Fraunhofer FOKUS

Dienste auf Basis elektronischer Safes für Daten und Dokumente

Dr. Sönke E. Schulz
Christian Hoffmann
Jens Klessmann
Andreas Penski
Thomas Warnecke

ISPRAT
Interdisziplinäre Studien zu Politik, Recht, Administration und Technologie e.V.

Berlin/Kiel, 2010

Dienste auf Basis elektronischer Safes für Daten und Dokumente

Eine Untersuchung gefördert durch den ISPRAT e.V.

Durchgeführt von

Fraunhofer-Institut
für offene Kommunikationssysteme (FOKUS)
Kaiserin-Augusta-Allee 31
10589 Berlin
www.fokus.fraunhofer.de

Lorenz-von-Stein-Institut für Verwaltungswissenschaften
an der Christian-Albrechts-Universität zu Kiel
Olshausenstraße 40
24098 Kiel
www.lorenz-von-stein-institut.de

Autoren:
Dr. Sönke E. Schulz
Christian Hoffmann
Jens Klessmann
Andreas Penski
Thomas Warnecke

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Zusammenfassung

Mit Hilfe elektronischer Safes für Daten und Dokumente zur Ablage und Freigabe digitaler Unterlagen wird eine Infrastruktur etabliert, mit der der Austausch zwischen Verwaltung, Wirtschaft und Bürgern einfacher und schneller möglich wird. Die Abwicklung organisationsübergreifender digitaler Geschäftsprozesse wird mit dem Einsatz elektronischer Safes vereinfacht. Unternehmen, die für ein Verwaltungsgeschäft benötigte Daten und Dokumente in einem elektronischen Safe ablegen und gezielt freigeben, ermöglichen den beteiligten Behörden einen unkomplizierten Zugriff. Die notwendigen Bescheide erhält der Antragsteller durch eine sichere und verbindliche elektronische Zustellung in seinen eigenen Safe.

In der vorliegenden Untersuchung wird aufgezeigt, welche rechtlich-organisatorischen und technischen Maßnahmen geeignet sind, ein hohes Schutzniveau für Daten und Unterlagen zu gewährleisten. Im Ergebnis der Arbeit wurden folgende potentielle Dienste auf Basis elektronischer Safes für Daten und Dokumente identifiziert und untersucht:

- **Dienste externer Anbieter:** Diese setzen die Freigabe der benötigten Daten durch den Safeeigentümer voraus. Der Dienstanbieter hat dabei uneingeschränkten lesenden Zugriff auf diese Freigabe.
- **Lokale Dienste:** Hierbei wird am vertrauenswürdigen System des Safeeigentümers der Safeclient um Plugins für verschiedene Aufgaben erweitert. Die Plugins können die unverschlüsselten Daten lokal, auf dem vertrauenswürdigen System des Safenutzers lesen, analysieren und weiter verarbeiten.
- Die vorrangige Funktion von **Integrationsdiensten** ist das Vergrößern der Datenbasis, der in elektronischen Safes gespeicherten Informationen durch Anbindung verschiedener Datenquellen.

Elektronische Safes und darauf basierende Dienste werden sich aller Voraussicht nach allerdings nur durchsetzen, wenn Anbieter, Safe und Dienste durch einen geeigneten gesetzlichen Rahmen reglementiert werden. Ein solcher muss dabei vor allem die Aspekte der Datensicherheit, der Datenvertraulichkeit und der Datenverfügbarkeit adressieren. Vorhandene Regelungskomplexe (bspw. BDSG und BSI-Zertifizierungen) sind dazu bereichsspezifisch fortzuentwickeln. Sachgerecht erscheinen darüber hinaus eine eigenständige Akkreditierung vertraulicher Safeanbieter sowie effektive Instrumente einer staatlichen repressiven Kontrolle. Vorhandene Ansätze (bspw. der De-Mail-Gesetzentwurf) sollten dabei aufgegriffen und vor allem um safespezifische Vorgaben ergänzt werden. Angesichts der fehlenden 100-prozentigen Sicherheit informationstechnischer Systeme und elektronischer Safes kann ein Rechtsrahmen der Akzeptanzsteigerung dienen, Rechtsunsicherheiten abbauen und so

einen Einsatz auch in und durch die öffentliche Verwaltung forcieren. So kommen beispielsweise der Nachweisbarkeit (elektronischer) Zustellungen, Fragen der Zugangseröffnung und ähnlichem in Verwaltungsverfahren erhebliche Bedeutung zu. Der flächendeckende Einsatz von Safe-Kommunikation und Diensten ohne eine Anpassung der rechtlichen Grundlagen und – wie heute – ausschließlich basierend auf einzelfallbezogener Rechtsprechung erscheint wenig wahrscheinlich.

2. Einleitung

Mit der vorliegenden, vom Verein für Interdisziplinäre Studien zu Politik, Recht, Administration und Technologie (ISPRAT) geförderten Untersuchung werden Potentiale der digitalen Aufbewahrung von Daten und Dokumenten sowie darauf aufbauende Dienste untersucht. Dem interdisziplinären Ansatz von ISPRAT folgend, erfolgt die Betrachtung aus technischer und rechtlicher Perspektive. Die durchführenden Einrichtungen, das Fraunhofer-Institut FOKUS und das Lorenz-von-Stein-Institut für Verwaltungswissenschaften der Christian-Albrechts-Universität zu Kiel, haben hierzu aktuelle Entwicklungen in den Domänen Trusted Computing, Identitätsmanagement[1], Datenschutz und den Anwendungsfeldern E-Government und E-Business analysiert.

2.1. Notwendigkeit der vertraulichen Aufbewahrung und Bereitstellung elektronischer Daten und Dokumente

Elektronische Safes für Daten und Dokumente zur Ablage und Freigabe digitaler Unterlagen bieten eine Infrastruktur, um den Austausch zwischen Verwaltung, Wirtschaft und Bürgern zu vereinfachen und zu beschleunigen[2]. Unternehmen, die für ein Verwaltungsgeschäft benötigte Dokumente in einem elektronischen Safe ablegen, vereinfachen den beteiligten Behörden einen Zugriff. Die notwendigen Bescheide erhält der Antragsteller durch eine sichere und verbindliche elektronische Zustellung in seinen Safe. Als Komponente zur Umsetzung der EU-Dienstleistungsrichtlinie[3] ermöglichen elektronische Safes zudem ein vereinfachtes und datenschutzkonformes Fallmanagement[4].

Grundlage für eine Benutzung elektronischer Safes, welche von IT-Dienstleistern betrieben werden, ist das Vertrauen in die Sicherheit und den Schutz der sensiblen Daten. Der technische Verlust, unerlaubte interne und externe Zugriffe sowie unkontrollierte Verbreitung vertraulicher Unterlagen müssen unbedingt vermieden werden. Aktuelle Meldungen zur Verbreitung vertraulicher Datensätze verdeutlichen den Handlungsbedarf.

---

1 Aus rechtlicher Perspektive *Sönke E. Schulz*, Rechtsprobleme des Identitätsmanagements“, DuD 2009, S. 601-606.

2 Zur Ausgangssituation auch *Sönke E. Schulz/Jens Klessmann*, Elektronische Daten- und Dokumentensafes – Rechtliche und technische Koordinaten für einen erleichterten Bürgerkontakt, Datareport 3/2009, S.28-31.

3 RL 2006/123/EG v. 12.12.2006 über Dienstleistungen im Binnenmarkt, ABl L 376 v. 27.12.2006, 36; grundlegend dazu Schliesky (Hrsg.), Die Umsetzung der EU-Dienstleistungsrichtlinie in der deutschen Verwaltung – Teil I: Grundlagen, 2008; Teil II: Verfahren, Prozesse, IT-Umsetzung, 2009; Teil III: Wissen, Information, Verantwortung, 2010.

4 Breitenstrom, Christian; Eckert, Klaus-Peter; Lucke, Jörn von; Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS; Interdisziplinäre Studien zu Politik, Recht, Administration und Technologie e.V. (ISPRAT) (Hrsg.) (2008): IT-Umsetzung der EU-Dienstleistungsrichtlinie – Gestaltungsoptionen, Rahmenarchitektur, technischer Lösungsvorschlag - White Paper Version 2.0. Stuttgart: Fraunhofer IRB-Verl. (FOKUSbasic).

Zur umfänglichen Realisierung der Potentiale elektronischer Dienstleistungen im öffentlichen Sektor ist eine Ausrichtung auf Prozesse von wesentlicher Bedeutung. Eine Abkehr von der Aufgaben- und Organisationsorientierung, verbunden mit organisationsübergreifenden Wertschöpfungsketten, kann helfen, die Grenzen einzelner Einrichtungen mit IT-basierten Prozessen zu überwinden.

Traditionell richtet sich die öffentliche Verwaltung an öffentlichen Aufgaben und an zu deren Erfüllung eingerichteten Behörden aus. Ämter und ihre Abteilungen sind entsprechend zugeschnitten. Diese Orientierung führt zu einer Sichtweise auf Prozesse, die häufig an den Organisationsgrenzen einzelner Verwaltungen endet. Im Zeitalter IT-basierter Prozesse erweist sich diese aufgabenorientierte Sichtweise als zu eng. Vielfach sind die Verwaltungsabläufe ein Ausschnitt aus größeren Prozessen, die über die Grenzen von Organisationen und Verwaltungsebenen hinweg führen.

Besonders Unternehmen müssen regelmäßig zur Erfüllung gesetzlicher Melde- und Informationspflichten interne Vorarbeiten (Nachweise) leisten. Nach Abschluss der Verwaltungsvorgänge fließen die Ergebnisse (Bescheide) wiederum in interne Prozesse der Unternehmen ein, werden aber auch als Nachweise für weitere Verwaltungsvorgänge benötigt. Insofern findet ein Zusammenspiel von öffentlichem und privatem Sektor statt, das umso flüssiger und fehlerfreier ablaufen kann, je weniger Unterbrechungen und Medienbrüche auftreten. Im Interesse eines leistungsfähigen Standorts Deutschland ist daher eine prozessorientierte Ausrichtung des öffentlichen Sektors und eine Prozessinfrastruktur notwendig. Die Orientierung auf Prozesse erlaubt eine umfassendere Ausschöpfung vorhandener Potentiale des Electronic Government. Unterschiedliche Verfahren und IT-Systeme können entlang von Prozessen zu einem System integriert werden. Da Prozesse sich in ihren Grundbestandteilen ähneln, können standardisierte Komponenten und Architekturen Verwendung finden. Die Bildung durchgängiger Prozesse setzt die Bereitstellung von Daten in einheitlichen Formaten und über standardisierte Schnittstellen voraus. Die Weitergabe elektronischer Daten entlang organisationsübergreifender Prozessketten stellt eine Herausforderung für den Datenschutz dar. Elektronische Safes und darauf basierende Dienste können den Übergang zu einer Prozessorientierung und zu übergreifenden Prozessketten zwischen Wirtschaft und Verwaltung unterstützen und beschleunigen.

Prozesse und Prozessbausteine lassen sich zu neuartigen Prozess- und Wertschöpfungsketten verknüpfen, etwa auf Basis von Prozessanalysen, indem diese gestrafft oder in eine neue Reihenfolge gebracht werden, indem Vorgangsschritte wegfallen, hinzukommen oder parallel durchgeführt sowie indem Verfahren vereinfacht werden oder wegfallen.

Elektronische Safes bilden die Grundlage dafür, dass Safeeigentümer die Kontrolle über ihre in digitale Prozesse eingebundenen Daten behalten. Bei elektronischen Behördengängen können aus dem Safe heraus gezielt die von der Verwaltung benötigten Daten und Dokumente freigegeben werden. Mitarbeiter der Verwaltung oder automatisierte Prozesse greifen bei Bedarf auf diese freigegebenen Daten zu. Mit einem digitalen Rechtemanagement könnten Safeeigentümer genaue Vorgaben hinsichtlich der Verwendung ihrer Daten treffen. So könnten Daten ausschließlich für den laufenden vertrauenswürdigen Prozess lesbar sein, sofern durch die Prozessmodellierung sichergestellt ist, dass der Prozess die Daten aus dem Safe nicht an andere Prozesse oder Fachverfahren weiterreicht, sondern stattdessen auf die Daten im Safe referenziert. Zugriffe außerhalb des Prozesses wären nicht oder nur eingeschränkt (und nach Freigabe des Eigentümers) möglich. Dies setzt die Einführung eines Prozesstypregisters und die darin gepflegten Berechtigungszertifikate der Prozesstypen voraus, was eher der langfristigen Vision des nutzerzentrierten Prozessmanagements zuzuordnen ist.

