach ist er erfolgreich bei sign-me registriert.
4. Jetzt hat er die Möglichkeit, den aktuellen Vertrag noch einmal detailliert zu prüfen. Ist er mit den Konditionen einverstanden, fordert er einen persönlichen Autorisierungscode an, der ihm als SMS-TAN an seine Mobilfunknummer geschickt wird.
5. Mit Eingabe der SMS-TAN als zweiter Faktor wird das Dokument mit einer Qualifizierten Elektronischen Signatur versehen. Abschließend hat der Kunde die Möglichkeit, den unterschriebenen Vertrag herunterzuladen.

Ablauf bei einer rechtsverbindlichen, elektronischen Fernsignatur



3.2 Die Fernsignatur in der Praxis – vielfältige Anwendungsszenarien

Das größte Einsatzpotenzial besitzt die Qualifizierte Elektronische Fernsignatur. Nur sie entspricht der Schriftform nach § 126 BGB und gilt vor Gericht als Beweis. Die Anwendungsszenarien sind umfangreich und betreffen die unterschiedlichsten Branchen.

Banken und Versicherungen

Mit der Fernsignatur können Geschäftsprozesse mit Schriftformerfordernis komplett elektronisch durchgeführt werden. Im Bankensektor zum Beispiel bei der Kontoeröffnung und der Kreditvergabe – vom elektronischen Identitätsnachweis bis zur digital geleisteten Unterschrift des Kunden. Die Fernsignatur macht auch Versicherungen den Weg frei für komplett digitalisierte Antrags- und Entscheidungsprozesse. Darin eingeschlossen sind beispielsweise alle Anträge, die Gesundheitsfragen enthalten, etwa bei Policen für Lebensversicherungen oder private Krankenversicherungen. Weitere Anwendungsbereiche sind gesetzlich vorgeschriebene Beratungsprotokolle und Schadensmeldungen, die dann ebenfalls elektronisch unterschrieben werden müssen.

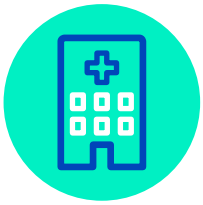
Behörden

Öffentliche Verwaltungen können die Fernsignatur für alle Prozesse nutzen, bei denen die Unterschrift des Antragsstellers gesetzlich gefordert ist. Dazu gehören zum Beispiel Förderanträge, Baugenehmigungen, Abfallbegleitscheine sowie Dokumentationen zum Erwerb von Zertifikaten im Emissionshandel. Ein weiterer zentraler behördlicher Einsatzbereich der Fernsignatur liegt bei öffentlichen Ausschreibungen über E-Vergabe-Plattformen. Durch die Überführung von bisher papierbasierten Abläufen in elektronische Workflows reduziert sich nach den Berechnungen der EU-Kommission der Zeitaufwand von ein bis zwei Wochen auf maximal wenige Tage und die Kosten sinken von 100 Euro auf 10 Euro pro Antrag[5].

Industrie

Die Anwendungsfelder von Fernsignaturen erstrecken sich über alle Bereiche eines Unternehmens. So sorgen mobil unterschriebene Verträge und Vereinbarungen mit Lieferanten für kostengünstige und effiziente Einkaufsworkflows. In Personalabteilungen unterstützen Fernsignaturen sogenannte Onboarding-Prozesse, die das Einstellen und die Integration neuer Mitarbeiter beinhalten. So sind zum Beispiel neue Arbeitsverträge durch digitale Signaturen innerhalb weniger Stunden vereinbart, während dieser Vorgang papiergestützt bis zu mehrere Wochen beanspruchen kann. Zudem steigert die Fernsignatur die Produktivität beim Vertragsmanagement. Kaufverträge lassen sich im Idealfall in wenigen Minuten abschließen und sofort elektronisch archivieren. Und per mobiler Unterschrift bestätigen die Mitarbeiter den Erhalt wichtiger Informationen wie Änderungen in den Geschäftsbedingungen oder Serviceanpassungen.

