

eIDAS-ready?

Status Quo und Roadmap zur Umsetzung elektronischer
Vertrauensdienste in Behörden und Unternehmen



Inhalt

Vorwort – Ziele und Aufbau der Umfrage	3
Einleitung	4
Einführung zur eIDAS-Verordnung	4
Vorgehensweise und Teilnehmerkreis der Umfrage .	6
Umfrageergebnisse: Aktuelle Umsetzung digitaler Geschäftsprozesse	7
Nutzung digitaler Geschäftsprozesse und Digitalisierungsstrategie	7
Einsatz elektronischer Signaturen und Zeitstempel	8
Ersetzendes Scannen	9
Nachweisfähigkeit und Internationalität elektronischer Geschäftsprozesse	10
Sichere elektronische Kommunikation	10
Umfrageergebnisse: Umsetzungsstand der eIDAS-Verordnung	13
Bekanntheitsgrad und Grundlagen elektronischer Vertrauensdienste gemäß eIDAS-Verordnung ...	14
Umsetzung von Vertrauensdiensten	14
Unterstützungsbedarfe	15
Bericht aus der Praxis – eIDAS in einer europäischen Bank	16
Fazit und Handlungsempfehlungen	18
Abkürzungsverzeichnis	20
Anlage: Marktübersicht	22

eIDAS-ready?

Status Quo und Roadmap zur Umsetzung elektronischer Vertrauensdienste in Behörden und Unternehmen

Vorwort – Ziele und Aufbau der Umfrage

Mit der EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen (eIDAS) liegt nun seit rund zwei Jahren eine EU- und EFTA-weit einheitliche Vorgabe für vertrauenswürdige elektronische Geschäftsprozesse vor. Zeit, eine Zwischenbilanz zu ziehen:

- Sind die Inhalte der eIDAS-Verordnung und damit verbundene Verpflichtungen bekannt?
- Sind die Chancen und Herausforderungen der eIDAS-Verordnung bekannt?
- Wie ist der Umsetzungsstand der eIDAS-Verordnung in Deutschland?
- Welche Vertrauensdienste werden wie genutzt?
- Inwieweit sind die Voraussetzungen für vollständig digitale Prozesse unter Nutzung der eIDAS-Verordnung geschaffen?
- Welche Produkt- und Lösungsanbieter gibt es am deutschen Markt?

Diesen und weiteren Fragen geht die vorliegende Umfrage zum Umsetzungsstand der eIDAS-Verordnung nach. Ziel war es, zum einen zu analysieren, inwieweit die Voraussetzungen zur Umsetzung der eIDAS-Verordnung gegeben sind. Beispiele dafür sind

- die möglichst umfangreiche Nutzung vollständig digitaler Geschäftsprozesse,
- das Vorhandensein einer entsprechenden Digitalisierungsstrategie,
- die Umsetzung des ersetzenden Scannens sowie
- die Einführung elektronischer Dokumentenmanagementsysteme.

Zum anderen wurde der aktuelle Stand der Einführung und Nutzung elektronischer Vertrauensdienste in Behörden und Unternehmen analysiert.

Auf Basis beider Analyse-Bestandteile werden Handlungsempfehlungen abgeleitet, um im Sinne des Standorts Deutschland die Potenziale der Verordnung effizient zu nutzen, aber auch Herausforderungen wirksam gerecht zu werden für eine vollständige wie vertrauenswürdige Digitalisierung – Anfang bis Ende.

Vertrauenswürdige digitale Geschäftsprozesse Anfang bis Ende mit eIDAS



Vor diesem Hintergrund ist die Umfrage folgendermaßen gegliedert:

- Teil 1: Fachliche Betrachtung (Organisatorisch-technische Rahmenbedingungen und Voraussetzungen zur Umsetzung der eIDAS-Verordnung; Umsetzungsstand der eIDAS-Verordnung)
- Teil 2: Handlungsempfehlungen
- Teil 3: Marktübersicht von Vertrauensdienste-/Produkt- und Lösungsanbietern

Wir wünschen Ihnen eine anregende Lektüre.


Steffen Tampe
Director
 BearingPoint


Dr. Matthias Flügge
Leiter Geschäftsbereich
Digital Public Services
Fraunhofer FOKUS

Einleitung

Einführung zur eIDAS-Verordnung

Verbunden mit der Anerkennungspflicht jedes qualifizierten Vertrauensdiensteanbieters für elektronische Signaturen/Siegel/Zeitstempel (QES/QESI/QZS) bieten sich mit der eIDAS erhebliche Erleichterungen zur Umsetzung vollständig digitaler Prozesse zwischen Behörden, Unternehmen und Bürgern – auch in hochregulierten Branchen.

Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen (eIDAS) vom 23. Juli 2014 bildet die aktuelle rechtliche Grundlage für die Nutzung elektronischer Vertrauensdienste und Identifizierungsmittel.

Die Regelungen und Ausführungsbestimmungen hinsichtlich elektronischer Vertrauensdienste (elektronische Signaturen, Siegel und Zeitstempel) sind zum 01.07.2016 in Kraft getreten. Die Vorgaben für Einschreib- und Zustelldienste gelten bereits seit Inkrafttreten der Verordnung zum September 2014.

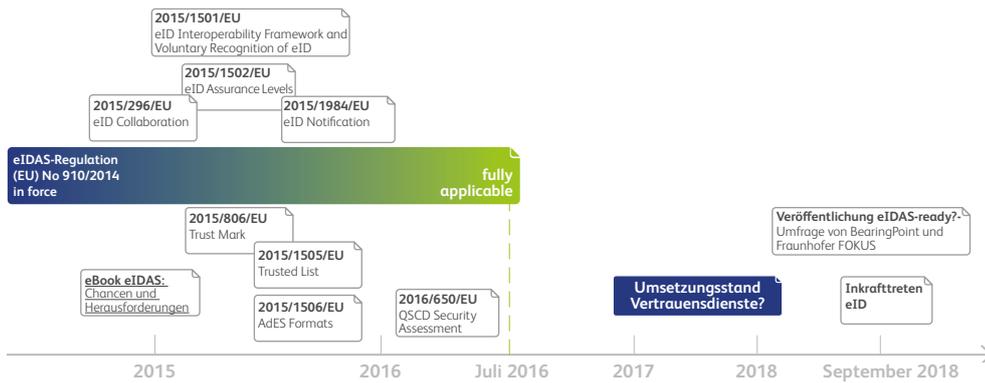
Seit 23.07.2017 liegt das deutsche eIDAS-Durchführungsgesetz vor. Ein elementarer Bestandteil des Gesetzes ist die Verkündung des Vertrauensdienstegesetzes (VDG), das das bisher geltende Signaturgesetz (SigG) sowie die Signaturverordnung (SigV) ablöst. Es ernennt die Bundesnetzagentur (BNetzA) zur nationalen Aufsichtsstelle für Vertrauensdienste und spezifiziert deren Aufgaben. Weiterhin werden Anforderungen an (qualifizierte) Vertrauensdienste (Mitwirkungspflichten, [nationale] Vertrauenslisten, Haftung, Identitätsprüfung für Nutzer der Dienste oder mögliche Attribute), an Beweiserhaltung im Allgemeinen sowie für qualifizierte elektronische Signaturen und Siegel und Einschreib- und Zustelldienste im Besonderen spezifiziert.

Die eIDAS-Verordnung bringt weitreichende Neuerungen mit sich. Die Zulassung von Serversignaturen, die Fern- und mobile Signaturen ermöglichen, und die Einführung von elektronischen Siegeln für Organisationen bedeuten einen vereinfachten Einsatz von elektronischen Vertrauensdiensten. Zudem ergeben sich Möglichkeiten neuer Geschäftsmodelle, seien es ad-hoc-/mobile Verträge, Siegelung elektronischer Bescheide, vereinfachtes ersetzendes Scannen oder die Digitalisierung komplexer Zulassungsverfahren in Luftfahrt, Pharma oder der Chemiebranche sowie in kritischen Infrastrukturen wie HealthCare, Energiewirtschaft oder Endlagerung durch den Einsatz von QES/QESI/QZS und Beweiserhaltung¹.

Durch einheitliche Normen, die durch die eIDAS-Durchführungsrechtsakte veranlasst werden, liegen zudem kohärente technische Rahmenbedingungen vor, um die Potenziale der eIDAS-Verordnung stringent umzusetzen.

Zum 25.09.2018 kommen darüber hinaus die Regelungen für elektronische Identifizierungsmittel – kurz eID – in der EU/EFTA hinzu, mit der äquivalenten Maßgabe, dass alle notifizierten eID-Mittel durch alle öffentlichen Stellen anzuerkennen sind, sobald ein eID-Mittel als Pflichtenanforderung zu nutzen ist. Mit der Verpflichtung zur Zugangseröffnung für den neuen Personalausweis (nPA) in den E-Government-Gesetzen ist dies in Deutschland der Fall.

Zeiträume für die Umsetzung der eIDAS-Verordnung



Vorgehensweise und Teilnehmerkreis der Umfrage

In den fachlichen Teil 1 der Umfrage wurden im Jahr 2017 mehr als 500 Behörden sowie Unternehmen der Finanzindustrie und hochregulierten Branchen mithilfe eines Onlinefragebogens einbezogen. Die Erhebung umfasste Fragenkomplexe zu den genannten Themengebieten:

- Organisatorisch-technische Rahmenbedingungen zur Umsetzung der eIDAS-Verordnung
- Umsetzungsstand der eIDAS-Verordnung

mit ja/nein-Fragen sowie der Möglichkeit, zusätzliche Erläuterungen in Freitextfeldern hinzuzufügen. Hinsichtlich des Teilnehmerkreises wurden Branchen ausgewählt, bei denen aufgrund der vergleichsweise hohen regulatorischen Anforderungen an vollständig digitale Prozesse G2B2C ein möglichst hoher Nutzen durch die eIDAS-Verordnung und die hier definierten Vertrauensdienste sowie deren rechtlich-organisatorischen wie technischen Rahmenbedingungen erwartbar ist.