Sicherheit und Vertraulichkeit im elektronischen Geschäftsverkehr

In der Kommunikation von Behörden und Gebietskörperschaften untereinander und mit Bürgern und Unternehmen werden zunehmend elektronische Daten und Dokumente ausgetauscht. Gerade im Austausch zwischen öffentlicher Verwaltung und Unternehmen besteht die Notwendigkeit eine Vertraulichkeit der Übermittlung sicherzustellen. Verschiedene Ansätze existieren hierzu bereits oder befinden sich derzeit in der Umsetzung. Beispielsweise findet bei Gerichten in Deutschland das Elektronische Gerichts- und Verwaltungspostfach (EGVP)[5] Anwendung. Dieses Angebot erlaubt die Zustellung von Dokumenten durch Verfahrensbeteiligte, wie zum Beispiel Unternehmen und Rechtsanwälte, in elektronischer, rechtswirksamer Form an teilnehmende Institutionen der Justiz oder Verwaltung. Für die Umsetzung des EGVP wurde dabei auf den OSCI-Standard der deutschen öffentlichen Verwaltung zurückgegriffen[6]. Das EGVP wurde allerdings, wie auch die De-Mail, primär zur Übermittlung von Einzelnachrichten entwickelt. Elektronische Safes und darauf basierende Dienste setzen demgegenüber perspektivisch auf eine direkte Integration von Daten und Dokumenten in übergreifende Prozesse. Mit dem Projekt De-Mail[7] verfolgt das Bundesministerium des Innern die Entwicklung eines Dienstes, welcher eine elektronisch verbindliche Kommunikation zwischen Behörden, Unternehmen und Bürgern ermöglicht. Hierzu bieten u.a. herkömmliche E-Mail-Provider, welche sich einer speziellen Zertifizierung un-

[5] Weitere Informationen zum Elektronischen Gerichts- und Verwaltungspostfach unter: http://www.egvp.de/.

[6] Weitere Informationen zum OSCI-Standard bietet zum Beispiel die OSCI-Leitstelle unter: http://www.osci.de.

[7] Weitere Informationen zu De-Mail unter: http://www.de-mail.de.

terzogen haben, einen besonders gesicherten Postfach- und Versanddienst an. De-Mails werden über beidseitig authentisierte und verschlüsselte Kommunikationskanäle verschickt. Eine Transportverschlüsselung der Inhalte erfolgt automatisiert durch die De-Mail-Provider. Weiterhin können De-Mail-Provider optional auch einen Safedienst (im ursprünglichen Gesetzentwurf als „sicherer Speicherplatz“ bezeichnet) und einen Identitätsbestätigungsdienst anbieten. Ein Einsatz des De-Safes über die Funktion einer „Online-Festplatte“ hinaus zur direkten Kommunikation mit behördlichen Prozessen ist derzeit nicht vorgesehen.

Identitätsmanagement

Mit der Zunahme elektronischer Prozesse in allen Lebensbereichen werden immer mehr Daten zur eigenen Identität in digitale Vorgänge eingespeist. Damit wird die zuverlässige und vertrauliche Verwaltung dieser Daten zusehends zur Herausforderung. Die Kontrolle der mit den verschiedenen (Teil-) Identitäten verbundenen Informationen und Eigenschaften gestaltet sich bisher oft für Benutzer ohne Expertenwissen schwierig. Mit Unterstützung eines Systems zum Identitätsmanagement soll es einfacher werden, die Identitätseigenschaften vertraulich zu verwalten[8]. Elektronische Safes können bei der Umsetzung einer Infrastruktur für ein Identitätsmanagement eine wesentliche Rolle spielen, in dem die Nutzer im Mittelpunkt stehen. Mit Hilfe des eigenen elektronischen Safes können neben Dokumenten auch diese Daten gezielt für einzelne Diensteanbieter und Geschäftsprozesse freigegeben werden. Mit der Sicherheit und Vertraulichkeit der elektronischen Safes erhalten Bürgerinnen und Bürger ein Werkzeug, das sie befähigt, sich vergleichsweise einfach in der digitalen Welt zu bewegen. Gleichzeitig werden zur Implementierung elektronischer Safes Mechanismen des Identitätsmanagements wie Rollenkonzepte oder Logging Services benötigt.

2.2. Ziele des ISPRAT-Projektes

Deutschland verfügt im Kern über eine gute und in vieler Hinsicht auch vorbildliche öffentliche Verwaltung. Wesentliche Vorhaben zur Modernisierung haben in den letzten Jahren viele Verwaltungsvorgänge vereinfacht und beschleunigt. Die Arbeit großer Teile der deutschen Verwaltung wäre mittlerweile ohne Informations- und Kommunikationstechnologien nicht mehr denkbar. An der Schnittstelle zu den externen Kunden der Verwaltung ist der Austausch von Daten und Dokumenten vielfach allerdings noch mit Medienbrüchen verbunden.

[8] S. auch *Sönke E. Schulz*, Der neue „E-Personalausweis – elektronische Identitätsnachweise als Motor des E-Government, E-Commerce und des technikgestützten Identitätsmanagement?, CR 2009, S. 267-272.

Elektronische Safes für Daten und Dokumente können den Austausch zwischen Bürgern, Wirtschaft und öffentlicher Verwaltung vereinfachen und eine preiswerte Zustellung vertraulicher Unterlagen ermöglichen. Solche Safes sind auf modernen Informations- und Kommunikationstechnologien basierende und über elektronische Medien erreichbare virtuelle Schließfächer zur Ablage, Verwaltung und Freigabe elektronischer Dokumente. Diese Safes können verschiedene Ausprägungen haben und in der Verfügungsgewalt von Bürgern, Verwaltung oder weiteren Dritten stehen. Wesentlich zur erfolgreichen Etablierung solcher Systeme ist das Vertrauen der potentiellen Nutzer in die hochsichere Ablage ihrer sensiblen Daten. Die Absicherung durch technische Vorkehrungen kann dabei allerdings nur ein Teil der Lösung sein. Datensicherheit- und -schutz bedürfen immer auch zuverlässiger rechtlich-organisatorischer Grundlagen.

Zur Ansiedlung des Betriebs elektronischer Safes im privatwirtschaftlichen Raum muss daher zunächst die Grundlage für ein besonderes Vertrauensverhältnis zwischen Betreibern und Nutzern geschaffen werden. Es ist zu prüfen, inwieweit dieses Vertrauensverhältnis mittels technischer Vorsorgemaßnahmen gewährleistet und welche rechtlichen Rahmenbedingungen und Organisationsstrukturen zusätzlich entwickelt werden müssten, um unbefugte interne und externe Zugriffe auf die Safes der Kunden auszuschließen.

Ziel des Projektes ist es, in einem Gesamtkonzept aufzuzeigen, welche rechtlich-organisatorischen und technischen Grundvoraussetzungen notwendig sind, das für eine rechtssichere Kommunikation im E-Government und E-Business erforderliche hohe Schutzniveau für Daten und Dokumente zu erreichen. Im Ergebnis der Arbeit werden potentielle Dienste auf Basis elektronischer Safes für Daten und Dokumente identifiziert und aus technischer sowie rechtlicher Perspektive untersucht. Abschließend erfolgt die Darstellung des elektronischen Safes und ausgewählter Dienste im Rahmen unterschiedlicher Anwendungsszenarien.

Die Rechtsfragen des Einsatzes elektronischer Safes, von Datennotardiensten sowie allgemein des Identitätsmanagements wurden im Teilprojekt des Lorenz-von-Stein-Instituts ausführlich begutachtet. Die Ergebnisse werden im Sommer 2010 in der Reihe „Schriften zur Modernisierung von Staat und Verwaltung“ dokumentiert und der Fachöffentlichkeit zur Verfügung gestellt (Schliesky (Hrsg.) 2010: „Rechtsfragen des Identitätsmanagements“, Kiel 2010).

Die ursprüngliche Fokussierung des Projektes auf die Entwicklung einer vor allem aus organisatorisch-rechtlicher Perspektive sicheren Instanz („Datennotar“), die den elektronischen Safe anbietet oder zumindest überwacht, hat sich im Projektverlauf als wenig sinnvoll erwiesen. Zum einen wurde seit Projektbeginn die technische Ausgestaltung elektronischer Safes so fortentwickelt,

dass von einem neuen Niveau bezüglich Datensicherheit und –schutz ausgegangen werden kann. Trotz einer verbesserten technischen Sicherheit kommt der Ausgestaltung der organisatorischen und rechtlichen Rahmenbedingungen eine gewisse Bedeutung zu, da kein technisches System vollständige Sicherheit gewährleisten kann. Zum anderen stellte sich in Gesprächen und insbesondere Workshops mit einer wesentlichen Zielgruppe, den Notaren, heraus, dass der ursprüngliche Ansatz nicht sachgerecht gewesen wäre. Auch unterscheidet sich das bisherige Aufgabenprofil der Notare von der im Rahmen der Studie zu entwickelnden Perspektive, die vielmehr eine Verortung elektronischer Safes im privatrechtlichen Raum bei gleichzeitiger Sicherstellung der Vertraulichkeit und Akzeptanz durch staatliche Reglementierung und Überwachung nahelegt. Denkbar erscheint aber eine Einbindung der Notare bei einzelnen Diensten (beispielsweise als Trusted Third Party oder im Kontext der vertraulichen und beweissicheren Digitalisierung analoger Dokumente). Auf der Grundlage dieser vorläufigen Untersuchungsergebnisse wurde die Zielstellung des Projektes von den Partnern, wie oben beschrieben, angepasst und um die Analyse weiterer Dienste ergänzt.

2.3 Struktur der Studie

Die vorliegende Studie gliedert sich in sieben Kapitel.

In Kapitel 2 werden die Rahmenbedingungen, Ziele und die Struktur der vorliegenden Studie skizziert.

In Kapitel 3 werden die Grundlagen elektronischer Safes und Safeanbieter dargelegt. Die Darstellung der Anforderungen an elektronische Safes erfolgt aus technischer Sicht.

Im anschließenden Kapitel 4 werden Dienste sowohl auf Basis als auch unter Einbeziehung elektronischer Safes exemplarisch vorgestellt und diskutiert.

Die rechtlichen Aspekte der Akkreditierung von Safeanbietern, von elektronischen Safes und deren Einsatz vor allem im E-Government werden in Kapitel 5 erläutert.

In Kapitel 6 wird anhand potentieller Anwendergruppen beispielhaft verdeutlicht, wie elektronische Safes und damit verbundene Dienste in der Praxis eingesetzt werden und welche Zielgruppen davon profitieren können.

Abschließend werden in Kapitel 7 die Untersuchungsergebnisse zusammengefasst und ein Ausblick auf die weitere Entwicklung gegeben.

3. Elektronische Safes

3.1. Verständnis elektronischer Safes

„Verbrieften Rechten“[9] und anderen werthaltigen Daten und Dokumenten kommt in der gesellschaftlichen Entwicklung eine bedeutende strukturbildende Rolle zu. Entsprechend hoch ist deren Schutzbedarf[10]. Zur langfristigen Sicherung werden diese daher in Safes gelegt. Mit Blick auf die Entwicklung moderner Informations- und Kommunikationstechnologien und insbesondere auf die zunehmende Digitalisierung weiter Teile des gesellschaftlichen Lebens stellt sich die Frage, wie ein solcher Schutz künftig zu realisieren ist. Benötigt wird ein elektronisches Äquivalent zu physischen Tresoren, welches den gleichen langfristigen Schutz vor Verlust der eingestellten Daten sowie vor unberechtigter Einsichtnahme garantiert. Der Umgang mit einem elektronischen Safe ist dabei für den Safeeigentümer möglichst einfach zu gestalten. Zudem eröffnet die Übertragung in die digitale Welt Zusatzfunktionalitäten, die herkömmliche Safes nicht zur Verfügung stellen können.