5 Infografik der EU-Kommission



Krankenhäuser

Beim Einsatz der Fernsignatur in Krankenhäusern steht die elektronische Patientenakte im Vordergrund. Oft ist eine Unterschrift gesetzlich vorgeschrieben. Erst danach können Patienteninformationen in die elektronische Akte aufgenommen werden.

Beispiele sind Formulare, die der Röntgen- oder Strahlenschutzverordnung oder dem Bluttransfusions- und Organtransplantationsgesetz unterliegen. Unterschriften erfordern auch Wahlleistungsvereinbarungen, Aufklärungsbogen und OP-Einwilligungserklärungen. Alle genannten Formular- und Dokumententypen lassen sich mit der Fernsignatur einfachmund ortsunabhängig mit mobilen Endgeräten unterschreiben.

Wie das eingangs beschriebene Zukunftsszenario zeigt, hebt die Fernsignatur auch das Notfallmanagement von Krankenhäusern auf eine neue Qualitätsstufe.

Beispieldokumente für die Fernsignatur

Banken und Versicherungen

- Kreditanträge
- Kontoeröffnungsunterlagen
- Policen für Lebensversicherungen
- Policen für private Krankenversicherungen
- Beratungsprotokolle

Behörden

- Ausschreibungsunterlagen
- Förderanträge
- Baugenehmigungen
- Abfallbegleitscheine
- Ausfuhrgenehmigungen

Krankenhäuser

- Formulare im Bereich Röntgen und Strahlenschutz
- Formulare im Bereich Bluttransfusion und Organtransplantation
- Wahlleistungsvereinbarungen
- Aufklärungsbogen
- OP-Einwilligungserklärungen
- Notfallbogen

Industrie

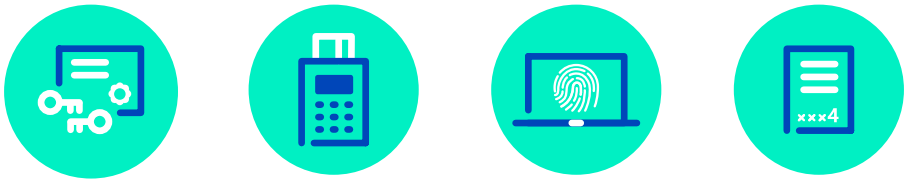
- Kaufverträge
- Lieferantenvereinbarungen
- Arbeitsverträge

4. HERKUNFTSNACHWEIS UND INTEGRITÄTSSCHUTZ MIT DEM ELEKTRONISCHEN SIEGEL

Die Siegel-Lösung der Bundesdruckerei basiert auf einer Siegelkarte, die analog zur Signaturkarte ein Zertifikat und das Schlüsselpaar aus öffentlichem und privatem Schlüssel enthält. Technisch entspricht ein elektronisches Siegel einer elektronischen Signatur, nur mit dem Unterschied, dass die Zertifikate unterschiedlich ausgestellt sind, beim Siegel auf eine Organisation (Behörde, Unternehmen etc.), bei der Signatur auf eine Einzelperson.

In der praktischen Nutzung bedeutet das: Anwender, die bereits eine Signatur-Lösung im Einsatz haben, können die vorhandene Infrastruktur aus Hardware- und Softwarekomponenten auch für das elektronische Siegel nutzen. Erhältlich ist die Siegelkarte bei D-TRUST in zwei Varianten: Erstens für Einzeldokumente und zweitens als Multisiegelkarte für die Stapelverarbeitung von Dokumenten.

Benötigte Komponenten für ein elektronisches Siegel:



Siegelkarte mit qualifiziertem Zertifikat und Schlüsselpaar

Kartenlesegerät

Computer mit Signatur-Software

Siegel-PIN

GUT ZU WISSEN

Beim Siegel auf qualifizierte Anbieter achten

Die Siegel-Lösung der Bundesdruckerei wird von D-TRUST bereitgestellt und erfüllt die hohen Sicherheitsanforderungen der eIDAS-Verordnung. Das Tochterunternehmen der Bundesdruckerei ist ein qualifizierter Vertrauensdiensteanbieter (qVDA) gemäß eIDAS. Die EU-Verordnung definiert qualifizierte Vertrauensdiensteanbieter als besonders sicher und vertrauenswürdig. Dafür müssen sich die Lösungen der qVDA einer detaillierten Konformitätsprüfung unterziehen. Diese hat D-TRUST für seine Siegel-Lösung erfolgreich absolviert. Die Bundesnetzagentur als Aufsichtsbehörde hat das elektronische Siegel der Bundesdruckerei deshalb in die öffentlich einsehbare eIDAS-Vertrauensliste aufgenommen.