Analog gestaltete sich die Datenerhebung zur Marktübersicht. Hier wurde die Umfrage den Anbietern unter Einbeziehung des Branchenverbands BITKOM (Arbeitskreis „Anwendung elektronischer Vertrauensdienste“) sowie des Vereins Sichere Identität Berlin-Brandenburg e.V. und anhand der Marktkenntnis von Fraunhofer und BearingPoint zur Verfügung gestellt. Ebenso wurde die Weiterverbreitung des Onlinefragebogens, über den BITKOM hinaus, durch die Nutzung sozialer Medien sowie den Branchenverband gefördert. Die Ergebnisse beruhen auf Selbstauskünften der Anbieter. Die Marktübersicht erhebt daher keinen Anspruch auf Vollständigkeit oder die Förderung einzelner Unternehmen, sondern soll lediglich als ein erster Überblick möglicher Anbieter dienen. Sie ersetzt keine fundierte Marktanalyse im Rahmen konkreter Projekte oder Beschaffungen oder ein Vergabeverfahren selbst.

Umfrageergebnisse:

Aktuelle Umsetzung digitaler Geschäftsprozesse

Umfrageergebnisse: Aktuelle Umsetzung digitaler Geschäftsprozesse

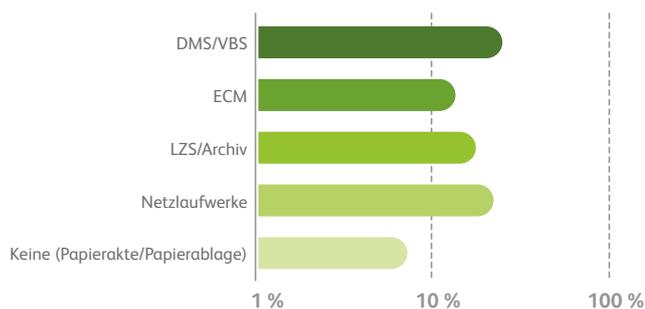
Nutzung digitaler Geschäftsprozesse und Digitalisierungsstrategie

Der erste Fragenkomplex zielte sowohl auf die bestehende Nutzung digitaler Geschäftsprozesse als auch die existierenden Strategien zur Einführung vollständig medienbruchfreier Prozesse in den beteiligten Behörden und Unternehmen. Die elektronische Abbildung der Geschäftstätigkeiten zwischen Behörden, Unternehmen und Bürgern (G2B2C) ist eine wesentliche Voraussetzung zur Nutzung elektronischer Vertrauensdienste für vertrauenswürdige Transaktionen.

Rund die Hälfte der befragten Organisationen haben bereits vollständig oder teilweise medienbruchfreie Geschäftsprozesse umgesetzt. Gleichzeitig planen 38 Prozent der Befragten alle Geschäftsprozesse vollständig zu digitalisieren. Mit Blick auf bestehende gesetzliche Verpflichtungen im öffentlichen Bereich sowie die organisatorischen wie technischen Möglichkeiten, die sich aus der eIDAS-Verordnung ergeben, erscheint dies wenig. Jedoch sind 40 Prozent der Teilnehmer derzeit noch unentschlossen – ein breites Potenzial für eine ganzheitliche Digitalisierung.

Hinsichtlich der Anwendungsfälle für die weitere Digitalisierung stehen sowohl die E-Akte und ECM, die Umsetzung von Fachprozessen als auch die elektronische Abbildung von Vertragsabschlüssen und Finanzdienstleistungen im Vordergrund. Interessant dabei ist, dass rund 40 Prozent der Beteiligten noch offen sind, welche Prozesse sie künftig digital abwickeln wollen.

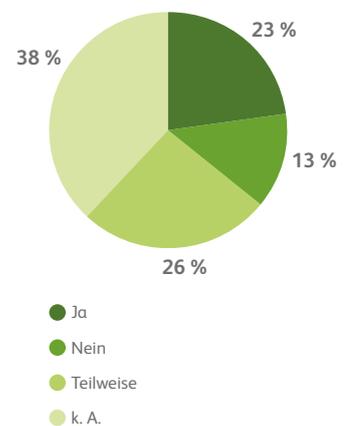
Umfang der Nutzung elektronischer Ablagen



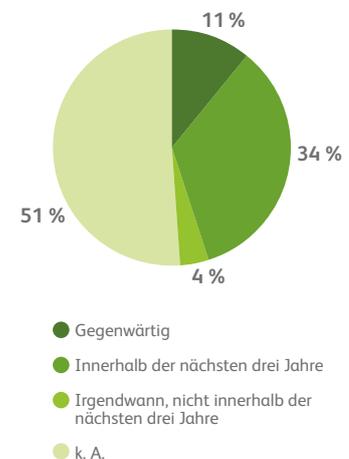
Hinsichtlich des zeitlichen Rahmens der Umsetzung planen diese 45 Prozent gegenwärtig beziehungsweise innerhalb der nächsten drei Jahre. Mit Blick auf die Erfordernisse aus E-Government-Gesetz, EU-DSGVO, eIDAS oder zum Beispiel der Payment Service Directive 2, kurz PSD2-Richtlinie der EU im Zahlungsverkehr, erscheint dieser Prozentsatz gering – hier ist das Bewusstsein für die Notwendigkeit und die gegebenenfalls vorhandene Verpflichtung einer digitalen Abwicklung von Transaktionen zu schärfen.

Rund die Hälfte der befragten Organisationen haben bereits vollständig oder teilweise medienbruchfreie Geschäftsprozesse umgesetzt.

Sind in Ihrer Organisation medienbruchfreie elektronische Geschäftsprozesse umgesetzt?



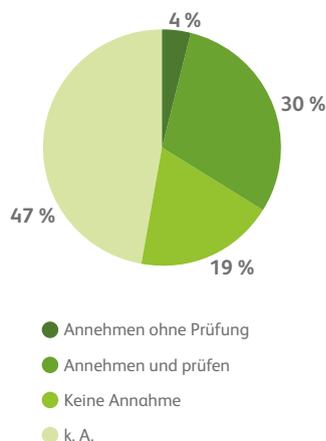
Wann planen Sie die medienbruchfreie elektronische Umsetzung der Geschäftsprozesse in Ihrer Organisation?



Einsatz elektronischer Signaturen und Zeitstempel

Im Ergebnis der Umfrage nutzen bislang rund die Hälfte der teilnehmenden Organisationen die QES faktisch nicht. Von den übrigen nehmen 30 Prozent der Beteiligten eine Signaturprüfung bei Eingang signierter Dokumente vor.

Wie werden in Ihrer Organisation qualifizierte elektronische Signaturen (QES) oder qualifizierte elektronische Siegel (QESI) im Eingangsfall verarbeitet?



Die eIDAS-Verordnung bietet erhebliche Vereinfachungen zur Nutzung (qualifizierter) elektronischer Signaturen durch Server-/Fern- und mobile Signaturen und durch den Einsatz des neuen QESI, sei es für rechtsverbindliche elektronische Unterschriften, Bestätigungen oder beim ersetzenden Scannen. Vergleichbares gilt für den Einsatz von QZS. Im Hinblick auf die konkrete Umsetzung war es relevant, den Status quo bezüglich der Nutzung der QES zu untersuchen. Daraus ergibt sich, inwieweit die eIDAS-Verordnung hier tatsächlich unterstützend wirken kann.

Im Ergebnis der Umfrage nutzen bislang rund die Hälfte der teilnehmenden Organisationen die QES faktisch nicht. Von den übrigen nehmen 30 Prozent der Beteiligten eine Signaturprüfung bei Eingang signierter Dokumente vor. Das kann ein Risiko darstellen, wenn das betreffende Dokument der Notwendigkeit der Schriftform unterliegt, denn ohne Prüfung bleiben etwaige Manipulationen unbemerkt und die Nachweisfähigkeit ist damit eingeschränkt.

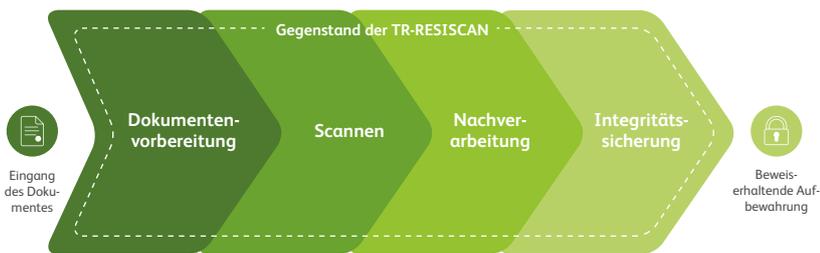
Gleichzeitig ist festzustellen, dass mehrheitlich ein unterschiedliches Vorgehen für die einzelnen Geschäftsprozesse gewählt wird. Mit Blick auf die Gleichartigkeit der Tätigkeit bei der Prüfung der QES besteht Optimierungsbedarf für durchgängig vertrauenswürdige wie nachweisfähige elektronische Prozesse unter Erfüllung der einschlägigen Formvorschriften. Nur so kann die Integrität der Daten sowie die gegebenenfalls nötige Erfüllung der Schriftform gewährleistet werden.

Von dem rund einem Drittel der befragten Institutionen, die Erfahrung im Umgang mit QES/QZS besitzen, nutzt die Mehrheit die Technologien zudem sowohl zur Erzeugung als auch zur Prüfung von Signaturen beziehungsweise Zeitstempeln – setzt also auf die volle Funktionalität dieser Sicherheitskomponenten zur Abbildung vertrauenswürdiger elektronischer Transaktionen. Dies korreliert auch mit dem Fakt, dass 38 Prozent der Befragten angaben, elektronisch unterschriebene Dokumente versehen mit QES zu erhalten respektive diese auch selbst zu erzeugen. Wer den Schritt in Richtung QES/QZS also einmal gegangen ist, nutzt diese Möglichkeiten mehrheitlich auch umfangreich. Aufschlussreich ist dabei der Fakt, dass zum Schriftformersatz eher die QES selbst und weniger De-Mail genutzt wird, was gemäß E-Government-Gesetz möglich wäre. Allerdings besteht angesichts der Tatsache, dass es sich bei beiden derzeit immer noch um eine begrenzte Nutzeranzahl handelt, erheblicher Nachholbedarf zur beweisensicheren wie vertrauenswürdigen Digitalisierung in Deutschland. Die eIDAS könnte hier als Motor dienen, zumal sich unter den Nutzern auch Institutionen befinden, die zum Beispiel bereits Siegel oder Signaturen gemäß eIDAS einsetzen.