Elektronische Safes bieten dem Eigentümer unbedingte Vertraulichkeit der eingestellten Informationen. Sie sind durch gesetzliche und organisatorische Rahmenbedingungen sowie durch technische Maßnahmen vor unberechtigten Zugriffen langfristig geschützt. Nur durch die Einwilligung des Eigentümers können Informationen von Dritten eingesehen, bzw. an diese weitergegeben werden. Kryptographische Methoden garantieren dabei eine Ende-zu-Ende-Verschlüsselung zwischen den Kommunikationspartnern. Ein web-basierter Zugriff auf die Inhalte des elektronischen Safes ist damit ausgeschlossen. Der Zugriff erfolgt vielmehr immer über einen dedizierten (Rich-) Client, der auf dem System des jeweiligen Nutzers installiert ist.

„Verbriefte Rechte“ müssen regelmäßig in verschiedenen gesellschaftlichen Situationen nachgewiesen werden. Dieser Nachweis erfolgt in der Regel durch Vorlage des Dokumentes oder einer beglaubigten Kopie. Der elektronische Safe bietet dem Eigentümer neben der sicheren Verwahrung von Daten und Dokumenten auch eine Freigabe- bzw. Nachweisfunktion.

Der Eigentümer kann Dritten einen feingliedrigen Zugriff auf benötigte Inhalte gewähren. Der Inhaber behält somit die Kontrolle über seine Daten. Auch der jeweilige Anbieter des Safedienstes kann nicht auf die Inhalte der elektronischen Safes zugreifen. Die im elektronischen Safe enthaltenen Protokollfunk-

[9] Unter „verbrieften Rechten“ sollen alle (Papier-) Dokumente verstanden werden, die in irgendeiner Form für den Einsatz im Rechtsverkehr bestimmt sind und Rechtswirkungen entfalten können (Bescheide, Rechnungen, Belehrungen, Verträge, Mahnungen u.v.m.).

[10] Breitenstrom u.a. (2008). White Paper Elektronische Safes für Daten und Dokumente. (S. 5 f.). Abgerufen von: http://www.fokus.fraunhofer.de/de/elan/_docs/_hpp-gruppe/esafe_white-paper_081219.pdf.

tionen erlauben dem Eigentümer Zugriffe auf seine erstellten Freigaben nachzuvollziehen.

Der hier beschriebene Ansatz des elektronischen Safes folgt dem Prinzip des „Privacy by Design“. Datenschutz und -sicherheit stellen in diesem Ansatz von Beginn an zentrale Aspekte dar. Von der Idee, der Konzeption, der Umsetzung bis hin zum anschließenden Betrieb und der späteren Außerbetriebnahme (Einstellung) werden der Schutz der Privatsphäre und die Sicherheit der Daten als bedeutende Entwicklungsziele berücksichtigt[11].

Mit dem elektronischen Safe erhält der Bürger ein Instrument zur Verwaltung seiner elektronischen Daten und Dokumente. Er garantiert dem Eigentümer eine hohe Sicherheit seiner Daten und wahrt gleichzeitig die Privatsphäre. Die Bedienung des Safes ist dabei nicht komplizierter als die Handhabung gängiger E-Mail-Programme.

Grundsätzlich kann der Safeeigentümer bei Bedarf verschiedene Safeaccounts bei unterschiedlichen Safeanbietern einrichten. Diese können über die einheitliche Benutzeroberfläche des Safeclients verwaltet werden. Kein Safeeigentümer sollte allerdings unterschiedliche Safes pflegen müssen, um mit diversen Dienstleistern Daten austauschen zu können.

Einheitliche Protokolle garantieren eine größtmögliche Interoperabilität zwischen verschiedenen Safes, Safeanbietern und Dienstleistern. Die Inhalte eines elektronischen Safes sollten bei einem Wechsel des Anbieters durch den Eigentümer einfach transferiert werden können. Eine einheitliche Safestruktur und eine standardisierte Form des Im- und Exports der Daten und Dokumente erlauben einen solchen einfachen Wechsel.

Neben der sicheren und vertraulichen Aufbewahrung sowie der individuellen Freigabe von Daten an Dritte ist die Bereitstellung dieser Daten zur Einbindung in Geschäftsprozesse ein wesentlicher Aspekt des elektronischen Safes. Über die Bereitstellung strukturierter elektronischer Daten können Prozesse zwischen Bürgern, Unternehmen und der öffentlichen Verwaltung effizient realisiert werden. Mittels medienbruchfreier Prozesse können organisationsübergreifende Vorgänge bedeutend schneller, genauer und schlussendlich kostengünstiger abgewickelt werden.

Elektronische Safes sind der Baustein einer Kommunikationsinfrastruktur, über den die verschiedenen Akteure einer umfassend vernetzten digitalen Welt ihre vertraulichen Informationen für den Einsatz in verschiedenen Situationen bereithalten.

---

[11] Hustinx, P. (19.3.2010). Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy. Abgerufen von http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf.

Der **Safeeigentümer** verwaltet dabei seine Daten und Dokumente in einem elektronischen Safe, welcher von einem **Safeanbieter** bereitgestellt wird. Der Safeeigentümer steht in einem Vertragsverhältnis mit dem Safeanbieter, welches ihm die Einhaltung gesetzlicher Aufbewahrungsfristen und technischer Dienstgütevereinbarungen (Service Level Agreements) seitens des Safeanbieters garantiert. Zugriff auf die Daten des elektronischen Safes erhalten Dritte als **Safenutzer** nur nach der Freigabe durch den Safeeigentümer. Safenutzer können andere Safeeigentümer, aber auch IT-Systeme sein, welche Daten für bestimmte Prozesse benötigen.

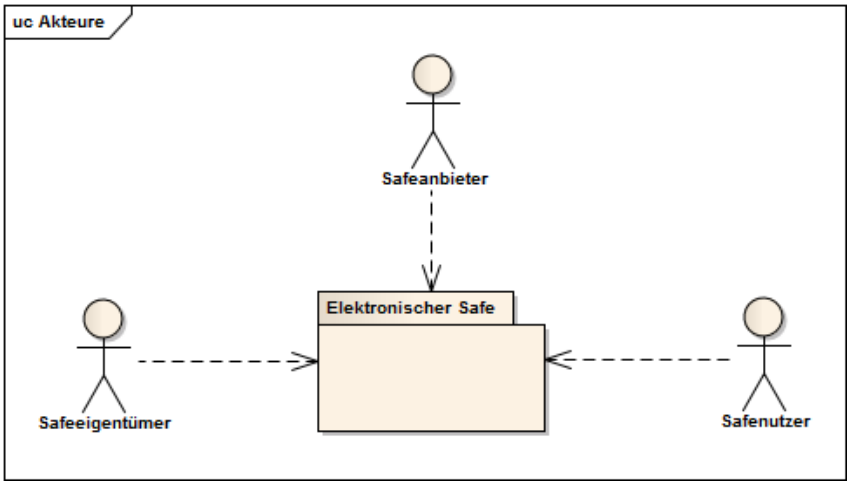

Abbildung 1: Akteure um den elektronischen Safe

3.2. Funktionale Aspekte elektronischer Safes

Für eine hohe Akzeptanz elektronischer Safes beim Bürger ist es erforderlich, den Mehrwert für den Bürger klar darzustellen. Es gibt im Wesentlichen drei Aspekte, die dem Safeeigentümer in der hier definierten Variante einen Nutzen verschaffen:

- Die Online-Verfügbarkeit von persönlichen Daten ermöglicht dem Safeeigentümer ständig seine Daten abzurufen, unabhängig vom eigenen Standort. Die komfortable Beauftragung und effiziente Abwicklung verschiedener Vorgänge unter Einbeziehung seiner persönlichen Daten in der Kommunikation mit Dritten ist jederzeit und von jedem Ort aus möglich. Voraussetzung hierfür ist der Zugriff auf die Inhalte des Safes mit Hilfe eines geeigneten Safeclients. Neben einer Desktop-Variante kann es ebenso Safeclients für mobile Endgeräte mit mehr oder weniger vollständiger Funktionalität geben.

- Weiterhin ist die sichere Aufbewahrung von elektronischen Dokumenten, die für den Safeeigentümer aktuell oder zu einem späteren Zeitpunkt von Bedeutung sein können, ein wesentlicher Vorteil für den Bürger. Die Aufbewahrung erfolgt in strukturierter Form. Der Safeei-

gentümer muss hierfür keine eigene Infrastruktur vorhalten oder sich um technische Details der Aufbewahrung sorgen. Der Safeanbieter übernimmt für den Safeeigentümer diese Aufgabe und kann zudem die Einhaltung gesetzlicher Vorschriften überwachen. Er garantiert die langfristige Verfügbarkeit und Unveränderlichkeit der eingestellten Daten und Dokumente.

- Die Freigabefunktion ermöglicht eine differenzierte Vergabe von Zugriffsrechten an Kommunikationspartner auf die Sammlung privater, schützenswerter Daten im elektronischen Safe. Durch das Festlegen von Zugriffszweck und -methoden (nur Lesen, Speichern, etc.) bleibt der Safeeigentümer Herr seiner Daten. Gegenüber der bisher praktizierten unkontrollierten Weitergabe der Daten verbessert die Nutzung eines elektronischen Safes die Privatsphäre des Eigentümers im Internet.

Die wesentlichen funktionalen Aspekte eines elektronischen Safes sind: Bereitstellung, Verwaltung von Daten, Freigabe von Daten und Dokumenten, Mailboxfunktion, Protokollierung, Trusted Third Party. Diese werden nachfolgend dargestellt und erläutert.

Bereitstellung

Der Safeanbieter stellt einem Benutzer in der Rolle des Eigentümers einen elektronischen Safe für Daten und Dokumente bereit.

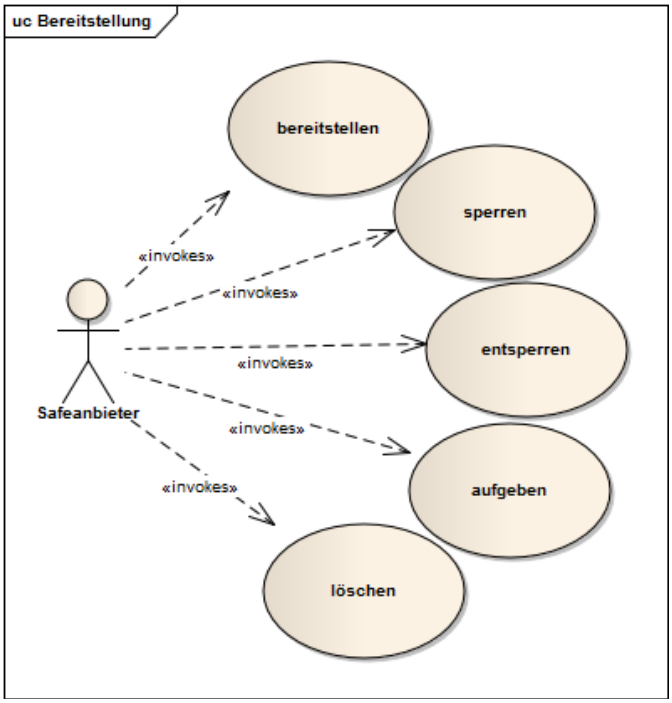

Abbildung 2: Bereitstellung elektronischer Safes

Safe bereitstellen	Der Safeanbieter stellt einen Account, entsprechende IT-Infrastrukturen und Zugriffsmöglichkeiten zur Verfügung, die der Eigentümer (gegen Gebühren) nutzt.
Safe sperren	Der Safeanbieter kann den bestehenden Safe sperren, wenn der Eigentümer den Vertragsbedingungen nicht nachkommt. Damit kann sich der Eigentümer nicht mehr am Safe anmelden. Der Safe wird auch bei misslungenen Authentifizierungsversuchen gemäß der Sicherheitsrichtlinien automatisch gesperrt. Von der Sperrung ist zunächst nur der Zugang des Safeeigentümers betroffen. Posteingang und erteilte Freigaben stehen Dritten in einer Übergangszeit weiterhin zur Verfügung.
Safe entsperren	Ein gesperrter Safe kann vom Safeanbieter wieder entsperrt werden.
Safe aufgeben	Der Eigentümer kann den Safe aufgeben, anschließend ist ihm keine Nutzung des Safes mehr möglich. Grundsätzlich impliziert das Aufgeben eine sofortige Löschung der Safeinhalte durch den Safeanbieter. Eine vorherige Archivierung der Safeinhalte bzw. ein Transfer in ein Drittsystem obliegt dem Safeeigentümer.
Safe löschen	Der Safeanbieter muss den Safe löschen, wenn die Vertragsbeziehung zum Eigentümer nicht mehr besteht und alle Aufbewahrungsfristen abgelaufen sind.