4.1 Die Siegelkarte im Workflow

1. Die Beantragung einer Siegelkarte geht gesetzlich immer mit der Identifizierung des Antragstellers (Geschäftsführer, Zeichnungsberechtigte etc.) einher. Belege dafür können ein gültiger Personalausweis oder Reisepass sein. Soll der Name einer Organisation in ein Zertifikat übernommen werden, muss dies durch einen Zeichnungsberechtigten der Organisation bestätigt werden – beispielsweise unter Vorlage eines Handelsregisterauszugs, des IHK-Firmenspiegels oder der Gewerbeanmeldung.

2. Wurde der Identitätsnachweis erbracht, stellt D-TRUST ein qualifiziertes Zertifikat auf den Namen der Organisation aus, erzeugt ein Schlüsselpaar aus öffentlichem und privatem Schlüssel und überträgt das Zertifikat auf die Siegelkarte. Zusätzlich generiert D-TRUST die Siegel-PIN, mit der das elektronische Siegel ausgelöst wird.

3. Der Einsatz der Siegelkarte setzt ein Kartenlesegerät und eine spezielle Signatursoftware voraus. Bei der notwendigen Installation der Siegelkarte hilft eine detaillierte Bedienungsanleitung von D-TRUST. Alle erforderlichen Komponenten – Siegelkarte, Lesegerät und Signatur-Software – sind bei D-TRUST erhältlich.

4. Das Aufbringen des elektronischen Siegels erfolgt mittels Zwei-Faktor-Authentifizierung: erstens durch die Siegelkarte im Lesegerät und zweitens durch die Eingabe der Siegel-PIN

4.1 Das elektronische Siegel in der Praxis – vielfältige Anwendungsszenarien

Das elektronische Siegel dient als Integritätsschutz und Herkunftsnachweis für digitale Dokumente. Dieser doppelte Anwendernutzen erlaubt neue Szenarien für den Dokumentenaustausch. Erstmals ist es möglich, die Beweiskraft eines Behördensiegels und eines Firmenstempels in die elektronische Kommunikation einzubinden. Die Verbreitung medienbruchfreier Workflows erhält dadurch einen großen Schub, wie die folgenden Anwendungsbeispiele zeigen.

Banken und Versicherungen

Im Bankensektor sorgen gesiegelte Dokumente und E-Mails für eine sichere und vertrauenswürdige elektronische Kommunikation. Laut der neuen EU-Zahlungsrichtlinie PSD2 müssen Anfragen von Drittanbietern (beispielsweise Fintech) an die kontoführende Stelle (in der Regel eine Bank) mit einem qualifizierten elektronischen Siegel oder qualifiziertem Website Zertifikat abgesichert sein. Zudem beseitigen elektronische Siegel einen gravierenden Medienbruch im Online-Banking: Mit einem Siegel versehene Kontoauszüge erfüllen die steuerrechtliche Anforderung an die Unveränderbarkeit der Auszüge und lassen sich daher elektronisch übermitteln.

Behörden

Mit elektronischen Siegeln können deutlich mehr behördliche Bescheide digital verschickt werden. Denn beim Erlass von Verwaltungsakten ist es erforderlich, dass sie die ausstellende Behörde erkennen lassen. Besonders bei Massenverfahren wie bei Steuer- oder Rentenbescheiden ergibt sich ein großes Einsparpotenzial. Elektronische Siegel stellen aber nicht nur den Ursprung, sondern auch die Unversehrtheit von elektronischen Daten sicher, ein wichtiges Merkmal für amtliche Beglaubigungen.