Ersetzendes Scannen

Mit der BSI TR-03138 RESISCAN liegt ein Standard zum rechtssicheren ersetzenden Scannen vor, auf den als Stand der Technik gesetzlich zum Beispiel in den E-Government-Gesetzen von Bund und Ländern sowie der Zivilprozessordnung (ZPO) verwiesen wird. Darüber hinaus empfehlen auch die Simulationsstudien der DATEV sowie Musterverfahrensdocumentationen aus öffentlicher Verwaltung und Privatwirtschaft die Anwendung der TR-RESISCAN. Aktuell liegt Version 1.1 mit Stand vom 02.03.2017 vor. Die technische Richtlinie besteht aus einem modularen Anforderungs- und Maßnahmenkatalog und beschreibt einen generischen Scanprozess.

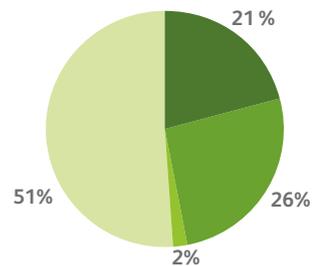
Generischer Scanprozess



Für die Integritätssicherung wird bei einem Schutzbedarf von mindestens „hoch“ bezüglich der Integrität des Scanprodukts oder falls dieses als Beweismittel vor Gericht dienen soll, der Einsatz von QES oder QESI empfohlen. Die Anforderung eines ersetzenden Scannens nach TR-RESISCAN unter Verwendung von QES beziehungsweise QESI findet sich zudem zunehmend in einschlägigen Urteilen. Gerade die Nutzung des qualifizierten elektronischen Siegels nach eIDAS bietet erhebliche Vereinfachungen, indem nur noch ein Zertifikat für die gesamte Institution benötigt wird. Insofern war es von Interesse zu prüfen, welche Rolle das ersetzende Scannen überhaupt spielt und ob die TR-RESISCAN zur Digitalisierung in der Praxis relevant ist.

Sofern eine Digitalisierung papierner Unterlagen vorgenommen wird, halten sich Aufbewahrung und Vernichtung der Papieroriginale derzeit die Waage. Mehr als die Hälfte der beteiligten Organisationen besitzt derzeit noch keine klare Strategie zur Digitalisierung papierner Dokumente. Hinsichtlich der Standards zum Scannen setzen rund 40 Prozent der Institutionen, die bereits Papierdokumente digitalisieren, auf die TR-RESISCAN. In ähnlichem Umfang werden interne Standards angewandt. Nur eine Minderheit hat hierzu noch keine klaren Vorstellungen.

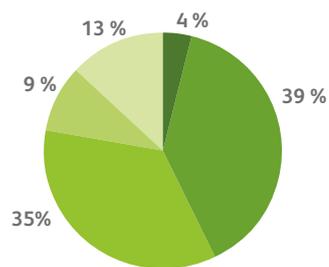
Werden in Ihrer Organisation papierne Dokumente digitalisiert?



- Ja, Papieroriginale werden anschließend langfristig aufbewahrt
- Ja, Papieroriginale werden anschließend vernichtet
- Nein
- k. A.

Mehr als die Hälfte der beteiligten Organisationen besitzt derzeit noch keine klare Strategie zur Digitalisierung papierner Dokumente.

Welche Standards werden bei der Digitalisierung papierner Dokumente berücksichtigt?



- Andere
- BSI-TR-RESISCAN
- Interne Standards
- k. A.
- Keine

Nachweisfähigkeit und Internationalität elektronischer Geschäftsprozesse

Rund die Hälfte derjenigen, die über internationale Geschäftsbeziehungen verfügen, nutzen bereits Lösungen, um Verträge, Genehmigungen etc. elektronisch abzuschließen. Nahezu der gleiche Anteil sieht den Bedarf hierfür und würde dies umsetzen, wenn entsprechende Lösungen vorliegen.

Ein wesentlicher Erfolgsfaktor der Digitalisierung von Geschäftsprozessen und damit verbunden der hierbei entstehenden geschäftsrelevanten Unterlagen, ist die Beachtung der geltenden regulatorischen Vorgaben und damit die Fähigkeit zum Nachweis geschäftlicher Entscheidungen gegenüber Gerichten, Prüfbehörden und sonstigen Dritten. Dies erfordert Wahrung und Nachweis der Authentizität, Integrität, Verfügbarkeit, Verlässlichkeit (Nachvollziehbarkeit) und vor allem Verkehrsfähigkeit der geschäftsrelevanten Unterlagen bis zum Ablauf der geltenden Aufbewahrungsfristen. Die Nutzung elektronischer Vertrauensdienste nach eIDAS erleichtert dies, zum einen durch einen einheitlichen Rechtsrahmen, zum anderen durch verbindliche internationale technische Standards. Insofern stellt sich die Frage, wie relevant die Nachweisfähigkeit für die teilnehmenden Institutionen und vor allem für diejenigen ist, die bereits digitale Prozesse nutzen oder diese ausbauen wollen.

Für 37 Prozent der Befragten besitzt die Nachweisfähigkeit elektronischer Prozesse einen erfolgskritischen, für 19 Prozent einen hohen Status. Zur Erinnerung: rund 50 Prozent der Teilnehmer setzt bereits digitale Geschäftsprozesse ein. Ebenso plant die Hälfte der Beteiligten eine (nahezu) vollständige Digitalisierung ihrer Abläufe. Für die Mehrheit dieser Institutionen ist die Nachweisfähigkeit also erfolgskritisch. Wer mit der Digitalisierung begonnen hat beziehungsweise diese ausbauen will, für den spielt der Nachweis der Abläufe eine entsprechend entscheidende Rolle.

Ein vergleichbares Bild zeigt sich bei grenzüberschreitenden Prozessen.

Sichere elektronische Kommunikation

Ein ähnliches Bild wie im vorherigen Kapitel zeigt sich bei der sicheren elektronischen Kommunikation. Um digitale Transaktionen Anfang bis Ende umzusetzen, ist die Gewährleistung von Datenschutz und Informationssicherheit in der Datenübermittlung ein nicht zu unterschätzender Faktor – ein Aspekt, wofür in Deutschland mit De-Mail oder EGVP zumindest im öffentlichen Bereich bereits Lösungsansätze entwickelt wurden.

Für 32 Prozent der Beteiligten spielt sichere Datenübermittlung an Unternehmen, Behörden sowie Privatpersonen eine erfolgskritische respektive wichtige Rolle. Auch hier wird die Einschätzung aus dem Kapitel „Nachweisfähigkeit und Internationalität elektronischer Geschäftsprozesse“ bestätigt.

Insgesamt setzen rund 50 Prozent der Teilnehmer bereits digitale Geschäftsprozesse ein. Ebenso plant die Hälfte der Beteiligten eine (nahezu) vollständige Digitalisierung ihrer Abläufe. Für die Mehrheit dieser Institutionen ist sichere Datenübermittlung mindestens von hoher Bedeutung. Wer dementsprechend mit der Digitalisierung begonnen hat und/oder diese ausbauen will, für den ist die Sicherheit der übermittelten Informationen in der elektronischen Kommunikation ein wesentlicher Erfolgsfaktor.



Umfrageergebnisse:

Umsetzungsstand elektronischer Vertrauensdienste
gemäß eIDAS-Verordnung

Umfrageergebnisse: Umsetzungsstand elektronischer Vertrauensdienste gemäß eIDAS-Verordnung

Nachdem im ersten Fragenkomplex ermittelt wurde, wie weit die Umsetzung digitaler Geschäftsprozesse in Organisationen vorangeschritten ist und damit die Voraussetzungen für die Nutzung der eIDAS-Verordnung gegeben sind, wurde durch den zweiten Teil erfragt, inwieweit die Regelungen der eIDAS-Verordnung bekannt sind und gegebenenfalls bereits umgesetzt werden.

Bekanntheitsgrad und Grundlagen der eIDAS-Verordnung

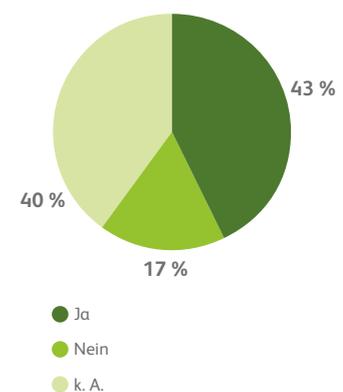
43 Prozent der Befragten sind die wesentlichen Inhalte der eIDAS bekannt. 17 Prozent kennen die Verordnung nach eigener Aussage nicht. Bei den übrigen 40 Prozent, die bei dieser Frage keine Angabe gemacht haben, ist davon auszugehen, dass auch in diesen Fällen die Regelungen eIDAS nicht geläufig sind. Dies ist insoweit nachvollziehbar, da diese Menge faktisch mit der Anzahl derjenigen korreliert, die, wie im vorigen Kapitel ausgeführt, bislang noch nicht mit der Digitalisierung begonnen haben oder hierzu noch unentschlossen sind.

In Anbetracht der Tatsache, dass es sich bei den Befragten um in diesem Bereich tätige Personen handelt und die eIDAS verpflichtende Regelungen insbesondere für öffentliche Stellen beinhaltet, ist der ermittelte Kenntnisstand auch bezüglich derjenigen, die bereits mit der Digitalisierung ihrer Prozesse begonnen oder diese abgeschlossen haben, als eher begrenzt einzustufen. Das Bewusstsein für die Relevanz und vor allem Chancen der Verordnung ist aktuell insofern noch zu stärken.

Ein ähnliches Bild zeichnet die Frage nach der Bekanntheit des Vertrauensdienstegesetzes. Hier geben lediglich 38 Prozent der Befragten an, dass sie die wesentlichen Inhalte des Gesetzes kennen. Insofern lässt sich feststellen: wer sich mit den Maßgaben zur Nutzung

43 Prozent der Befragten sind die wesentlichen Inhalte der eIDAS bekannt. 17 Prozent kennen die Verordnung nach eigener Aussage nicht.

Sind Ihnen bzw. Ihrer Organisation die wesentlichen Inhalte der eIDAS-Verordnung bekannt?



Durch das Vertrauensdienstegesetz (VDG) vom 18.07.2017 werden die Regelungen der eIDAS-Verordnung in der nationalen Gesetzgebung umgesetzt. Es löst damit das Signaturgesetz sowie die Signaturverordnung ab und bildet die nationale gesetzliche Grundlage bezüglich elektronischer Vertrauensdienste sowie elektronischer Identifizierung.