Verwaltung von Daten

Eigentümer können über ihre Benutzeroberfläche Daten im Safe bearbeiten und auswerten.

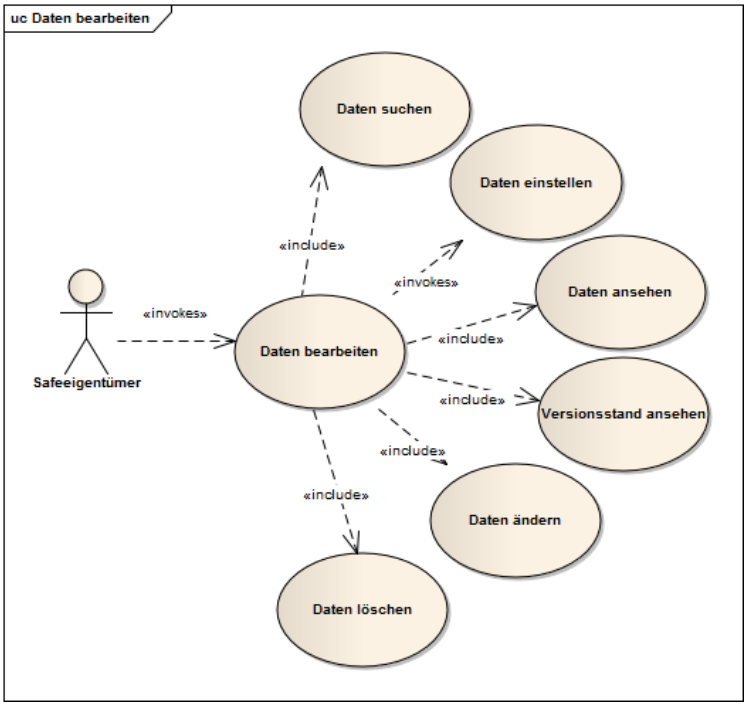

Abbildung 3: Verwaltung von Daten

Daten einstellen	Der Eigentümer kann Daten und Datengruppen einstellen.
Daten ansehen	Der Eigentümer kann Daten und Datengruppen einsehen.
Daten ändern	Eigentümer können Daten und Datengruppen ändern.
Daten suchen	Da es potentiell sehr viele verschiedene Anwendungsfälle gibt, die ggf. Daten in verschiedenen Versionen und Kontexten erfordern, muss der Eigentümer sehr leicht in der Lage sein, Daten zu finden. Es bieten sich Suchkriterien wie Datengruppen, geändert ab, freigegeben für oder Volltext an.
Versionsstand ansehen	Eigentümer können sich Daten und Datengruppen in verschiedenen Versionen ansehen und gegebenenfalls Vergleiche durchführen.
Daten löschen	Eigentümer können Daten und Datengruppen löschen.

Freigabe von Daten und Dokumenten

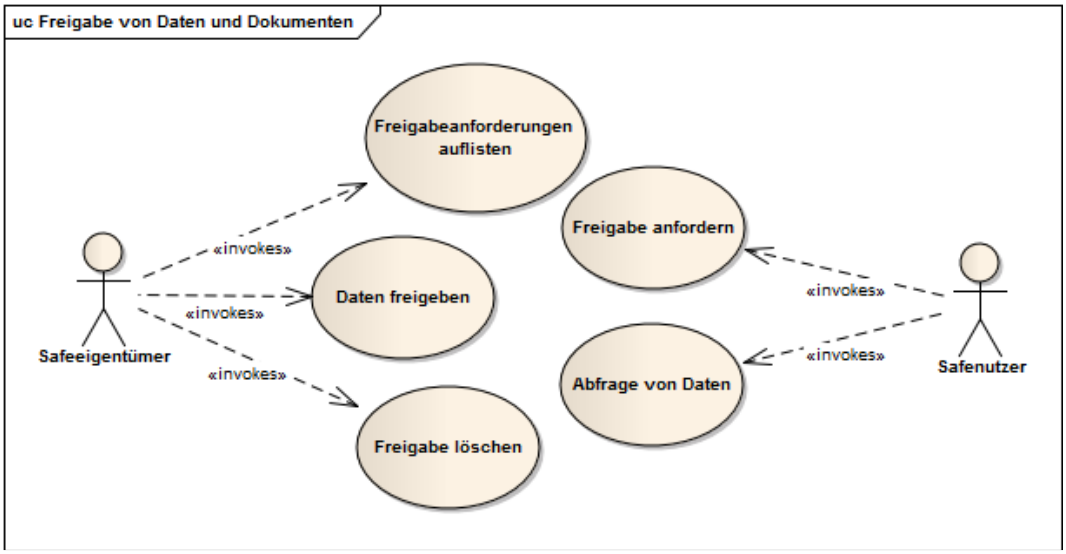

Abbildung 4: Freigabe von Daten und Dokumenten

Freigabe von Daten und Dokumenten	Eine Kopie vorhandener Daten bzw. Dokumente wird für den Zugriff durch Dritte im Freigabebereich des elektronischen Safes hinterlegt. Die Kopie ist mit dem privaten Schlüssel des Eigentümers signiert und mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.
Freigabe löschen	Der Eigentümer kann die Kopie im Freigabebereich löschen. Der Zugriff durch Dritte ist danach nicht mehr möglich.
Freigabe anfordern	Safenutzer können Freigabeaufforderungen in den Safe eines Safeeigentümers einstellen. Freigabeaufforderungen spezifizieren Art und Umfang der Daten, Verwendungszweck, zugreifende Partei und andere Metainformationen, welche es dem Safeeigentümer ermöglichen, die Rechtmäßigkeit dieser Anfrage zu überprüfen.
Abfrage freigegebener Daten	Ein Safenutzer kann die für ihn im Freigabebereich des elektronischen Safes hinterlegten Daten und Dokumente aus dem Safe abrufen.
Freigabeaufforderung auflisten	Der Safeeigentümer kann die von Dritten eingestellten Freigabeaufforderungen auflisten und deren Metainformationen einsehen.

Mailboxfunktion (Einstellen von Daten durch Dritte)

Externe Systeme greifen auf den Safe zu, um dem Safe eines Safeeigentümers Daten hinzuzufügen. Der Eigentümer kann später entscheiden, ob die von externen Systemen eingestellten Daten und Dokumente übernommen werden.

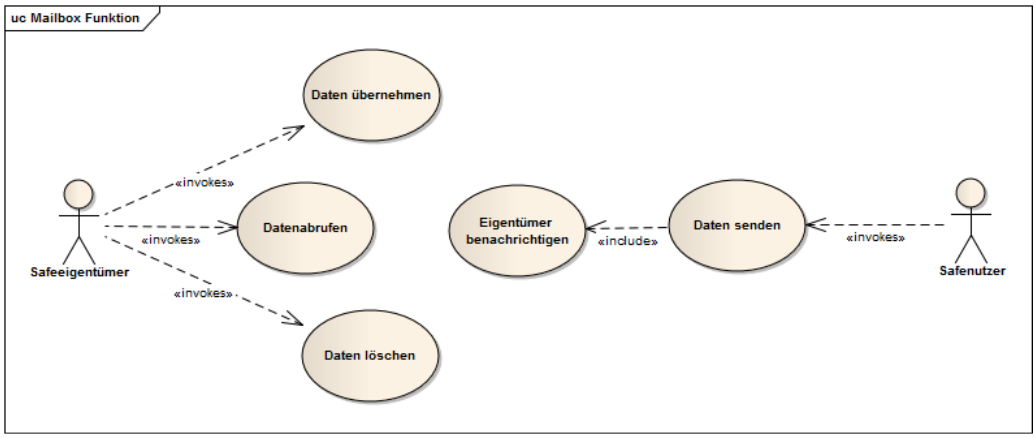

Abbildung 5: Mailboxfunktion

Daten senden	Ein neues Dokument (etwa eine Rechnung) wird in den Posteingangsbereich des elektronischen Safes eingestellt. Das Dokument ist mit dem öffentlichen Schlüssel des Eigentümers verschlüsselt und mit dem privaten Schlüssel des Absenders signiert.
Eigentümer informieren	Der Eigentümer wird über die neuen Daten und Dokumente informiert, wenn er Benachrichtigungen in den Einstellungen des Safes konfiguriert hat.
Daten abrufen	Der Safeeigentümer kann die durch Dritte in seinen Posteingang eingestellten Informationen lesen.
Daten übernehmen	Die Daten im Posteingang des elektronischen Safes können vom Safeeigentümer in den allgemeinen Bereich übernommen werden. Der Safeeigentümer wird damit Eigentümer dieser Daten. Sie stehen den Funktionen des elektronischen Safes, wie „Freigabe von Daten und Dokumenten“ oder „Daten senden“, zur Verfügung.
Daten löschen	Der Safeeigentümer kann nicht mehr benötigte Informationen in seinem Posteingang löschen.

Protokollierung

Der Eigentümer schaut sich die automatisch erzeugten Protokolle entsprechend seiner Einstellungen an.

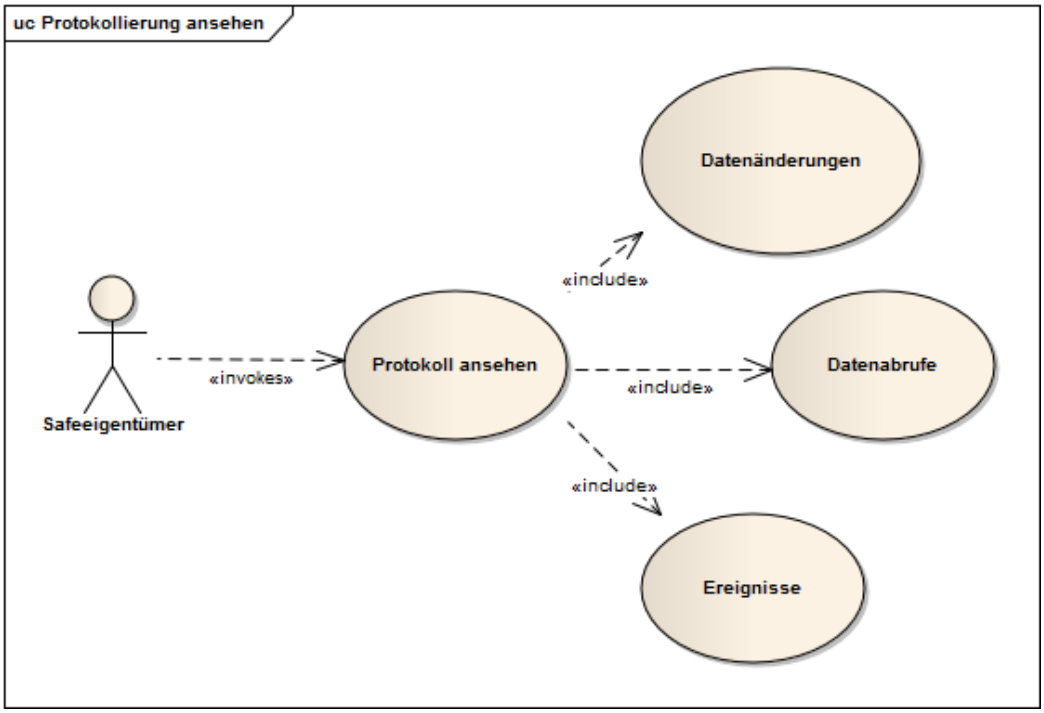

Abbildung 6: Protokollierung

Protokoll ansehen	Der Eigentümer schaut sich ein Protokoll an. Er kann das Protokoll nach relevanten Kriterien filtern und sortieren.
Datenänderungen	Der Eigentümer schaut sich die Änderungen an Daten oder an einer Datengruppe an.
Datenabrufe	Der Eigentümer schaut sich Datenabfragen Dritter an.
Ereignisse	Der Eigentümer schaut sich sonstige Ereignisse, wie etwa fehlgeschlagene Authentifizierungen, an.