So lassen sich Urkunden jeglicher Art (Geburts-, Heirats- und Sterbeurkunden) und Zeugnisse elektronisch zustellen. Rechtswirksame öffentliche Bekanntmachungen im Internet, die gegen Löschung und Verfälschung geschützt werden müssen, sind ein weiterer Anwendungsfall. Zudem sieht das eIDAS-Durchführungsgesetz ausdrücklich vor, dass elektronische Siegel in Vergabeverfahren öffentlicher Verwaltungen neben der elektronischen Signatur zugelassen sind[6]. Weitere rechtliche Öffnungen für das elektronische Siegel im Verwaltungsrecht sowie im Zivil- und Verfahrensrecht sind in Aussicht gestellt[7].

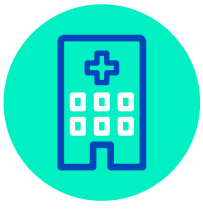
6 eIDAS-Durchführungsgesetz, Artikel 6 bis 9

7 Bundesministerium für Wirtschaft und Energie, eIDAS-Durchführungsgesetz

Industrie

Angriffe auf die IT-Sicherheit von Unternehmen erfolgen größtenteils mit manipulierten E-Mails und Dokumenten, die beim Aufrufen Erpressungstrojaner oder Viren freisetzen bzw. den Empfänger über fingierte Websites wertvolle Informationen wie Kontodaten entlocken. Mit elektronischen Siegeln wird der Versand sensibler Informationen und Dokumenten daher erheblich sicherer. Denn bei gesiegelten Mails und Dokumenten kann der Empfänger darauf vertrauen, dass ihre Herkunft und Integrität belegt sind.

Einen hohen Schutz bieten elektronische Siegel auch für Software, was aufgrund umfassender Bedrohungen durch Schad-, Erpressungs- und Ausspähprogramme wichtiger denn je ist. Vor Installation oder Ausführung der Software wird der Herausgeber mittels Siegel eindeutig identifiziert. Außer von einer gesteigerten IT-Sicherheit profitieren Unternehmen zusätzlich von produktiveren Geschäftsprozessen, beispielsweise bei der elektronischen Rechnungsverarbeitung. So berechtigen elektronisch versandte Rechnungen zum Vorsteuerabzug erst dann, wenn die Echtheit und die Korrektheit der Rechnungsdaten belegt werden können. Die dafür geforderten innerbetrieblichen Kontrollverfahren lassen sich mit elektronischen Siegeln hervorragend umsetzen.



Krankenhäuser

Eine Vernetzung von ambulantem, stationärem und rehabilitativem Sektor hilft dabei, langfristig ein optimales Behandlungsergebnis zu erzielen. Dies gelingt nur dann, wenn Informationen im Rahmen der intersektoralen Kommunikation effizient ausgetauscht werden. Eine zentrale Lösung dafür ist die elektronische Patientenakte. Durch den Einsatz elektronischer Siegel lassen sich zusätzliche Dokumentenarten in die elektronische Patientenakte integrieren, wie Entlassungsbriefe oder Überführungsbescheide beispielsweise vom Krankenhaus in die Rehaklinik.

Elektronische Archivierung

Ein Anwendungsbereich, der alle vorgestellten Branchen betrifft, ist die elektronische Archivierung. Immer mehr Papierdokumente, für die eine gesetzliche Aufbewahrungspflicht besteht, werden eingescannt und digital abgelegt. Bei diesem Prozess muss sichergestellt sein, dass der Beweiswert der Dokumente erhalten bleibt.

Die technische Richtlinie TR-RESISCAN des Bundesamts für Sicherheit in der Informationstechnik (BSI) sieht dafür bisher das Aufbringen einer Qualifizierten Elektronischen Signatur vor. Jetzt gibt es mit dem qualifizierten elektronischen Siegel eine komfortable Alternative.