Es werden Festlegungen zu folgenden Regelungsbereichen getroffen:

- Festlegung der nationalen Aufsichtsstellen
 - Bundesnetzagentur für den Bereich der Erstellung, Prüfung, Validierung und Bewahrung von elektronischen Signaturen, Siegeln, Zeitstempels sowie elektronischer Zustelldienste
 - Bundesamt für Sicherheit in der Informationstechnik für den Bereich der Website-Authentifizierung
- Rahmenbedingungen für die Durchführung der Aufsichtspflichten der nationalen Aufsichtsstellen sowie die Mitwirkungspflichten der Vertrauensdiensteanbieter in diesem Zusammenhang
- Barrierefreiheit und Datenschutz
- Ergänzende Attribute in qualifizierten Zertifikaten für elektronische Signaturen und Siegel (u.a. Regelungen für Vertreter und Pseudonyme)
- Verpflichtung zur Unterrichtung von Personen, die planen, Vertrauensdienste zu nutzen
- Schaffung der Möglichkeit und Gründe für den Widerruf eines Zertifikats
- Übergangsvorschriften bzgl. der Regelungen des Signaturgesetzes

elektronischer Vertrauensdienste befasst hat, kennt die wesentlichen juristischen Rahmenbedingungen. Mit Blick auf Regelungsumfang und Auswirkungen der Verordnung auf sichere elektronische Prozesse besteht jedoch noch Aufklärungsbedarf bei Behörden und Unternehmen.

Die folgenden Fragen nach spezifischen Regelungsinhalten der Verordnung wurden nur denjenigen Befragten angezeigt, die angaben, die eIDAS-Verordnung zu kennen (43 Prozent).

Fünf Prozent der befragten Organisationen ist bekannt, dass

- jede qualifizierte elektronische Signatur (QES) von zertifizierten europäischen Vertrauensdiensteanbietern (VDA) das *Schriftformerfordernis in Deutschland* und in der EU erfüllt.
- *qualifizierte elektronische Siegel (QESI)* zum Nachweis von Authentizität und Integrität genutzt werden können.
- gemäß der eIDAS-Verordnung *nicht zwingend deutsche Vertrauensdiensteanbieter (VDA)* genutzt werden müssen.

Keine der befragten Organisationen gab an, dass

- ihnen die Möglichkeit zur Erzeugung von *Serversignaturen* bekannt ist.
- ihnen die *Verpflichtung öffentlicher Stellen zur Annahme und Verarbeitung* von qualifizierten elektronischen Signaturen (QES) und qualifizierten elektronischen Siegeln (QESI) bekannt ist.

Insbesondere im Hinblick auf die Verpflichtung zur Annahme von QES sowie QESI, die bereits seit 01.07.2016 in Kraft ist, und die Tatsache, dass es sich bei einem Großteil der Umfrageteilnehmer um öffentliche Institutionen handelt, wird hier ein ausgeprägtes Informationsdefizit unter den Befragten sichtbar.

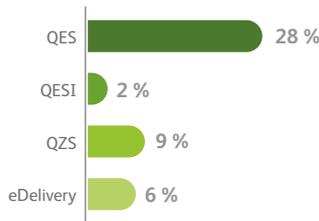
Weiterhin werden die Potenziale und Möglichkeiten, die die eIDAS im Hinblick auf durchgehende elektronische Geschäftsprozesse bietet, offensichtlich kaum bis gar nicht wahrgenommen.

Durch den Einsatz von QESI sowie von Server- und mobilen Signaturen wird die Umsetzung rechtssicherer wie nachweisbarer digitaler Transaktionen und auch die Erfüllung der Schriftformerfordernisse erheblich vereinfacht. Statt z.B. lokale Signaturen mithilfe einer personalisierten Signaturkarte der Mitarbeiter zu erstellen, können nun sowohl Server- und mobile Siegel auf Grundlage eines Organisationszertifikats, als auch mobile wie Fernsignaturen bedarfsgerecht erzeugt werden, ohne den erheblichen organisatorischen Aufwand klassischer Signaturkarten nach SigG. QESI gewährleisten hierbei den Nachweis von Authentizität und Integrität der gesiegelten Daten und erleichtern maßgeblich sowohl ein beweissicheres ersetzendes Scannen nach dem Stand der Technik als auch beispielsweise die Erstellung sicherer wie nachweisbarer elektronischer Bescheide. Vergleichbare Optimierungspotenziale lassen sich daneben durch den Einsatz qualifizierter Websitezertifikate nutzen.

Umsetzung von Vertrauensdiensten

Die folgenden Fragen zum aktuellen Einsatz von Vertrauensdiensten richteten sich wiederum an alle Befragten, um die ganzheitliche Verbreitung der Dienste zu ermitteln – unabhängig von Kenntnisstand bezüglich der eIDAS.

Welche Vertrauensdienste nutzen Sie bzw. nutzt Ihre Organisation bereits?



28 Prozent der Befragten geben an, QES einzusetzen. Neun Prozent nutzen zudem QZS sowie sechs Prozent elektronische Zustelldienste. Betrachtet man die Tatsache, dass die Verwendung von QES und QZS bereits seit 1997 durch das nicht mehr geltende Signaturgesetz, sowie der zentrale elektronische Zustelldienst De-Mail bereits seit 2011 durch das De-Mail-Gesetz geregelt und ermöglicht werden, ist die Verbreitung als relativ gering zu bewerten. Angesichts des im vorigen Kapitel festgestellten Informationsbedarfs hinsichtlich der Neuerungen und Erleichterungen der eIDAS-Verordnung ist dies jedoch nachvollziehbar. Die geringe Verbreitung von QESI (zwei Prozent) korreliert auch mit der bereits genannten Feststellung, dass der Beweiswert wie auch die leichtere Nutzung eines QESI, durch den Bezug auf ganze Organisationen statt einzelne Mitarbeiter nur sehr wenigen Befragten bekannt ist.

Werden Vertrauensdienste in Anspruch genommen, so nutzen die meisten Befragten die Dienstleistungen von deutschen Vertrauensdiensteanbietern (VDA). Nur zwei bis vier Prozent geben an, für den Einsatz von QES, QESI oder QZS die Angebote eines ausländischen VDA zu nutzen. Dies bestätigt wiederum die zuvor erläuterten Ergebnisse, wonach nur einem Bruchteil der Befragten (5 Prozent) bekannt ist, dass durch die eIDAS die Möglichkeit besteht, die Dienste jedes (qualifizierten) VDA, also auch aus anderen Mitgliedstaaten in Anspruch zu nehmen, ohne rechtliche Nachteile. Durch diese Öffnung können sich umfassende Vorteile für die Anwender ergeben – insbesondere im Hinblick auf eine günstigere Preisentwicklung sowie ein erhöhtes Innovationspotenzial durch die Auswahl bedarfsgerechter Lösungen aus einem breiten wie heterogenen Dienstangebot.

Die fehlende Einführung und Realisierung von Projekten in Bezug zur eIDAS lässt sich nach den bisher erläuterten Erkenntnissen sowohl auf die mangelnde Digitalisierung oder Unentschlossenheit von rund 40 Prozent aller Teilnehmer, als auch auf das fehlende Bewusstsein bei den befragten Institutionen bezüglich der Möglichkeiten, die die eIDAS im Rahmen der Digitalisierung von Geschäftsprozessen bietet, zurückführen.

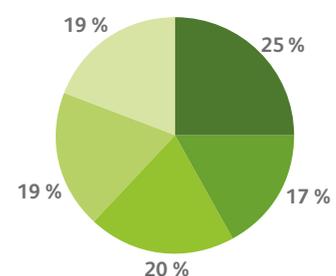
Unterstützungsbedarfe

Nicht nur die fehlenden Informationen sind ein Hemmnis für die Umsetzung von eIDAS-Projekten. Die Schwierigkeiten, auf die Organisationen nach eigenen Angaben bei der Umsetzung der eIDAS stoßen, sind vielfältig: Sie reichen von der Bewertung von marktgängigen Lösungen über organisatorische Fragestellungen und Unsicherheiten bezüglich der Rechtssicherheit elektronischer Vertrauensdienste bis zu technischen Umsetzungsproblemen.

Der geringe Bekanntheitsgrad der eIDAS sowie die genannten Hemmnisse aus Anwendersicht, die eine Umsetzung der eIDAS erschweren, offenbaren Unterstützungsbedarf bei den betroffenen Institutionen. Nach gewünschten Unterstützungsleistungen gefragt, sind sowohl Informationsveranstaltungen, als auch Best-Practice-Beispiele und spezifische Beratungsangebote gewünscht.

Gefragt nach einer ganzheitlichen Umsetzung der eIDAS in den relevanten Organisationen, geben 58 Prozent der Befragten an, noch keine konkreten Projekte zur Umsetzung der eIDAS durchgeführt zu haben. In fünf Prozent der befragten Organisationen ist eine Umsetzung der eIDAS weitestgehend oder vollständig erfolgt.

Welche Unterstützung wünschen Sie sich bzw. wünscht sich Ihre Organisation bei der Umsetzung von Maßnahmen?



- Informationsveranstaltungen/Konferenzen
- Best Practices der Aufsichtsbehörden
- Best Practices von Branchenverbänden
- Übergreifende Beratungsangebote (z.B. initiiert durch Aufsichtsbehörden/Branchenverbände)
- Spezifische Beratung



Bericht aus der Praxis – eIDAS in einer europäischen Bank

Die Autoren sprachen mit **Anja Schaffer, Cross Entity Project Management bei BNP Paribas.**

Was ist beziehungsweise war Ihre Motivation, sich mit der eIDAS zu beschäftigen? Bitte beschreiben Sie Ihren Anwendungsfall.

Die Digitalisierung unserer Geschäftsprozesse ist eines der strategischen Ziele von BNP Paribas und dementsprechend auch Thema der gruppenweiten Initiativen in Deutschland. Im Rahmen dieser Initiativen wurde das Projekt zur Einführung eines Dokumentenmanagement-Systems basierend auf SharePoint als zentrale Plattform gestartet. Neben der Einführung einer zentralen Scan-Strecke und dem Management von Dokumenten ist als zweiter Schritt die Einführung von ersetzendem Scannen zusammen mit einer sicheren und beweiswerterhaltenden Archivierung geplant. Die Pilotierung erfolgte für ausgewählte Prozesse am Standort Frankfurt/Main und wurde in fachlichen und technischen Fragen von BearingPoint unterstützt.