Trusted Third Party

Die Ende-zu-Ende-Verschlüsselung der Daten und Dokumente im elektronischen Safe wird durch die Nutzung kryptographischer Methoden auf ein Sicherheitsmodul (häufig kryptographische Chipkarte) konzentriert. Bei Verlust oder Beschädigung dieses Sicherheitsmoduls ist der Safeeigentümer von der Nutzung seines elektronischen Safes und seiner Daten und Dokumente ausgesperrt. Zur Absicherung des Safeeigentümers muss ein alternativer Zugang über eine Trusted Third Party eingerichtet werden.

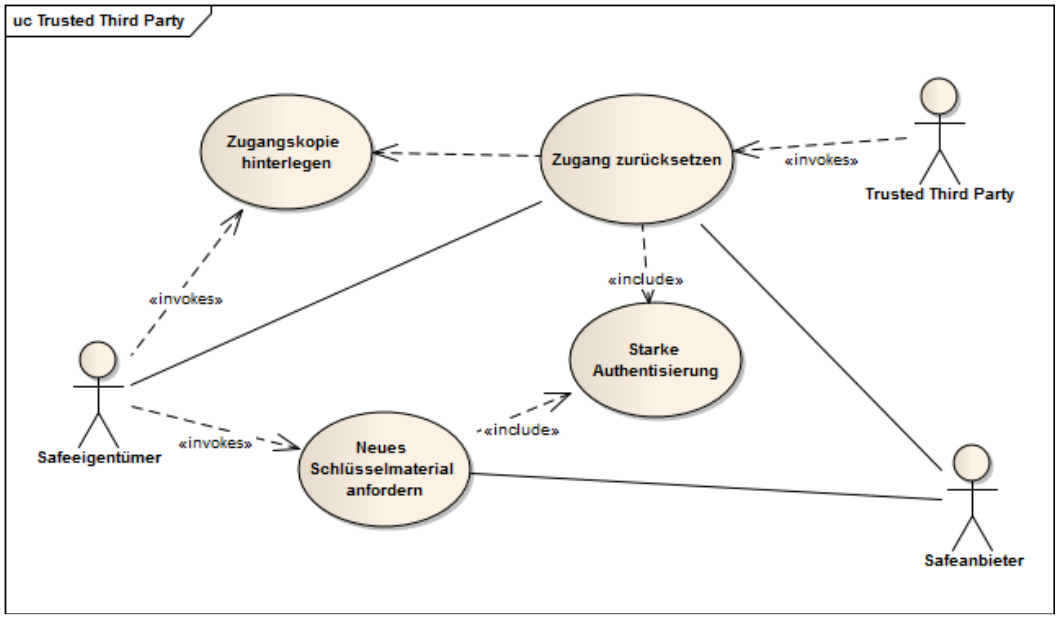

Abbildung 7: Trusted Third Party

Zugangskopie hinterlegen	Der Eigentümer hinterlegt eine Kopie seines Zugangs zum elektronischen Safe beim Safeanbieter. Diese Kopie ist mit dem öffentlichen Schlüssel der Trusted Third Party verschlüsselt.
Neues Schlüsselmaterial anfordern	Bei Verlust des Sicherheitsmoduls fordert der Eigentümer beim Safeanbieter Ersatz an. Das bisher genutzte Schlüsselmaterial (öffentlicher und privater Schlüssel) des Safeeigentümers wird ungültig. Mit dem neuen Sicherheitsmodul erhält der Safeeigentümer neues Schüsselmaterial.

Zugang zurücksetzen	Die Trusted Third Party setzt den Zugang mit Bevollmächtigung des Safeeigentümers unter Verwendung des neuen Schlüsselmaterials des Eigentümers zurück. Voraussetzung hierfür ist die zweifelsfreie Identitätsfeststellung durch starke Authentisierung von Trusted Third Party und Safeeigentümer durch den Safeanbieter. Anderenfalls blockiert der Safeanbieter das Zurücksetzen.
Starke Authentisierung	Die missbräuchliche Verwendung sensibler Funktionen verhindert eine starke Authentisierung von Safeeigentümer und Trusted Third Party gegenüber dem Safeanbieter.

3.3 Abgrenzung zu Systemen mit ähnlichen Funktionen

Um den eigentlichen Mehrwert elektronischer Safes weiter herauszuarbeiten, ist eine Abgrenzung gegenüber etablierten oder technisch möglichen Instrumentarien sinnvoll.

Abgrenzung zum elektronischen Postfach

Gegenüber der Kommunikation über elektronische Post (Push-Prinzip) favorisiert der elektronische Safe das Abholen (Pull-Prinzip) von Daten und Dokumenten durch Dritte. Das heißt, dass für Dritte bestimmte Daten und Dokumente von diesen aus dem Safe abgeholt werden. Dennoch bietet der elektronische Safe auch die Möglichkeit zum Empfang. Über diesen Mechanismus können beispielsweise Bescheide der öffentlichen Verwaltung, Rechnungen von Dienstleistern oder das Ergebnis einer Digitalisierung in den Safe gelangen.

Der elektronische Safe tritt damit allerdings nicht in Konkurrenz zur herkömmlichen E-Mail, da vorrangiges Ziel nicht die individuelle Kommunikation, sondern der Austausch von Daten und Dokumenten ist. Nach Möglichkeit hält der elektronische Safe Daten in strukturierter, wiederverwendbarer und geschützter Form vor. Ungeschützte oder unbekannte Daten- und Dokument-Typen können auf Wunsch des Safeeigentümers abgewiesen werden. Postfächer nehmen dagegen alle Daten in Empfang, solange sie in elektronischer Form bei ihnen ankommen.

Weiterhin ist das Prinzip der nachweisbaren sicheren Zustellung nicht das primäre Ziel des elektronischen Safes. Nach dem Prinzip der Teilung der Verantwortlichkeiten (separation of concerns) sind die für eine nachweisbare sichere Zustellung erforderlichen Werkzeuge einer anderen Komponente zuzuordnen. Eine Integration sollte dennoch möglich sein.

Vergleichbar einer client-seitigen E-Mail-Anwendung bietet der Safeclient dem Eigentümer eine gleichbleibende Handhabung verschiedener Accounts bei verschiedenen Safeanbietern. Der Benutzer kann also über eine einzige Benutzerschnittstelle verschiedene Accounts bedienen und wird somit nicht durch unterschiedliche Gestaltungen von der Verwaltung seiner Daten abgelenkt.

Abgrenzung zu Kollaborationsumgebungen

Ziel von Kollaborationsumgebungen ist das gemeinsame Erarbeiten von Ergebnissen. Hierfür stehen vielfältige Werkzeuge zur Verfügung, mit denen die gespeicherten Daten und Dokumente be- bzw. verarbeitet werden können.

Der elektronische Safe hingegen unterliegt der alleinigen Kontrolle des Eigentümers. Der Safe stellt keine gemeinsamen Sichten zur Verfügung. Er bietet einzig auf Anordnung des Eigentümers Einsicht in bestimmte Teildaten.

Kollaborationsumgebungen sind eher bunte und sich schnell entwickelnde Sammlungen von unterschiedlichen Werkzeugen, die nach zu verarbeitenden Dokumenten und der Art der Zusammenarbeit variieren.

Die gewünschte Sicherheit des Safes wird auch Einfluss auf die Gestaltung der Benutzeroberfläche für den Eigentümer haben. Durch eine bewusst reduzierte Funktionalität sowie einfache und kontinuierlich gleichbleibende Handhabbarkeit und Übersichtlichkeit in der Darstellung soll einer Fehlbedienung durch den Eigentümer vorgebeugt werden.

Abgrenzung zu Datei- bzw. Laufwerksverschlüsselungsansätzen

Vorhandene Lösungen zur Datei- bzw. Laufwerksverschlüsselung sollen die Privatsphäre des Nutzers garantieren. Die Daten und Dokumente des Nutzers liegen in verschlüsselter Form auf einem Speichermedium. Um den Klartext wiederherzustellen sind die entsprechende Verschlüsselungssoftware sowie die passenden Schlüssel notwendig.

Diese Systeme adressieren grundsätzlich nur die Privatsphäre des Nutzers. Das Thema Datensicherheit, beispielsweise der Schutz vor Verlust, kann von diesen Systemen nicht geleistet werden und muss ebenso wie die Online-Verfügbarkeit oder Bereitstellung von Daten für Dritte durch andere Komponenten sichergestellt werden.

Abgrenzung zu Online-Festplatten und Webspace-Anbietern

Es gibt verschiedene Lösungen zur serverbasierten Ablage von Dokumenten im Internet[12]. Die angebotene Funktionalität reicht von der einfachen technischen Ablagemöglichkeit via FTP oder WebDAV bis zu komplexen Funktionen wie Synchronisation auf mehrere Endgeräte, Freigabe von Informationen für Dritte oder Versionierung der Daten.

Im Unterschied zum elektronischen Safe ist die Privatsphäre des Nutzers nicht ausreichend gesichert, da die technischen Maßnahmen hierfür häufig nicht ausreichen. Viele Lösungen bieten bisher keine Verschlüsselung der eingestellten Informationen an. Bei einigen Lösungen kann aufgrund der Architektur die Zugriffsmöglichkeit des Anbieters grundsätzlich nicht ausgeschlossen werden (Web-basierte Systeme, Schlüsselmaterial unter Verwaltung des Anbieters). Darüber hinaus ist die langfristige Vertraulichkeit der eingestellten Informationen bisher bei keinem Anbieter ausreichend adressiert.

Eine Bereitstellung der vorgehaltenen Daten zur Nutzung in elektronischen Prozessen Dritter (bspw. der öffentlichen Verwaltung) ist nur in Ansätzen möglich und gestaltet sich aufgrund vieler verschiedener Schnittstellen eher schwierig.

3.4 Verortung der Safeanbieter

Dem Safeanbieter kommt die besondere Aufgabe zu, die verschiedenen Funktionen eines elektronischen Safes bereitzustellen. Er muss gegenüber dem Safeeigentümer vertrauenswürdig sein und die verwalteten Daten dauerhaft vor unberechtigtem Zugriff schützen.

Gefährdungen für diese Vertraulichkeit können grob in drei Kategorien eingeteilt werden:

- externe Gefährdungen (durch Einbruch in die Systeme des Safeanbieters)
- interne Gefährdungen (durch Mitarbeiter des Safeanbieters organisiert)
- staatlich organisierte Einsichtnahme.

Ein wichtiges Kriterium für die Vertrauenswürdigkeit des elektronischen Safes ist daher die physikalische und organisatorische Verortung des Safeanbieters.

Erste Überlegungen führten dazu, elektronische Safes bei neutralen Instanzen mit besonderen rechtlichen Befugnissen und Pflichten zur Aufbewahrung vertraulicher Informationen anzusiedeln. Vergleichbar mit dem Notar, ständen

[12] Bspw. GMX MediaCenter (http://www.gmx.de), Microsoft SkyDrive (http://skydrive.live.com), Dropbox (http://www.dropbox.com), Wuala (http://www.wuala.com).

diese „Datennotare“ unter einem besonderen gesetzlichen Schutz, der insbesondere auch den staatlichen Zugriff auf die von diesem Safeanbieter für einen Safeeigentümer bereitgehaltenen Daten verhindert bzw. erschwert hätte.