Beispieldokumente für das elektronische Siegel

Banken und Versicherungen

- Kontoauszüge
- Elektronische Anfragen im Rahmen der PSD2-Zahlungsrichtlinie
- Dokumente im Rahmen des ersetzenden Scannens nach TR-RESISCAN

Krankenhäuser

- Entlassungsbriefe
- Überführungsbescheide
- Dokumente im Rahmen des ersetzenden Scannens nach TR-RESISCAN

Industrie

- E-Mails mit sensiblen Informationen
- Dokumente mit sensiblen Informationen
- Softwareprogramme
- Elektronische Rechnungen
- Dokumente im Rahmen des ersetzenden Scannens nach TR-RESISCAN

Behörden

- Behördenbescheide (u.a. Steuer- und Rentenbescheide)
- Urkunden
- Zeugnisse
- Dokumente für elektronische Vergabeverfahren
- Dokumente im Rahmen des ersetzenden Scannens nach TRRESISCAN

5. IN FÜNF SCHRITTEN ZUR PASSENDEN DIGITALEN SIGNATUR

Daten und Fakten

800.000

aktive Handy-Signaturen gibt es bereits in Österreich.
QUELLE: Digitales Österreich

Daten und Fakten

Über

2.400

elektronische Dienste bietet Estland seinen Unternehmen an.
QUELLE: Tourismus Estlan

Alles wird digital möglich

Viele Services können bequem online von zu Hause oder von unterwegs mit Mobiltelefon genutzt werden: Bankkredite abschließen, Gewerbe anmelden, Duplikat der Geburtsurkunde anfordern, Alterspension und Kinderbetreuungsgeld beantragen oder die eigene Stimme bei Parlamentswahlen abgeben. Und das Beste: Wer Behördenanträge digital mit einer Fernsignatur einbringt, erhält noch Rabatt auf die Antragsgebühren. – Das ist kein neuer Ausblick auf die Zukunft, sondern bereits heute gelebte Praxis – in Österreich und Estland.

Nutzen auch Sie die Optimierungspotenziale von Fernsignatur und elektronischem Siegel für Ihre Geschäftsprozesse. Wir zeigen Ihnen in fünf Schritten, was Sie bei der Umsetzung alles beachten sollten, und geben gleichzeitig wertvolle Tipps und Ratschläge.

Schritt 1: Geschäftsprozesse analysieren

Analysieren Sie zunächst Ihre Geschäftsprozesse im Hinblick auf bestehende Hemmnisse und Barrieren für durchgängig elektronische Abläufe. Identifizieren Sie diejenigen Abläufe, die eine Unterschrift benötigen oder bei denen Sie die Herkunft und die Unversehrtheit der Dokumente nachweisen müssen. Diese Abläufe sind potenzielle Anwendungsfälle für die Fernsignatur und das elektronische Siegel.

Wenn Sie bereits die elektronische Unterschrift nutzen, vergleichen Sie die bisher eingesetzte Lösung mit den neuen Werkzeugen und Verfahren. Welche Gründe sprechen für die Beibehaltung der bestehenden Signatur-Infrastruktur, welche für den Einsatz der Fernsignatur oder des elektronischen Siegels?

Schritt 2: Werkzeug und Verfahren auswählen

Wählen Sie die für Ihren Anwendungsfall passende Kombination aus Werkzeug und Verfahren aus. Denken Sie immer daran, dass elektronische Signatur und elektronisches Siegel nicht in Konkurrenz zueinander stehen, sondern sich perfekt ergänzen. Allein die Qualifizierte Elektronische Signatur ersetzt eine rechtlich geforderte handschriftliche Unterschrift. Sie macht elektronische Daten zu einer persönlichen Willenserklärung.

Demgegenüber stellen elektronische Siegel sicher, dass die Daten von einer bestimmten Institution stammen (Herkunftsnachweis) und dass das Dokument vor unbeabsichtigten Veränderungen geschützt ist (Integritätsschutz).

Das elektronische Unterschreiben mit Signaturkarte ist für klar begrenzte Anwendungsfälle, die wenige Arbeitsplätze betreffen, vorgesehen. Diese lokalen Signatur-Lösungen sind für Einzelarbeitsplätze mit der entsprechenden Hardware und Software konzipiert.