Start war eine detaillierte IST-Analyse für drei Organisationseinheiten. Bereits in den ersten Gesprächen stellte sich heraus: Für den Projekterfolg ist nicht die Toolfokussierung von Bedeutung, sondern vor allem die Analyse der organisatorischen Rahmenbedingungen mit dem Ziel der Papierreduzierung. Einer der Hauptgründe für die Verwendung von Papier ist dabei die Notwendigkeit von Unterschriften. Demzufolge kann ein vollständig elektronischer Prozess bis hin zum Kunden nur durch die Einführung der elektronischen Unterschrift erfolgen.

Ebenso ist eine ersetzende Digitalisierung im Posteingang essenziell, um die weiterhin in Papierform eingehenden Dokumente der Kunden so früh wie möglich zu digitalisieren und gleichzeitig Aufwand und Kosten für die Papierlagerung einzusparen.

Für uns als international tätiges Unternehmen ist die eIDAS-Verordnung die wesentliche juristische Basis für die Umsetzung der beiden UseCases (eUnterschrift und ersetzendes Scannen), um auch eine Übertragbarkeit und Anwendbarkeit in anderen Einheiten von BNP Paribas zu gewährleisten. Im Fokus stand dabei die Anwendung qualifizierter Vertrauensdienste (qualifizierte elektronische Signatur und Siegel) hinsichtlich der Rechts- und Beweissicherheit.

Der Start für eIDAS-konforme Vertrauensdienste sollte als Grundlage für die internen Prozesse und digitalen Kundenakten im Inputmanagement (ersetzendes Scannen) erfolgen. Geplant war ein sicherer Scanprozess auf Basis einer dezidierten Verfahrensdokumentation sowie der Verwendung eines qualifizierten elektronischen Siegels zur Integritätssicherung. Die technische Lösung sollte sowohl Siegel als auch Signaturen erzeugen können, also erweiterbar sein für weitere Anwendungsfälle, insbesondere die eUnterschrift (QES/QESI/QZS).

Umgesetzt sind aktuell das DMS sowie das reine technische Scannen und automatische Indizieren von Dokumenten. Die Einführung der Vertrauensdienste ist derzeit im Projektstatus.

Welche Herausforderungen stellten sich und welche Lessons Learned sehen Sie?

Die Kommunikation im Vorfeld und während des Projektes im Sinne von Change Management ist notwendig und wichtig, insbesondere innerhalb der verschiedenen relevanten Gruppen (Fachbereich, Management, IT, Vendors, Legal & Compliance).



- **Fachbereich:**

Die größte Herausforderung im Fachbereich war vor allem die Verständigung, was die Digitalisierung der Geschäftsprozesse und Kundenakten für die Kolleginnen und Kollegen bedeutet. Rollenspiele hinsichtlich Projektarbeit und SOLL-Prozess helfen dabei, ein Gefühl für die Veränderungen (Projekt, Prozess und Arbeitsumfeld) zu schaffen und die Anforderungen bzw. Schnittstellen besser zu identifizieren (Design Thinking).

- **Management:**

Das Management muss als Innovationstreiber in dem Digitalisierungsprozess eine aktive Rolle spielen. Dabei sollten eigene Gewohnheiten wie zum Beispiel die Nutzung eines qualifizierten elektronischen Siegels statt personenbezogener qualifizierter eSignatur den Prozess unterstützen. Des Weiteren obliegt es dem Management, Überzeugungsarbeit für das Projekt zu leisten, besonders im Hinblick auf den multinationalen Konzern mit zentraler IT und Stakeholdern mit unterschiedlichem Erfahrungshintergrund.

- **IT:**

Die Beweiswerterhaltung signierter Dokumente ist gemäß eIDAS verpflichtend, stellt jedoch für den IT-Bereich die größte Veränderung dar. Hier ist die Unterstützung durch das Management wichtig, um die neuen Vorgaben und Anforderungen der langfristigen Nachweisbarkeit digitaler Prozesse und digitaler Unterlagen erfolgreich zu implementieren.

- **Legal & Compliance:**

Für Legal und Compliance gilt es ein gemeinsames Verständnis zu schaffen, um Siegel statt Signatur zu erlauben, wenn die qualifizierte elektronische Signatur nicht zwingend notwendig ist. Ein Umdenken von personenbezogener Signatur auf die Organisationssignatur muss hier stattfinden. Auch aus diesen Bereichen sind kompetente Ansprechpartner erforderlich, die juristische und technische Vorgaben an einen sicheren Scanprozess unter Verwendung der QES/QESI zur Integritätssicherung kennen, oder bereit sind sich kurzfristig einzuarbeiten. Diese Bereitschaft war bei BNP Paribas vorhanden und für das Projekt von großer Bedeutung.

Welche Potenziale über den bisherigen Anwendungsfall hinaus sehen Sie in der eIDAS respektive der Vertrauensdienste?

Potenziale sehe ich im Aufbau eines konzernweiten IT-Dienstes für qualifizierte elektronische Signaturen und Siegel und hier exemplarisch für folgende Anwendungsfälle:

- Procurement/Vertragsmanagement
- HR
- Wichtige Freigabeprozesse

Unser Ziel ist die Umsetzung vollständig digitaler, vertrauenswürdiger und medienbruchfreier Geschäftsprozesse mit Kommunikationspartnern und Kunden.

Fazit und Handlungsempfehlungen

Die Ergebnisse der Umfrage zum Umsetzungsstand elektronischer Vertrauensdienste gemäß eIDAS-Verordnung in Deutschland zeigen ein kritisch zu bezeichnendes Bild.

Trotz E-Government-Gesetz des Bundes sowie Pendanten auf Länderebene mit entsprechenden Verpflichtungen zur Einführung digitaler Prozesse, sei es durch Vorgaben hinsichtlich der E-Akte, Zugangseröffnungen für sichere elektronische Kommunikation oder die qualifizierte elektronische Signatur, ist ein Großteil der Befragten bislang noch unsicher, ob und wenn ja wie digitalisiert werden soll.

Besonders interessant dabei ist, dass dies nicht nur auf den Public Sector, sondern auch auf Unternehmen zutrifft. Durch die Vertrauensdienste der eIDAS wird für den digitalen europäischen Binnenmarkt, der immerhin rund ein Viertel des weltweiten Bruttoinlandsprodukts erwirtschaftet, die Basis für vertrauenswürdige wie sichere elektronische Transaktionen und Prozesse geschaffen. In diesem Zusammenhang identifiziert das ermittelte Bild mögliche Nachteile deutscher Institutionen gegenüber anderen europäischen Ländern, in denen die Digitalisierung weiter vorangeschritten ist, wie zum Beispiel die skandinavischen Länder, Österreich, die Benelux-Länder oder die baltischen Staaten. Wie in der Begründung, die der eIDAS vorangestellt ist, sehr deutlich wird, sieht die EU (vertrauenswürdige) elektronische Dokumente, authentische Datenquellen (was technisch derzeit faktisch nur mit Vertrauensdiensten realisierbar ist) und eID-Lösungen² als wesentliche Erfolgsfaktoren an, die es auszubauen gilt. eID-Lösungen wurden in der Umfrage nicht betrachtet, da diese Regelungen der eIDAS erst ab September 2018 greifen.

Um Medienbrüche zu vermeiden, sind die Gewährleistung einer sicheren wie nachweisbaren Übertragung geschäftsrelevanter Unterlagen, der Nachweis von Authentizität und Integrität der Daten wie des Ausstellers beziehungsweise Empfängers sowie eine sichere wie nachvollziehbare Identifizierung und Authentisierung der Beteiligten essentiell. Ziel ist es, hierdurch das Ausdrucken und händische Unterschreiben durch den Sender ebenso zu vermeiden wie das aufwändige Scannen beim Empfänger. Dies muss in einem pragmatischen Ausgleich von Sicherheit und Nachvollziehbarkeit mit einer mobilen wie nutzerfreundlichen Lösung einhergehen, die die erforderliche Akzeptanz beim Anwender erreicht. Genau hierfür bieten die Regelungen der eIDAS mit mobilen QES, elektronischen Siegeln, Websitezertifikaten sowie Einschreib- und Zustelldiensten entsprechende Lösungen an – dank eIDAS kann dabei jeder, auch ausländische Dienst, genutzt werden, um eine bedarfsgerechte Digitalisierung zu ermöglichen.

Die Tatsache, dass sowohl diese erleichterte Umsetzung vollständig digitaler Prozesse auf Basis der Vertrauensdienste, als auch die Verpflichtung zur Annahme und Prüfung jeder, auch ausländischer QES/QESI, nur einem ausgewählten Teilnehmerkreis bekannt ist, spricht für einen hohen Bedarf an Informationen und Unterstützung bei der Realisierung sicherer digitaler Transaktionen in Behörden und Unternehmen. Dieser Umstand kam zudem bei der direkten Frage nach Unterstützungsbedarfen zum Ausdruck. Die festgestellte Zurückhaltung bei der Nutzung von QES spiegelt diesen Informationsbedarf wider. Dass elektronische Signaturen kein Hindernis für die Digitalisierung darstellen, zeigt sich an Ländern wie Österreich, in denen diese flächendeckend genutzt werden. Hier ist bereits seit Jahren keine Signaturkarte für die Erzeugung von QES mehr notwendig. Ebenso wird seit längerem mit der Amtssignatur ein faktisches elektronisches Siegel eingesetzt, um beispielsweise behördliche Bescheide rechts- und beweissicher elektronisch abzuwickeln.

Ein Bewusstsein der Anwender für die Chancen der eIDAS ist unerlässlich, um die Digitalisierung voranzutreiben und neue Geschäftsmodelle zu ermöglichen (zum Beispiel ad-hoc-Verträge, digitale Zulassungsverfahren, elektronische Zeugnisse oder den leichteren übergreifenden Datenaustausch, wie im Gutachten des Normenkontrollrats gefordert³).

Es gilt, die Anwender insbesondere über die Möglichkeiten und Vereinfachungen, die die eIDAS bietet zu informieren.