Üblicherweise werden Dienstleistungen mit den hohen technischen Anforderungen, welche an einen elektronischen Safe gestellt werden, allerdings von spezialisierten IT-Dienstleistern mit entsprechenden Rechenzentren und Personal erbracht. Diese genießen bisher jedoch keinen besonderen Schutz und können daher die Rolle als neutrale Instanz nicht übernehmen. Auch eine Kooperation zwischen IT-Dienstleister und Notaren bietet kein besonderes Schutzniveau, da kein rechtlicher Rahmen existiert, der es ermöglicht, den Schutz, den ein Notar genießt, auf einen Kooperationspartner auszudehnen[13]. Die Einführung eines solchen Rechtsrahmens ist eher unwahrscheinlich und erscheint zudem nicht sachgerecht. Die technische Ausgestaltung elektronischer Safes legt vielmehr eine Verortung im privatrechtlichen Raum bei gleichzeitiger Sicherstellung der Vertraulichkeit und Akzeptanz durch staatliche Reglementierung und Überwachung nahe. Denkbar erscheint aber eine Einbindung der Notare bei einzelnen Diensten (beispielsweise als Trusted Third Party oder im Kontext der vertraulichen und beweissicheren Digitalisierung analoger Dokumente).

Jeder Safeanbieter trifft technische sowie organisatorische Vorkehrungen, welche die Einhaltung gesetzlicher Aufbewahrungsfristen und technischer Dienstgütevereinbarungen (Service Level Agreements) ermöglichen; ggf. werden die Safeanbieter zu bestimmten Maßnahmen durch einen speziellen Rechtsrahmen oder ein Akkreditierungsverfahren verpflichtet. Der Safeeigentümer hat bei der Einrichtung eines Safes verschiedene Anbieter zur Auswahl und kann sich für den aus seiner Perspektive vertrauenswürdigen Dienstleister entscheiden. Auch ein Umzug der Safeinhalte zu einem anderen Safeanbieter sollte möglich sein, wobei wiederum die rechtlichen Rahmenbedingen den alten Safeanbieter dazu anhalten sollten, die gespeicherten Inhalte des Safeeigentümers zeitnah und vollständig (das betrifft auch evtl. angelegte Backups) zu löschen.

Bei der Verortung können bestehende Ansätze berücksichtigt werden, um die Markteintrittsbarrieren für Safeanbieter gering zu halten. Eine elektronische Ablagemöglichkeit für Daten und Dokumente ist beispielsweise im Bürgerportalprojekt der Bundesregierung (De-Mail-Gesetz) als optionales Angebot vorgesehen[14]. Auch die Anbieter von Online-Festplatten und Webspace können potentielle Safeanbieter sein. Die aktuelle Ausgestaltung vorhandener Ansät-

[13] Vgl. hierzu den Ansatz des DigiNotar in den Niederlanden (http://www.diginotar.com/aboutdiginotar.aspx).

[14] Heyde; Wappenschmidt (2008). Grobkonzept Dokumentensafe Light. Version 0.96. Abgerufen von: http://www.cio.bund.de/cae/servlet/contentblob/78156/publicationFile/23654/grobkonzept_dokumentensafe_light_download.pdf.

ze und Dienste ist jedoch insbesondere hinsichtlich der Vertraulichkeit der eingestellten Daten und Dokumente nicht ausreichend für einen elektronischen Safe.

3.5 Technische Anforderungen an elektronische Safes

Wesentliche Voraussetzung für die Akzeptanz eines elektronischen Safes ist das Vertrauen in die technischen, organisatorischen und rechtlichen Gegebenheiten des Safeanbieters. Hierfür sind besonders die Sicherheitsziele und -anforderungen von ausschlaggebender Bedeutung. Ein Safeanbieter muss daher insbesondere die folgenden Aspekte mit seinem Angebot gewährleisten:

- **Datensicherheit**: Zum ersten werden bei Benutzung eines Safes die Verfügbarkeit und Unveränderlichkeit der eingestellten Daten und Dokumente unterstellt. Darauf müssen sich der Eigentümer aber auch die Safenutzer verlassen können. Eingestellte Rechnungen müssen noch nach Jahren, nach verschiedenen Safeclient-Software-Updates, Safeanbieter-Wechseln etc. unverändert zu entnehmen sein. Signaturen müssen regelmäßig erneuert werden, um dem Verfall an Sicherheit mit alten Schlüssellängen zu begegnen. Technische Mittel dafür sind die Verwendung professioneller Datenbanken und entsprechender Archivierungsinfrastruktur.

- **Vertraulichkeit**: Im Gegensatz zu den im WS-Security Kontext eingeführten Attribute-Providern setzen die Datenabfragen im Safe immer die Freigabe der abgefragten Daten durch den Eigentümer voraus. Bei der Freigabe der Daten werden sie am Client so verschlüsselt, dass sie ausschließlich für den Empfänger lesbar sind. Damit bleibt die Vertraulichkeit der Kommunikation **aus dem Safe heraus** immer gewahrt. **Eingehende Daten** sind immer mit dem öffentlichen Schlüssel des Eigentümers verschlüsselt, so dass sie erst am Client, d.h. für den Safeanbieter verdeckt entschlüsselt werden. In der Datenhaltungsschicht werden sie wieder abgelegt, nachdem sie mit dem öffentlichen Schlüssel des Eigentümers verschlüsselt sind. Deshalb ist auch die Vertraulichkeit eingehender Informationen immer gewahrt. Unverschlüsselt eingehende Daten werden vom Safe nicht akzeptiert. Somit sind die Daten des Eigentümers gegenüber Dritten und dem Safeanbieter immer geschützt.

- **Privacy**: Unter dem Begriff Privacy werden vielfältige Sicherheitsziele zusammengefasst, u.a. **Unverkettbarkeit** und **Unbeobachtbarkeit**. Da der Safeanbieter nicht wissen kann, wessen Daten im Safe aufbewahrt sind, können die Interaktionen mit dem Safe nicht auf Identitäten zurückgeführt werden. Der Beobachtung seiner Aktivitäten in Prozes-

sen kann sich der Eigentümer mit Hilfe des Safes entziehen, indem er den Prozess-Beteiligten Pseudonyme statt seiner richtigen Identitätsdaten freigibt.

Organisatorische sowie technische Vorkehrungen ermöglichen Safeanbietern diese Sicherheitsziele mit Blick auf den unautorisierten Zugriff von außen zu erreichen. Der Zugriff durch den Betreiber auf die Inhalte eines Safes kann mit konventionellen Mitteln allerdings nicht wirkungsvoll ausgeschlossen werden. Abhilfe schafft hier ein Rechtsrahmen für Safeanbieter, der einerseits die Einhaltung der beschriebenen Ziele absichert, andererseits aber vor allem Vorgaben für vertrauenswürdige Safeanbieter normiert.

Die verschiedenen Datenschutzverletzungen der Vergangenheit machen deutlich, dass es den vollständig vertrauenswürdigen Safeanbieter nicht geben kann. Auch wenn an die organisatorischen und technischen Maßnahmen zur Umsetzung dieser Ziele höchste Maßstäbe angelegt werden, kommt es durch den Faktor Mensch immer wieder zur Offenlegung sensibler Daten.

Aber auch technische Maßnahmen, wie die asymmetrische Verschlüsselung, sind kein Garant für eine dauerhafte Vertraulichkeit sensibler Daten. Bei pessimistischer Sichtweise sind mit heutigen Schlüssellängen chiffrierte Informationen in sechs bis zehn Jahren durch Weiterentwicklung in den Bereichen Hardware und Kryptoanalyse nicht mehr ausreichend geschützt (vgl. Abbildung 8). Anders als beim dauerhaften Nachweis der Authentizität der Daten durch Über-Signatur[15], reicht eine Um-Verschlüsselung der Daten nicht aus, um die Daten dauerhaft vor einer Offenlegung zu schützen. Werden mit derzeit aktuellen Mechanismen verschlüsselte Kopien sensibler Informationen von einem Angreifer aufbewahrt, kann er diese dechiffrieren, wenn die Mechanismen durch den technologischen Fortschritt ausreichend schwach geworden sind. Dafür benötigt er nicht die durch verbesserte Verschlüsselungsmechanismen geschützten Original-Daten.

[15] Vgl. § 17 SigV.

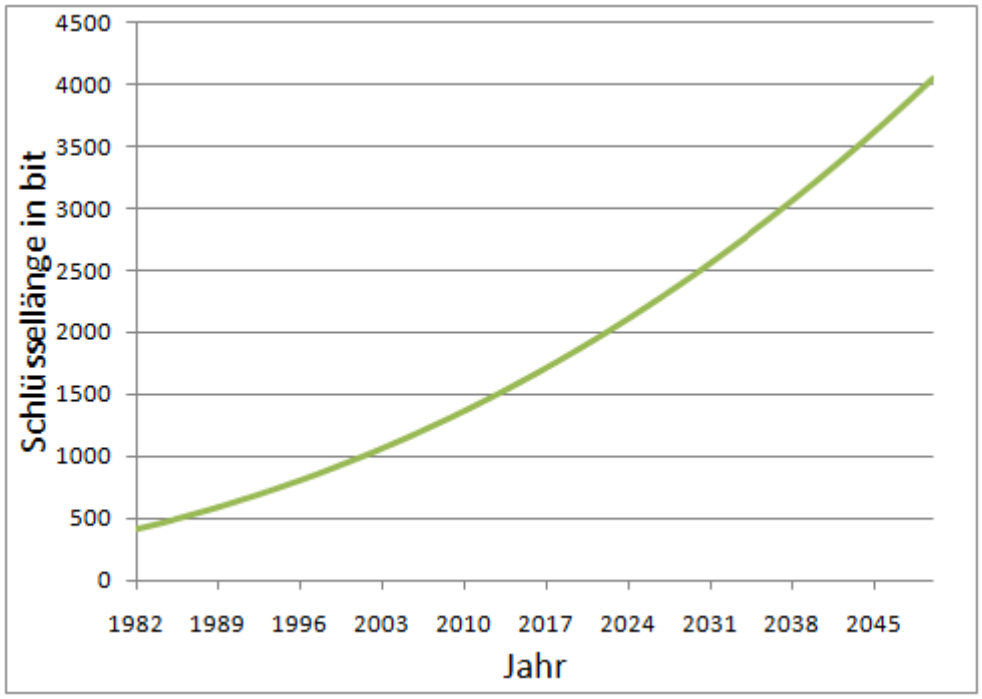

Abbildung 8: Empfohlene Schlüssellängen für asymmetrische Verschlüsselung[16]

Dem Privacy-By-Design-Prinzip folgend, müssen weitere Maßnahmen ergriffen werden, um die Einsichtnahme in die Daten des Eigentümers durch den Safeanbieter zu verhindern. In Zusammenarbeit mit der IBM Deutschland GmbH wurde beim Fraunhofer-Institut FOKUS ein Konzept entwickelt, um Daten bei wenig-vertrauenswürdigen Safeanbietern abzulegen. Kern des Konzepts ist die Verteilung der Daten auf verschiedene Safeanbieter. Jeder Safeanbieter erhält dabei nur einen Teil der Informationen in verschlüsselter Form. Kein Safeanbieter kann verschiedene Teilinformationen einander, noch einem bestimmten Safeeigentümer zuordnen. Das Wiederherstellen der Daten ist daher nur dem Safeeigentümer möglich, da nur er im Besitz der Information ist, wo sich die einzelnen Teile seiner Daten und Dokumente befinden. Sollte ein Safeanbieter dennoch in den Besitz dieser Verteil-Information gelangen, ist es ihm grundsätzlich nicht möglich die Daten wiederherzustellen, da er nicht über sämtliche Teile verfügt. Sofern einer der beteiligten Safeanbieter vertrauenswürdig und seinen Kunden gegenüber loyal ist und sich zudem an gesetzliche Vorschriften hält, kann kein anderer Safeanbieter in den Besitz aller Teile gelangen. Dadurch bleiben die Daten und Dokumente des Safeeigentümers geschützt.

Die weitreichende Vernetzung der verschiedenen Kommunikationspartner kann nur auf Basis einheitlicher Schnittstellen realisiert werden. Standardisierte Schnittstellen zu den Basisfunktionalitäten des elektronischen Safes müs-

[16] Lenstra; Verheul (2001). Selecting cryptogrphic key sizes. in: Journal of cryptology. (S. 255-293).

sen daher von jedem Safeanbieter bereitgestellt werden. Die Schnittstellendefinition sollte dabei von einer neutralen Instanz aufgebaut und fortlaufend gepflegt werden.