Überall dort, wo mobile Anforderungen bestehen und einfache Bedienung gefragt ist, ist die Fernsignatur erste Wahl. Mit der elektronischen Unterschrift über mobile Endgeräte lassen sich erstmals breite Anwenderkreise erreichen. Das betrifft sowohl den elektronischen Geschäftsverkehr im Unternehmensumfeld als auch die elektronische Kommunikation zwischen Behörden und Bürgern.

Für das Siegeln elektronischer Dokumente stehen zwei Verfahren – auf Grundlage der Siegelkarte – zur Verfügung. Neben der Einzelarbeitsplatzlösung ist auch eine Multi-Siegelkarte erhältlich. Diese eignet sich für Serverlösungen in einer gesicherten Umgebung oder für dien Siegelung einer großen Anzahl von Dokumenten in der Stapelverarbeitung. Dabei ist eine Mehrfachsiegelung nach einmaliger PIN-Eingabe möglich.

Schritt 3: Externe Unterstützung in Erwägung ziehen

Der Aufbau kundengerechter, eIDAS-konformer Lösungen erfordert neben strategischen Überlegungen und einer schlüssigen Konzeption auch Fragestellungen rund um die Lösungseinführung und Integrationsaufgaben. Hierbei können externe Berater wertvolle Hilfestellung leisten und den gesamten Implementierungsprozess kürzer und kosteneffizienter gestalten. Dies beinhaltet zum Beispiel:

- die Formulierung des strategischen Ziels und die Erstellung eines dezidierten Maßnahmenkatalogs (Strategie),
- die notwendigen organisatorischen Regelungen und Verantwortlichkeiten sowie die Beschreibung technischer Komponenten und deren Funktionalitäten (Konzeption),
- die notwendigen Schulungsmaßnahmen und die konkrete Überführung des Verfahrens in den Betrieb (Einführung) sowie damit zusammenhängend die Einbindung in bestehende IT-Infrastrukturen (Integration).

Schritt 4: Fernsignatur und elektronisches Siegel erwerben

Die technischen Systeme zur Siegelerzeugung und Fernsignaturerstellung werden von einem Vertrauensdiensteanbieter (VDA) gegen Entgelt bereitgestellt. Qualifizierte VDA besitzen den höchsten Vertrauensstatus. Sie unterliegen sehr strengen Sicherheitsvorschriften und Haftungsregelungen.

Dazu gehören die Meldung von Sicherheitsvorfällen innerhalb von 24 Stunden, die Gewährleistung von Datenschutz und Datensicherheit sowie der Einsatz vertrauenswürdiger IT-Systeme und IT-Infrastrukturen.

Qualifizierte VDA haften für alle vorsätzlich und fahrlässig zugefügten Schäden, die

durch ihre Arbeit entstehen. Dabei gilt für sie die Beweislastumkehr, das heißt, es wird grundsätzlich von Vorsatz und Fahrlässigkeit ausgegangen, es sei denn, sie können das Gegenteil beweisen.

Alle qualifizierten Vertrauensdienste – wie die qualifizierte Fernsignatur als Ersatz für die handschriftliche Unterschrift oder die Siegelkarten-Lösung – sind nur bei qualifizierten VDA erhältlich. Qualifizierte VDA werden alle zwei Jahre in einem aufwändigen Verfahren von unabhängigen Auditoren überprüft. Der Status als qualifizierter Vertrauensdiensteanbieter ist europaweit über eine Vertrauensliste und ein Gütesiegel nachprüfbar. Die deutsche Vertrauensliste ist auf der Webseite der Bundesnetzagentur abrufbar: www.nrca-ds.de

Schritt 5: Loslegen

Starten statt warten ist das Gebot der Stunde. Der rechtliche Rahmen ist klar definiert, die Technologien sind ausgereift und sofort einsetzbar – und all das für den gesamten EU-Raum.

Bundesdruckerei GmbH
Kommandantenstraße 18 10969 Berlin
Tel.: +49 (0)30 25 98-0 Fax: +49 (0)30 25 98-22 05
info@bdr.de www.bundesdruckerei.de

Stand: August 2017