Dabei handelt es sich u.a. um folgende:

- Qualifiziertes elektronisches Siegel mit einem Zertifikat für die ganze Organisation statt je Mitarbeiter
- Fern- und Serversignaturen sowie mobile Signaturen ohne aufwändige Nutzung einer Signaturkarte
- Möglichkeit zur Nutzung der Vertrauensdienste aller europäischen (qualifizierten) Anbieter
- Innovative Identifizierungsverfahren wie VideoIdent oder durch den Sachbearbeiter der Behörde beziehungsweise des Unternehmens, wie zum Beispiel in der Finanzindustrie bereits genutzt, statt der bisherigen Verfahren

² Vergleiche <https://ec.europa.eu/digital-single-market/en/news/eu-egovernment-report-2016-shows-online-public-services-improved-unevenly>

³ Vergleiche <https://www.normenkontrollrat.bund.de/Webs/NKR/Content/DE/Pressemitteilungen/2017-10-06-nkr-gutachten-2017.html>

Erste Umsetzungen dieser Art bestehen in Deutschland sowohl in Behörden als auch Unternehmen, zum Beispiel im Versicherungsumfeld. Nur scheinen diese nicht allgemein bekannt zu sein, sodass eine Nachnutzung im größeren Umfang bisher nicht erfolgt.

Möglicherweise spielen auch rechtliche Unsicherheiten bei den Umfrageteilnehmern eine Rolle, die zur bisher niedrigen Umsetzung der eIDAS führen. Ein Aspekt ist, dass die Nutzung des Siegels zur Erfüllung der Schriftform in Deutschland bisher nicht möglich ist. Wie eine Studie der Bundesdruckerei aufzeigte⁴, würden entsprechende rechtliche Anpassungen erhebliche Vereinfachungen für Behörden und Unternehmen mit sich bringen. Auch ohne diese spezifischen Regelungen bezüglich des Schriftformersatzes lassen sich die Chancen mobiler elektronischer Unterschriften, sicheren Datenaustauschs mit Website-zertifikaten und des einfachen ersetzenden Scannens mit Siegeln bereits heute nutzen.

Ebenso erscheint, angesichts der historisch bedingten Zurückhaltung gegenüber elektronischen Signaturen, ein gewisser Pragmatismus seitens der für die Zertifizierung nationaler Vertrauensdienste verantwortlichen Aufsichtsbehörden notwendig. Wie die vorliegende Umfrage zeigt, steigt die Nutzung elektronischer Unterschriften und vergleichbarer Dienste mit dem Grad der Digitalisierung. Sicherheit und Benutzerfreundlichkeit sind die wesentlichen Erfolgsfaktoren vollständig digitaler Transaktionen. Die durch die Anerkennungspflicht mögliche Inanspruchnahme ausländischer Anbieter erzeugt insoweit einen Wettbewerbsdruck auf deutsche Vertrauensdiensteanbieter – dieser lässt sich nur mit gesundem Pragmatismus lösen.

Zum September 2018 greifen die Vorgaben zur verbindlichen Anerkennung aller notifizierten eID-Systeme. Mit der Verpflichtung zur Zugangseröffnung für den neuen Personalausweis, wie er in nahezu allen E-Government-Gesetzen definiert ist, stellt sich die Maßgabe zur Annahme aller europäischen, notifizierten eID in Deutschland definitiv. Angesichts des ermittelten niedrigen Bekanntheitsgrads und Umsetzungsstands der Vertrauensdienste, besteht in Deutschland erheblicher Handlungsdruck, um in der Digitalisierung in Europa keine Nachteile zu erleiden. Die entsprechenden Produkte und Marktteilnehmer sind, wie die folgende Marktanalyse zeigt, bereits umfassend vorhanden. Es gilt nur noch, den Schritt in eine vertrauenswürdige wie vor allem medienbruchfreie Digitalisierung zu gehen.

Als Maßnahmen zur Unterstützung auf diesem Weg sind denkbar:



⁴ Vergleiche https://www.bundesdruckerei.de/de/system/files/dokumente/pdf/bdr_Umfrage_eIDAS.pdf

Abkürzungsverzeichnis

Abkürzung	Bedeutung
B2B	Business to Business
beA	besonderes Anwaltspostfach
beN	besonderes Notarpostfach
bePo	besonderes Behördenpostfach
BImA	Bundesanstalt für Immobilienaufgaben
BNetzA	Bundesnetzagentur
DMDA	De-Mail-Diensteanbieter
DMS	Dokumentenmanagementsystem
eANV	elektronischer Abfallnachweis
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
eIDAS	EU-Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen
G2B	Government to Business
G2B2C	Government to Business to Citizen
HSM	Hardware Sicherheitsmodul
IAM	Identity- & Access Management
KIS	Krankenhausinformationssystem
LBA	Luftfahrtbundesamt
PVS	Patientenverwaltungssoftware
QES	Qualifizierte elektronische Signatur
QESI	Qualifiziertes elektronisches Siegel
QM	Qualitätsmanagement
QZS	Qualifizierter elektronischer Zeitstempel
SigG	Signaturgesetz
SigV	Signaturverordnung
VDA	Vertrauensdiensteanbieter
VDG	Vertrauensdienstgesetz
VPS	Virtuelle Poststelle
ZPO	Zivilprozessordnung



Anhang: Marktübersicht I

Anbieter	procilon IT-Solutions GmbH	Adobe Systems GmbH	intarsys AG	DocuSign	secrypt GmbH	Giesecke+Devrient Mobile Security GmbH
Unternehmensdaten						
Straße	Leipziger Str. 110	Georg Brauchle-Ring 58	Kriegsstr. 100	9-15 Rue Maurice Mallet	Bessemerstr. 82	Prinzregentenstr. 159
Ort	Taucha	München	Karlsruhe	Issy-les-Moulineaux - Frankreich	Berlin	München
PLZ		80992	76133		12103	81677
URL	www.procilon.de	www.adobe.com	www.intarsys.de	www.docusign.de/	www.secrypt.de	www.gi-de.com
<i>zentraler Ansprechpartner Vertrauensdienste</i>	Jürgen Vogler	Rüdiger Herfrid	Markus Schuster	Sofia VILELA	Tatami Michalek	Werner Bschorr
Phone	+49 34298 4878 10	+49 89 31705 215	+49 721 38479-15	+33 1 73 05 28 69	+49 30 7565978-0	+49 89 4119-2608
Mobile		+491728280215	+49 172 7260732	+33 6 42 90 44 65	+49 162 2004252	+49 176 24 22 22 04
E-Mail	jürgen.vogler@procilon.de	rherfrid@adobe.com	mschuster@intarsys.de	sofia.vilela@docusign.com	tatami.michalek@secrypt.de	werner.bschorr@gi-de.com
<i>technische Ansprechpartner</i>	Mark Rüdiger	Stanislav Rosahatsky	Jörg Steinbach		Matthias Schlede	wie zentraler Ansprechpartner
Function	Business Development	Solution Consultant			Head of Research and Development	Produktmanagement
Phone	+49 34298 4878 10	+49-89-31705-197			+49 30 7565978-0	
Mobile						
E-Mail	mark.ruediger@procilon.de	rosahats@adobe.com	jsteinbach@intarsys.de		matthias.schlede@secrypt.de	
<i>Art des Anbieters</i>	Lösungsanbieter	Lösungsanbieter	Lösungsanbieter	Lösungsanbieter und qualif. Vertrauensdiensteanbieter	Lösungsanbieter	Lösungsanbieter
<i>Kundenkreise</i>						
Public Sector	ja	ja	ja	ja	ja	ja
HealthCare	ja	ja	ja	ja	ja	ja
Finance	ja	ja	ja	ja	ja	ja
Industry	ja	ja	ja	ja	ja	ja
Weitere	Utility		cross-industry	cross-industry	Justiz	ja
Portfolio						
fortgeschrittene elektronische Signatur	ja	ja	ja	ja	ja	ja
qualifizierte elektronische Signatur	ja	ja	ja	ja	ja	ja
fortgeschrittenes elektronisches Siegel	ja	ja	ja	ja	ja	ja
qualifiziertes elektronisches Siegel	ja	ja	ja	ja	ja	ja
fortgeschrittene elektronische Zeitstempel	ja	ja	ja	ja	ja	ja
qualifizierte elektronische Zeitstempel	ja	ja	ja	ja	ja	ja
mögliche Vertrauensdiensteanbieter						
QES (VDA)						
national	ja	ja	ja	ja	ja	ja
international	nein	ja	ja	ja	ja	nein
QESI (VDA)						
national	ja	ja	ja	ja	ja	ja
international	nein	ja	ja	ja	ja	nein

Satz-Rechen-Zentrum (SRZ)	DE-CODA GmbH	PrimeKey	Mentana-Claimsoft GmbH	Governikus KG	Bundesdruckerei GmbH	SecCommerce
Besemerstr. 82	Marienburger Str. 1	Krantzstr. 7	Griesbergstr. 8	Am Fallturm 9	Kommandantenstr. 15	Oberhauptstr. 5
Berlin	Berlin	Aachen	Bad Salzdetfurth	Bremen	Berlin	Hamburg
12103	10405	52070	31162	28359	10969	22335
www.srz.de	www.de-coda.de	www.hprimekey.com	www.mentana.de	www.governikus.com	www.bundesdruckerei.de	www.seccommerce.com
Hans-Joachim Hübner	Annette Floren	Andreas Philipp	Ina Gellner	Olaf Rohstock	Enrico Entschew	Falk Goossens
+49 30 753 01 - 379	+49 30 21 91 59 11	+49 151 23882818	+49 5063 27744-0	+49 421 204 95 965	+49 30 25983070	
+49 171 286 14 21		+49 151 23882818				
h-j.huebner@srz.de	floren@de-coda.de	andreas.philipp@primekey.com	ina.gellner@mentana.de	olaf.rohstock@governikus.com	enrico.entschew@bdr.de	falk.goossens@seccommerce.com
wie zentraler Ansprechpartner	wie zentraler Ansprechpartner	Martin Oczko	Jürgen Ludyga	Marc Horstmann	Frank Steinfeld	wie zentraler Ansprechpartner
Head of Solutions and Sales		Product Manager PKI Appliance	Product Owner	Prokurist	Bereichsleiter Trust Service Management	
		+49 151 25298693	+49 5063 27744-0	+494212049538	+49 30 25983952	
		+49 151 25298693				
		martin.oczko@primekey.com	juergen.ludyga@mentana.de	marc.horstmann@governikus.com	frank.steinfeld@bdr.de	
Lösungsanbieter	Lösungsanbieter	Lösungsanbieter	Lösungsanbieter	Lösungsanbieter	Lösungsanbieter und qualif. Vertrauensdiensteanbieter	Lösungsanbieter
ja	ja	ja	ja	ja	ja	ja
ja	nein	ja	ja	ja	ja	ja
ja	nein	ja	ja	nein	ja	nein
ja	nein	ja	ja	nein	ja	ja
ja; Real Estate, Housing Companies	nein	ja, Utilities, Cloud Service Provider, Telecommunication	ja, IT-Lösungsanbieter	nein	nein	nein
ja	ja	ja	ja	ja	ja	ja
ja	ja	nein	nein	ja	ja	ja
ja	nein	ja	ja	ja	nein	ja
ja	nein	nein	nein	ja	ja	ja
ja	nein	ja	ja	ja	nein	ja
ja	nein	nein	nein	ja	ja (qualif. VDA)	ja
ja	ja	nein	ja (fortgeschritten)	ja	ja	ja
nein	nein	ja (fortgeschritten)	nein	ja	nein	ja
ja	nein	nein	ja (fortgeschritten)	ja	ja	ja
nein	nein	ja (fortgeschritten)	nein	ja	nein	nein