Ein aus Nutzersicht durchgängiges Identitätsmanagement erfordert die Anbindung von Public-Key-Infrastrukturen (PKI) seitens des Safeanbieters. Um einen möglichst einfachen und transparenten Service zu bieten, sollten Safeanbieter mit etablierten PKI-Anbietern zusammenarbeiten.

Weitere technische Anforderungen ergeben sich aus dem Betrieb einer entsprechenden Infrastruktur zur Bereitstellung elektronischer Safes. Der Safeanbieter sollte grundsätzliche Anforderungen zum Betrieb eines Rechenzentrums umsetzen. Grundsätzliche Maßnahmen zur Absicherung finden sich in den Grundschutzkatalogen des BSI[17]. Dabei spielen naturgemäß die Sicherheitsanforderungen eine besondere Rolle. Es wird vom Safeanbieter allerdings nicht erwartet, dass er dieselben Sicherheitsstandards wie ein Trustcenter erfüllt. Die damit verbundenen Kosten würden verhindern, dass sich mehrere Anbieter elektronischer Safes auf dem Markt etablieren. Dem Safeanbieter steht es allerdings frei, ähnliche Sicherheitsstandards wie Trustcenter umzusetzen, um sich so von Wettbewerbern abzuheben oder Benutzergruppen mit speziellen rechtlichen Anforderungen (beispielsweise Behörden) anzusprechen.

Eine Grundvoraussetzung für das Vertrauen von Endnutzern gegenüber Dienstanbietern ist eine hohe Verfügbarkeit des angebotenen Services. Der Safeanbieter sollte daher durch geeignete technische Maßnahmen eine hohe Verfügbarkeit sicherstellen.

[17] BSI (November 2009): IT-Grundschutz-Kataloge – 11. Ergänzungslieferung. Abgerufen von: https://www.bsi.bund.de/cae/servlet/contentblob/478418/publicationFile/54741/it-grundschutz-kataloge_2009_EL11_de.pdf.

4. Dienste auf Basis elektronischer Safes

Der elektronische Safe bildet als vertrauenswürdige Infrastrukturkomponente die Basis für verschiedene Dienste und Anwendungen. Mit diesen Angeboten können Safeeigentümer und -nutzer weitere Funktionen in Anspruch nehmen, ohne dass die sichere und vertrauenswürdige Grundkonstruktion des Safes verändert wird. Die Infrastrukturkomponente elektronischer Safe ist mit Diensten modular erweiterbar und kann an individuelle Anforderungen angepasst werden. Im Folgenden wird dieses Konzept übersichtsartig dargestellt, um anschließend einzelne Dienste ausführlicher zu beschreiben.

4.1 Verständnis von Diensten

Grundsätzlich liegen die Informationen in einem Safe verschlüsselt vor. Sie stehen nur auf dem System des Safeeigentümers sowie in Form von heruntergeladenen Freigaben auf Systemen eines Safenutzers im Klartext zur Verfügung. Die Verarbeitung der Informationen in einem elektronischen Safe ist demnach auf diese beiden Stellen begrenzt.

Dienste externer Anbieter setzen die Freigabe der benötigten Daten durch den Safeeigentümer voraus. Diese Freigabe kann sowohl proaktiv als auch reaktiv – nach vorheriger Freigabe-Anfrage des Dienstanbieters – durch den Safeeigentümer erfolgen. Der Dienstanbieter hat dabei uneingeschränkt lesenden Zugriff auf diese Freigabe.

Externe Dienste können zum einen Workflowsysteme sein, welche Daten aus dem Safe entgegennehmen und nach mehreren Bearbeitungsschritten das Ergebnis (Bescheid) in Form von Daten und Dokumenten wieder in den Safe einstellen. Fallbearbeitungssysteme der öffentlichen Verwaltung können so (semi-) automatisiert und medienbruchfrei Anträge des Safeeigentümers bearbeiten und entsprechende Bescheide wieder in seinen Safe einstellen (siehe Abbildung 9).

Weitere externe Dienste können rein konsumierend sein, also nur die Daten des elektronischen Safes nutzen, ohne Informationen in den Safe einstellen zu müssen. Ein Beispiel hierfür sind die verschiedensten Informations- und Meldepflichten[18], die von Unternehmen erbracht werden müssen. Auch diese Dienste können mit dem elektronischen Safe auf vertrauenswürdige Art bedient werden.

[18] Vgl. hierzu zum Beispiel den Bericht der Bundesregierung, in dem die Zahl von ca. 10.000 verschiedene Informations- und Meldepflichten genannt wird. Die Bundesregierung (2009): Wachstum fördern: Bürokratieabbau und bessere Rechtsetzung. Abgerufen von: http://www.bundesregierung.de/Content/DE/__Anlagen/2009/12/2009-12-16-jahresbericht-buerokratieabbau,property=publicationFile.pdf S. 6.

Für den Zugriff auf Freigaben verwenden Dienstanbieter die gleichen Mechanismen wie Safeeigentümer. Auch der Zugriff von Dritten unterliegt den gleichen Vertraulichkeits- und Privacy-Anforderungen. Für den Safeanbieter sind somit keine Rückschlüsse auf Art und Umfang der von einem Safeeigentümer in Anspruch genommenen Dienstleistungen möglich.

Grundsätzlich kann sich der Dienstanbieter auf die Maßnahmen zur Datensicherheit seitens des Safeanbieters verlassen. Das bedeutet, er muss die freigegebenen Informationen nicht in eigenen IT-Systemen duplizieren. Er kann bei Bedarf jederzeit auf die Safeinfrastruktur zugreifen. Durch geeignete technische Maßnahmen kann dieses Verhalten forciert, eine Duplizierung der Daten auf Seiten des Dienstanbieters also durch den Safeeigentümer verhindert werden. Für den Safeeigentümer bedeutet dieser Ansatz mehr Kontrolle über die eigenen Daten. Diensteanbieter können den Aufwand für die eigene IT-Infrastruktur mitunter deutlich verringern.

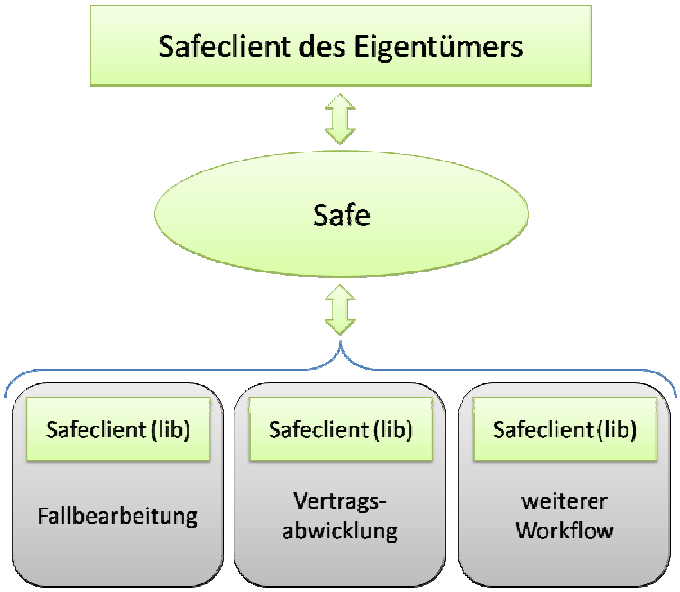

Abbildung 9: Externe Dienste

Viele Dienste ziehen Schlüsse aus den gelieferten Daten des Konsumenten. Häufig werden nur diese abgeleiteten Informationen (bspw. hat Einkommen kleiner X) benötigt. Eine Freigabe und die damit verbundene Aufdeckung vertraulicher Informationen sind hier nicht unbedingt nötig. Neben der Nutzung externer Dienstleistungen bietet sich daher an, die in einem elektronischen Safe gesammelten Daten auch lokal zu verwenden, entsprechende Schlüsse zu ziehen und nur diese weiter zu verwenden.

Es sind somit Dienstleistungen denkbar, die allein auf den Daten des Safes operieren und keine Interaktion mit Fremdsystemen durchführen. Beispiele hierfür wären Formatkonvertierungen, Notifikationsdienste, welche die Einhaltung von Fristen überprüfen bzw. mitteilen oder statistische Auswertungen auf den Daten des elektronischen Safes durchführen.

Eine weitere Kategorie bilden daher die **lokalen Dienste** am vertrauenswürdigen System des Safeeigentümers. Hierfür kann der Safeclient des Safeeigentümers um Plugins für verschiedene Aufgaben erweitert werden. Die Plugins können die unverschlüsselten Daten lokal, auf dem vertrauenswürdigen System des Safenutzers lesen, analysieren, weiter verarbeiten oder weitere Informationen ableiten. Abgeleitete Informationen dürfen von den Plugins in den elektronischen Safe eingestellt werden. Es stehen darüber hinaus verschiedene Schnittstellen zu den weiteren Funktionen des Safes, wie Freigabe oder Protokollierung zur Verfügung. Auf dieser Basis können die verschiedensten Applikationen umgesetzt werden. In Funktion und Anwendungszweck sind den verschiedenen Plugins wenig Grenzen gesetzt.

Grundsätzlich dürfen jedoch keine Informationen das lokale System bzw. den elektronischen Safe ohne die explizite Einwilligung des Safeeigentümers verlassen. Die Einhaltung dieser Richtlinie durch Plugins kann zwar automatisiert, jedoch nicht hinreichend genug geprüft werden. Die Verwendung von Plugins stellt daher immer auch ein gewisses Risiko dar, da diese Zugriff auf den unverschlüsselten Datenbestand des Safes haben. Hier muss die Mehrheit der Safeeigentümer entsprechenden Experten vertrauen, welche die Sicherheit der Plugins überprüfen bzw. zertifizieren.

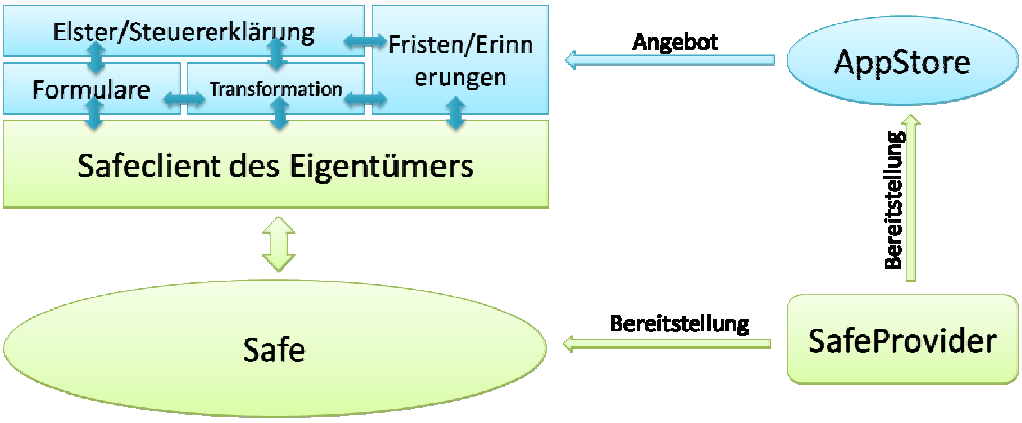

Abbildung 10: Plugin-Architektur des Safeclients für lokale Dienste

Eine Möglichkeit wäre die Nutzung einer geschlossenen Plattform für Plugins des Safeclients als Verteilmechanismus (AppStore) (siehe Abbildung 10). Dieser vom Safeanbieter angebotene Service bietet geprüfte Plugins zur Verwendung durch den Safeeigentümer an. Neben der aus solchen Systemen bekannten Voting-Funktion, bei der Nützlichkeit oder Ergonomie im Vordergrund stehen, können über eine weitere Voting-Funktion die Privacy-Eigenschaften des Plugins bewertet werden. Die durch den Safeanbieter geprüfte Vertrauenswürdigkeit des Plugins kann so durch versierte Nutzer bestätigt werden. Gerade dieser Bereich könnte sich außerhalb der staatlichen Reglementierung der eigentlichen Safeinfrastruktur und ihrer Anbieter bewe-

gen und so ausreichend Raum für privatwirtschaftliche Geschäftsmodelle und eine Abgrenzung von Konkurrenten bieten.