Anhang: Marktübersicht II

Anbieter	procilon IT-Solutions GmbH	Adobe Systems GmbH	intarsys AG	DocuSign	secript GmbH	Giesecke+Devrient Mobile Security GmbH
QZS (VDA)						
national	ja	ja	ja	ja	ja	ja
international	nein	ja	ja	ja	ja	nein
Produkteigenschaften						
<i>Lösungen zur Identifizierung</i>						
Inhouse		reine Cloudlösung				
QES						
VideoIdent	nein	nein	ja	ja	ja	nein
PostIdent	ja	nein	nein	nein	ja	nein
persönlich	ja	nein	ja	ja	ja	ja
eID	nein	nein	ja	nein	nein	nein
weitere	nein	nein	nein	ja	nein	nein
QESI						
VideoIdent	nein	nein	ja	nein	nein	nein
PostIdent	ja	nein	nein	nein	ja	nein
persönlich	ja	nein	ja	nein	ja	ja
eID	nein	nein	ja	nein	nein	nein
weitere	nein	ja, Plattform für Zugang zu verschiedenen qualif. VDA	nein	ja (Prüfung des Unternehmens)	nein	nein
<i>Remote</i>						
QES						
VideoIdent	ja	ja	ja	ja	ja	ja
PostIdent	nein	nein	nein	nein	nein	nein
eID	ja	ja	ja	nein	nein	nein
weitere	nein	nein	nein	ja	nein	nein
QESI						
VideoIdent	ja	ja	ja	nein	nein	ja
PostIdent	nein	nein	nein	nein	nein	nein
eID	ja	ja	ja	nein	nein	nein
weitere	nein	ja	nein	ja (Prüfung des Unternehmens)	nein	nein
		alle einbinden, Plattform für Zugang zum QTSP qualif. VDA				
<i>Lösungen zur Authentisierung (herstellerübergreifende Übersicht der möglichen Lösungen (es werden faktisch alle von den Herstellern angeboten))</i>						
Inhouse	Inhouse: 2-Faktor z. B.: Software-Token wie Kerberos, SAML (Siegel [Endnutzer nach Freischaltung der Karte], HSM), Hardware-Token (Chipkarte), PKI, MobileTAN,					
Remote	Remote: 2-Faktor z. B.: MobileTAN, MobileID, SW-Token wie Kerberos oder SAML					
<i>mögliche Formate (Erzeugung)</i>						
QES/QESI						
CAdES	ja	nein	ja	ja	ja	k.A.
XAdES	ja	nein	ja	ja	ja	k.A.
PAdES	ja	ja	ja	ja	ja	k.A.
ASiC	nein	nein	nein	ja	nein	k.A.
<i>mögliche Formate (Prüfung)</i>						
QES/QESI						
CAdES	ja	ja	ja	ja	ja	ja
XAdES	ja	ja	ja	ja	ja	ja
PAdES	ja	ja	ja	ja	ja	ja
ASiC	nein	nein	nein	ja	nein	ja
QZS (Erzeugung und Prüfung)	ja	ja	ja	k.A.	ja	ja
Schnittstellen zu Geschäftsanwendungen						

Satz-Rechen-Zentrum (SRZ)	DE-CODA GmbH	PrimeKey	Mentana-Claimsoft GmbH	Governikus KG	Bundesdruckerei GmbH	SecCommerce
ja	nein	nein	ja (fortgeschritten)	ja	ja	ja
nein	nein	ja (fortgeschritten)	nein	ja	nein	ja
nein	nein	nein	ja	nein	nein	ja
ja	ja	nein	ja	ja	ja	ja
ja	ja	nein	ja	ja	ja	nein
nein	nein	nein	ja	ja	nein	nein
ja, Notarident	nein	ja (fortgeschritten)	ja	nein	ja, Notarident	nein
nein	entfällt	nein	nein	nein	nein	nein
ja	entfällt	nein	nein	ja	ja	ja
nein	entfällt	nein	nein	ja	nein	nein
nein	entfällt	nein	nein	nein	nein	nein
ja, Notarident	entfällt	ja (fortgeschritten)	nein	nein	nein	nein
ja	nein	nein	ja	nein	ja	ja
nein	nein	nein	ja	nein	nein	ja
ja	nein	nein	ja	nein	ja	nein
nein	nein	nein	nein	nein	nein	nein
nein	entfällt	nein	nein	nein	nein	nein
nein	entfällt	nein	nein	nein	nein	ja
nein	entfällt	nein	nein	nein	nein	nein
nein	entfällt	nein	nein	nein	nein	nein
NotarIdent						
ja	k.A.	fortgeschritten	fortgeschritten	ja	ja	ja
ja	k.A.	ja	ja	ja	ja	ja
ja	k.A.	ja	ja	ja	ja	ja
ja	k.A.	ja	nein	nein	ja	ja
ja	k.A.	ja	ja	ja	ja	ja
ja	k.A.	ja	ja	ja	ja	ja
ja	k.A.	ja	ja	ja	ja	ja
ja	k.A.	ja (fortgeschritten)	ja	ja	ja (qualif. VDA)	ja

Anhang: Marktübersicht III

Anbieter	procilon IT-Solutions GmbH	Adobe Systems GmbH	intarsys AG	DocuSign	secrypt GmbH	Giesecke+Devrient Mobile Security GmbH
----------	----------------------------	--------------------	-------------	----------	--------------	--

Schnittstellen zu Geschäftsanwendungen

ERP	ja	ja	ja (SAP, SEEBURGER AG, SEAL Systems AG, Somentec Software GmbH)	ja, SAP und Lösungen marktführender Integriertoren	ja, SAP etc.	ja (Kundenlösung)
ECM	ja	ja	ja (u.a. d.velop, ELO, windream, Alfresco, rubicon IT GmbH, SEAL Systems AG, SharePoint)	ja, OpenText, IBM, OnBase und Lösungen marktführender Integriertoren	ja, SharePoint etc.	ja (Kundenlösung)
weitere	ja (Fachverfahren) Lösung für: <ul style="list-style-type: none"> • IAM zwecks Zugang zu Onlinediensten einer Behörde/eines Unternehmens resp. mehreren • Onlinebereitstellung von Services basierend auf den Securitylösungen von procilon: wie z.B. Zeitstempelservice, Signaturservice (bis hin zu QES), Signaturprüfung, sichere Kommunikation z.B. Mailverschlüsselung • Einbindung der Fernsignaturlösung (resp. weiterer Dienste) von VDA über die Plattform und Nutzung der jeweiligen technischen Lösungen für die Fernsignatur (VideoIdent+MobileTAN), Abruf des Zertifikats und Nutzung mit der SAK von procilon • Einbindung unterschiedlicher VDA möglich • Transparente Integration in Unternehmens-IT und damit Abbildung vollständiger G2B/B2B-Prozess möglich • Nutzung der Plattformservices in Abhängigkeit unterschiedlicher Identifizierungslevel (E-Mail, Videoident, Personalausweis) 	ja	ja (u.a. Fachverfahren, KIS)	ja, CRM, HR, Finanzlösungen	KIS und Archiv (z.B. AGFA HealthCare, Cerner, Marabu, synedra, März), diverse PVS, Scansoftware, Labor, Fachverfahren etc.	ja (Kundenlösung)

Anwendungsfälle

QES						
ersetzendes Scannen	ja	nein	ja	ja	ja (u.a. LBA; BImA)	ja (Kundenlösung)
eUnterschrift	ja	ja	ja	ja	ja, u.a. Verträge (eContracts), Arbeitnehmerüberlassungen, Geschäftskorrespondenz, Arztbriefe, Befunde, Laboranforderungen, Patientenakten und Telekonsile (auch Telekonzile)	ja (Kundenlösung)
weitere	nein	ja	u.a. eArztbrief	ja	ja, Qualitätsmanagementdokumente, QM-Dokumente, Abfallnachweisdokumente (eANV), Konstruktionszeichnungen, Baupläne	ja (Kundenlösung)
QESI						
ersetzendes Scannen	nein (bisher keine Kunden)	k.A.	ja	k.A.		ja (Kundenlösung)
eUnterschrift	nein (bisher keine Kunden)	k.A.	ja	k.A.	ja, u.a. eVergabe, Bescheide, Urkunden, Zeugnisse	ja (Kundenlösung)
weitere	nein (bisher keine Kunden)	k.A.	Integritätssicherung beim Posteingang	k.A.	ja, u.a. Massenbelege, z.B. E-Rechnungen, Kontoauszüge	ja (Kundenlösung)
QZS						
ersetzendes Scannen	nein	nein	ja	entfällt	k.A.	ja (Kundenlösung)
eUnterschrift	nein	nein	ja	entfällt	ja, u.a. Onlineklausuren	ja (Kundenlösung)
weitere	ja (Posteingang, Beweiserhaltung)	ja	Integritätssicherung beim Posteingang	entfällt	ja, u.a. archivnahes Zeitstempeln, z.B. Patientenakten	ja (Kundenlösung)

Satz-Rechen-Zentrum (SRZ)	DE-CODA GmbH	PrimeKey	Mentana-Claimsoft GmbH	Governikus KG	Bundesdruckerei GmbH	SecCommerce
---------------------------	--------------	----------	------------------------	---------------	----------------------	-------------

ja, SAP, Oracle etc.	k.A.	ja	ja, Salesforce, SAP	ja	ja, gängige ERP-Systeme wie z.B. SAP	ja, Integration der gängigen, marktführenden Produkte
ja, Ceyoniq, Optimal Systems, OpenText DOMEA etc. (offene XML-Schnittstelle)	k.A.	ja	ja, Optimal Systems enaio, Lobo DMS, D3, SAP, IBM	ja	ja, gängige ECM-Systeme	ja, Integration der gängigen, marktführenden Produkte
k.A.	k.A.	ja, BuildServer Archivierung	ja, Ephesoft Transact, Kodak capture, Kofax, IBM Content Manager	ja, Langzeitarchive	k.A.	ja, Integration der gängigen, marktführenden Produkte

|--|--|--|--|--|--|--|

ja	k.A.	ja	ja	ja	ja	ja
k.A.	k.A.	k.A.	ja	ja	ja	ja
ja, Dokumente/Bescheinigungen Unfallkassen	k.A.	ja, Notariatsservice	k.A.	k.A.	ja, z.B. Arztbrief, Zeugnisse, Ursprungszeugnis, Exportbescheinigungen etc.	k.A.
ja (u.a. LBA; BImA)	entfällt	k.A.	ja	ja	ja	k.A.
k.A.	entfällt	k.A.	ja	ja	k.A.	k.A.
k.A.	entfällt	k.A.	ja	k.A.	ja, z.B. Beglaubigungen	ja
k.A.	entfällt	k.A.	ja	k.A.	k.A.	k.A.
k.A.	entfällt	k.A.	ja	k.A.	k.A.	k.A.
k.A.	entfällt	k.A.	k.A.	Posteingang	ja, Archivzeitstempel	k.A.

Anhang: Marktübersicht IV

Anbieter	procilon IT-Solutions GmbH	Adobe Systems GmbH	intarsys AG	DocuSign	secript GmbH	Giesecke+Devrient Mobile Security GmbH
Beweiswerterhaltung						
TR-ESOR	ja	nein	nein	nein	ja	ja
LTANS-ERS	nein	nein	ja	nein	ja	ja
weitere	nein	ja	nein	nein	nein	nein
Integration						
ERP	ja	ja	ja	entfällt	ja	ja (Kundenlösung)
ECM	ja	ja	ja	entfällt	ja	ja (Kundenlösung)
weitere	ja	ja	ja	entfällt	ja, E-Archiv-Lösungen (z.B. AGFA HealthCare, Cerner, Marabu, synedra, März)	ja (Kundenlösung)
Anwendungsfälle						
ersetzendes Scannen	ja	k.A.	k.A.	entfällt	ja	ja (Kundenlösung)
IT-Dienst	ja (i.V.m. VPS)	k.A.	ja	entfällt	ja	ja (Kundenlösung)
Weitere	ja (TrustCenter)	k.A.	k.A.	entfällt	ja	ja (Kundenlösung)
eDelivery						
De-Mail	ja	k.A.	k.A.	nein	nein	nein
Integration QES	ja	k.A.	k.A.	nein	nein	nein
Integration QESI	ja	k.A.	k.A.	nein	nein	nein
Integration QZS	ja	k.A.	k.A.	nein	nein	nein
Integration						
ePoststelle	ja	k.A.	k.A.	entfällt	entfällt	entfällt
ERP	ja	k.A.	k.A.	entfällt	entfällt	entfällt
ECM	ja	k.A.	k.A.	entfällt	entfällt	entfällt
weitere	ja	k.A.	k.A.	entfällt	entfällt	entfällt
UseCases	Integration De-Mail, EGVP, beA, beN, beBPo, AS2, AS4 und viele weitere in Mailsysteme und Fachverfahren	k.A.	k.A.	entfällt	entfällt	entfällt

Satz-Rechen-Zentrum (SRZ)	DE-CODA GmbH	PrimeKey	Mentana-Claimsoft GmbH	Governikus KG	Bundesdruckerei GmbH	SecCommerce
ja (über Partner)	nein	nein	ja	ja	ja (über Partner)	
ja (über Partner)	nein	nein	nein	ja	ja (über Partner)	ja
nein	nein	nein	nein	nein	nein	ja
ja (über Partner)	entfällt	entfällt	ja, SAP, Salesforce	ja	ja (über Partner)	ja, Integration der gängigen, marktführenden Produkte
ja (über Partner)	entfällt	entfällt	ja, Optimal Systems enaio, D3, Lobo DMS, SAP	ja	ja (über Partner)	ja, Integration der gängigen, marktführenden Produkte
k.A.	entfällt	entfällt	ja, Oracle, filebasierte Ablage	nein	k.A.	ja, Integration der gängigen, marktführenden Produkte
ja (RESISCAN)	entfällt	entfällt	ja, Krankenkassen, Kliniken	ja	ja (über Partner)	ja, (Altakten)
k.A.	entfällt	entfällt	k.A.	ja	ja (über Partner)	k.A.
k.A.	entfällt	entfällt	ja, Unfallversicherung, Sozialkassen, Versicherungen, Banken, Kliniken, Behörden, Krankenkassen, Kliniken	ja, E-Akte, eRechnung, Fachverfahren	k.A.	k.A.
ja (über Partner)	nein	nein	ja	ja	ja (via Partner: Mentana Claimsoft)	k.A.
ja (über Partner)	nein	nein	ja	ja	ja (via Partner: Mentana Claimsoft)	k.A.
ja (über Partner)	nein	nein	ja	ja	ja (via Partner: Mentana Claimsoft)	k.A.
ja (über Partner)	nein	nein	ja	ja	ja (via Partner: Mentana Claimsoft)	k.A.
ja (über Partner)	entfällt	entfällt	k.A.	ja	k.A.	k.A.
ja (über Partner)	entfällt	entfällt	ja, Salesforce, SAP	ja	ja (via Partner: Mentana Claimsoft)	k.A.
ja (über Partner)	entfällt	entfällt	ja, OS enaio, D3, Lobo DMS, SAP	k.A.	ja (via Partner: Mentana Claimsoft)	k.A.
ja (über Partner)	entfällt	entfällt	ja, Capture-/ Inputmanagement lösungen	k.A.	ja (via Partner: Mentana Claimsoft)	k.A.
	entfällt	entfällt	De-Mail Portal, De-Mail Gateway inkl. EGVP, beBPo bei voller Integration in MS Outlook und Archivschnittstelle in DMS etc.	ja, Einbindung DMDA bzw. Einschreib- und Zustelldienste in ePoststelle	s. Partner Mentana Claimsoft	k.A.

Kontakt



Stefan Zimmermann
Partner
BearingPoint
stefan.zimmermann@bearingpoint.com



Steffen Tampe
Director
BearingPoint
steffen.tampe@bearingpoint.com



Dr. Matthias Flügge
Leiter Geschäftsbereich
Digital Public Services
Fraunhofer FOKUS
matthias.fluegge@fokus.fraunhofer.de



Steffen Schwalm
Researcher
Digital Public Services
Fraunhofer FOKUS
steffen.schwalm@fokus.fraunhofer.de

Autoren:

Theresa Vogt (BearingPoint), Steffen Schwalm (Fraunhofer FOKUS)

© 2018 BearingPoint GmbH, Frankfurt/Main. Alle Rechte vorbehalten. Gedruckt in der EU. Der Inhalt dieses Dokuments unterliegt dem Urheberrecht. Veränderungen, Kürzungen, Erweiterungen und Ergänzungen, jede Veröffentlichung, Übersetzung oder gewerbliche Nutzung zu Schulungszwecken durch Dritte bedarf der vorherigen schriftlichen Einwilligung durch BearingPoint GmbH, Frankfurt/Main. Jede Vervielfältigung ist zum persönlichen Gebrauch gestattet und nur unter der Bedingung, dass dieser Urheberrechtsvermerk beim Vervielfältigen auf dem Dokument selbst erhalten bleibt. WP_1184_DE

Über BearingPoint

BearingPoint ist eine unabhängige Management- und Technologieberatung mit europäischen Wurzeln und globaler Reichweite. Das Unternehmen agiert in drei Bereichen: Consulting, Solutions und Ventures. Consulting umfasst das klassische Beratungsgeschäft, Solutions fokussiert auf eigene technische Lösungen in den Bereichen Digital Transformation, Regulatory Technology sowie Advanced Analytics, und Ventures treibt die Finanzierung und Entwicklung von Start-ups voran. Zu BearingPoints Kunden gehören viele der weltweit führenden Unternehmen und Organisationen. Das globale Netzwerk von BearingPoint mit mehr als 10.000 Mitarbeitern unterstützt Kunden in über 75 Ländern und engagiert sich gemeinsam mit ihnen für einen messbaren und langfristigen Geschäftserfolg.

Für weitere Informationen: www.bearingpoint.com

Über Fraunhofer FOKUS

Das Fraunhofer Institut für Offene Kommunikationssysteme (FOKUS) erforscht und entwickelt die vernetzte Welt – sicher, zuverlässig und vertrauenswürdig. Der Geschäftsbereich Digital Public Services unterstützt Politik, Verwaltung und Wirtschaft bei der strategischen Umsetzung von interoperablen und sicheren IKT-Lösungen im öffentlichen Raum und in der öffentlichen Verwaltung.

Behörden und öffentlichen Einrichtungen bietet FOKUS Leistungen von der Bestandsaufnahme bestehender Strukturen über strategische Planung, Machbarkeitsstudien, und Architekturkonzepte bis hin zur Unterstützung bei der Ausschreibung, Implementierung und Einführung neuer IT-Systeme. Der Wirtschaft hilft FOKUS, Technologien und Lösungen auf die Bedürfnisse des öffentlichen Sektors auszurichten und diese in herstellerübergreifende Anwendungsszenarien einzubinden.

Für weitere Informationen: www.fokus.fraunhofer.de/dps