Eine weitere Kategorie bilden die **Integrationsdienste**. Deren vorrangige Funktion ist das Vergrößern der Datenbasis, der in elektronischen Safes gespeicherten Informationen durch Anbindung verschiedener Datenquellen (siehe Abbildung 11). Dazu stellen sie beispielsweise Adapter bereit, deren Schnittstellen von Legacy-Systemen angesprochen werden können. Denkbar wären Schnittstellen für FAX, nicht-standardisierte HTTP-Schnittstellen oder Schnittstellen für OSCI. Ein weiterer Dienst dieser Kategorie wäre die Digitalisierung vorhandener physischer Dokumente.

Die vertrauliche Verwahrung sensibler Daten und Dokumente ist Kernkompetenz des elektronischen Safes. Die Nutzung von Safeinhalten außerhalb der gesicherten Safeinfrastruktur ist zu vermeiden. Aus Sicherheitsgründen ist die Interaktion der Integrationsdienste mit der Safeinfrastruktur daher auf das Einstellen von Informationen begrenzt. Die Integration von Diensten mit lesendem Zugriff auf den elektronischen Safe sollte ausschließlich über definierte Safemechanismen erfolgen, um die Sicherheitseigenschaften nicht zu beeinträchtigen.

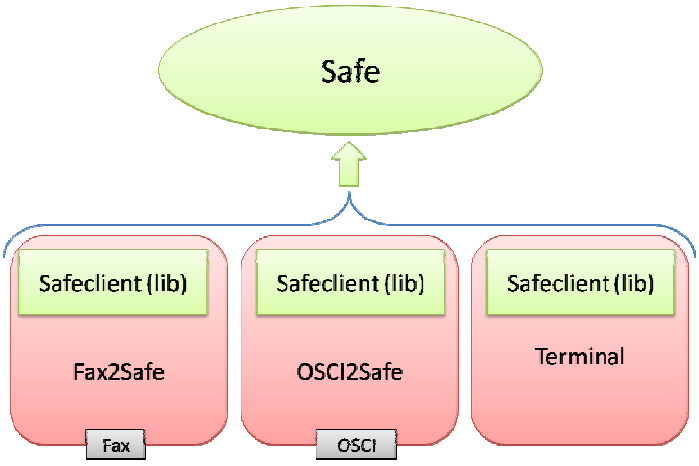

Abbildung 11: Integrationsdienste

4.2. Spezifische Dienste auf Basis elektronischer Safes

4.2.1 Externe Dienste

Der elektronische Safe bietet mit der Freigabefunktion die Möglichkeit, sensible Daten Dritten auf vertrauenswürdige Art zur Verfügung zu stellen. Externe Dienste nutzen die für diesen Zweck vom Safeeigentümer freigegebenen Daten.

Fallbearbeitung in der öffentlichen Verwaltung

Bürger haben durchschnittlich 1,5 Verwaltungskontakte pro Jahr[19]. Unternehmen stellen etwa 130 Anträge im Jahr an die öffentliche Verwaltung[20]. Sämtliche Daten und Dokumente hierfür befinden sich potentiell im elektronischen Safe und können über die Freigabefunktion Antrags- bzw. Fallbearbeitungssystemen zur Verfügung gestellt werden. Der medienbruchfreie Zugriff auf die Informationen des Antragsstellers schafft weitreichende Möglichkeiten zur Prozessoptimierung für die öffentliche Verwaltung.

Insbesondere die Möglichkeit der elektronischen Auswertung der bereitgestellten Informationen bietet großes Potential, die Antragsbearbeitung zu beschleunigen. Vor der Bearbeitung durch Mitarbeiter der öffentlichen Verwaltung können die bereitgestellten Informationen des Antragsstellers auf Vollständigkeit überprüft oder die Authentizität elektronisch signierter Dokumente überprüft werden. Weiterhin können durch Analyse der bereitgestellten Informationen durch das Fallbearbeitungssystem automatisiert verschiedene Teilprozesse angestoßen werden.

Liegen die Informationen des Antragsstellers in maschinenlesbaren Formaten vor, kann die Antragsbearbeitung weiter automatisiert werden. Zukünftig ist durch Einsatz juristischer, regelbasierter Informatiksysteme auch eine weitestgehend automatisierte, elektronische Erstellung eines Bescheides denkbar.

Das Ergebnis eines Antragsprozesses stellt das Fallbearbeitungssystem automatisiert in Form eines elektronischen Bescheides in den Posteingangsbereich des elektronischen Safes des Antragsstellers ein. Dieser Bescheid ist von der ausstellenden Behörde elektronisch signiert und steht anschließend für weitere Anträge des Safeeigentümers zur Verfügung.

---

19 Lenz (2001) E-Government und E-Non Profit (S. 56). Stuttgart. Schäffer-Poeschel Verlag.

20 DIHK (2007) Bürokratieabbau und E-Government – Einsparpotenziale nutzen, Handlungsspielräume vergrößern. Abgerufen von: http://www.dihk.de/positionen/buerokratie.pdf.

Vertragsabwicklung mit Dienstleistern

Ein weiteres Beispiel externer Dienste rund um den elektronischen Safe stellt ganz allgemein die Vertragsabwicklung mit Dienstleistern dar. Safeeigentümer stellen dem Dienstleister die für die Vertragsanbahnung benötigten Informationen über den Safe gesichert zur Verfügung. Der Dienstleister nutzt diese Informationen zum Aufsetzen eines Vertrages.

Mit Hilfe eines Safeclients für mobile Endgeräte können Safeeigentümer auch ad-hoc Daten für die Vertragsabwicklung bereitstellen. Werden beispielsweise für den Kauf eines Gutes Nachweise über die Kreditwürdigkeit in Form von Gehaltsnachweisen benötigt, können mit Hilfe des elektronischen Safes und eines mobilen Clients die entsprechenden digitalen Unterlagen direkt freigegeben und durch den Händler als Safenutzer geprüft werden.

Nach erfolgreichem Abschluss des Vertrages, z.B. durch die Unterzeichnung mit Hilfe einer qualifizierten elektronischen Signatur, stellt der Dienstleister das Vertragsdokument in den elektronischen Safe des Safeeigentümers ein. Ist die Verwendung einer QES nicht möglich, so kann zumindest eine elektronische Version des Vertrages zur Überprüfung des Inhalts und der Konditionen bereitgestellt werden.

4.2.2 Lokale Dienste am vertrauenswürdigen System des Safeeigentümers

Um zu verhindern, dass persönliche Daten ungewollt von Dritten eingesehen werden können, werden Prozesse zukünftig verstärkt auf dem vertrauenswürdigen System des jeweiligen Inhabers der Daten ausgeführt. Entsprechend liegen im Ansatz des elektronischen Safes die Inhalte lediglich im Safeclient im Klartext vor. Mittels einer Plugin-Architektur kann der Safeeigentümer seinen Client flexibel um weitere Fähigkeiten erweitern. So sind Erweiterungen zur Bearbeitung von Formularen, der semantischen Zuordnung von Safeinhalten zu Anträgen oder der Datenkonvertierung denkbar.

Ein **Formularplugin** mit eingebautem **Zuständigkeitsfinder** erweitert die Funktionalität des Safeclients um die Möglichkeit, Anträge an die öffentliche Verwaltung direkt aus dem elektronischen Safe heraus anzustoßen. Für die Auswahl des korrekten Verwaltungsprozesses nutzt der Zuständigkeitsfinder die im Safe hinterlegten Informationen wie etwa Wohnort oder Nachname. Das Formularplugin bezieht daraufhin eine Beschreibung dieses Prozesses von der zuständigen Stelle der öffentlichen Verwaltung. Diese Metainformationen umfassen unter anderem

- die benötigten Daten und Dokumente (optional, erforderlich),
- deren Qualität (unsigniert, signiert),

- deren Datenformat (.pdf, .xml) und Datenrepräsentation (xml-Schema)
- deren Verwendungszweck (nur zur Ansicht, Duplizierung zur Dokumentation)
- Zuordnung der einzelnen Daten und Dokumente auf bearbeitende Stellen
- öffentliches Schlüsselmaterial der bearbeitenden Stellen
- Schnittstelle zum Antragssystem.

Auf Basis dieser Metainformationen prüft das **Formularplugin** die Existenz der geforderten Informationen im elektronischen Safe. Fehlende Informationen können nachgepflegt werden. Sind alle erforderlichen Unterlagen im Safe vorhanden, kann mit Hilfe des Formularplugins der Antrag gestellt werden. Dabei werden die geforderten Daten und Dokumente entsprechend der Metainformationen als Freigaben für die bearbeitenden Stellen im Safe hinterlegt und über die Schnittstelle zum Antragssystem der öffentlichen Verwaltung der Antrag eingereicht.

Bei der Bereitstellung der Daten kann das Formularplugin auf weitere Plugins zurückgreifen, um den Prozess der Antragsstellung für den Antragssteller so einfach wie möglich zu gestalten. Die semantische Zuordnung angefragter Daten auf im Safe vorhandene Informationen kann durch ein **Mappingplugin** übernommen werden. Die Anfrage nach der Adresse des Antragsstellers kann so zum Beispiel auf die elektronisch signierte Meldebescheinigung abgebildet werden. Dienstleister pflegen dabei Kataloge der vielen verschiedenen Mapping-Möglichkeiten und garantieren die Konsistenz.

Die Abbildung von Informationen auf verschiedene Datenrepräsentationen übernehmen **Transformationsplugins**. Die in einzelnen Datengruppen vorliegenden Informationen können damit in eine zusammengesetzte XÖV-kompatible Datenstruktur transformiert und als Freigabe zur Verfügung gestellt werden. Das Antragssystem der öffentlichen Verwaltung erhält somit die geforderten Informationen in der geforderten bzw. erwarteten Repräsentation.

Weiterhin kann ein **Konvertierungsplugin** die im elektronischen Safe hinterlegten Daten (sofern nötig) in die geforderten Datenformate (z.B. PDF/A) konvertieren. Die Kopie wird in Form einer Freigabe der öffentlichen Verwaltung zur Verfügung gestellt und kann optional als weiteres Dokument in den Safe übernommen werden.

Plugins sind allerdings nicht nur als kleine, nützliche Werkzeuge zu verstehen. Auch komplexe Produkte sind denkbar. Ein **ELSTER-Plugin** könnte etwa

GoBS[21]-konform den Safeeigentümer bei seiner jährlichen Einkommensteuererklärung unterstützen. Bei einer durchgängig elektronischen Kommunikation liegen alle relevanten Informationen für die jährliche Einkommenssteuererklärung im elektronischen Safe. Fehlende Informationen und Nachweise können ergänzt werden. Die Einkommensteuererklärung kann also direkt aus dem Safe heraus angestoßen werden.

Großes Potential bietet die Integration einer **Inferenzmaschine als Plugin** in den Safeclient, welche es erlaubt, durch Schlussfolgerungen auf Basis vorhandener Informationen im elektronischen Safe und bereitgestellten (gesetzlichen) Regeln neue Erkenntnisse zu ziehen. Der Safeeigentümer kann damit beispielsweise durch vergleichende Analyse seiner Lebenssituation auf Basis der Daten in seinem Safe (z.B. Einkommen, Kinder, Erkrankungen, etc.) in der Wahrnehmung seiner Rechte (spez. Förderung wie Wohngeld, Kindergeld, etc.) und in der Ausübung seiner Pflichten (Zahlung von Unterhalt) unterstützt werden. Er bleibt dabei gegenüber Dritten völlig anonym, da die Analyse vertraulich auf dem eigenen Rechner stattfindet.

4.2.3 Integrationsdienste

Um die Datenbasis für elektronische Safes zu vergrößern, werden Dienste entwickelt, welche eine einfache Integration weiterer digitaler Informationen in den eigenen Safe ermöglichen. Ein Beispiel für solch einen Dienst stellt die vertrauenswürdige Digitalisierung dar. Hieran wird im Folgenden die Funktionsweise solcher Dienste exemplarisch dargestellt.

Vertrauenswürdige Digitalisierung

Die Digitalisierung der Gesellschaft schreitet immer weiter voran. Viele Prozesse und Dienstleistungen können heute schon elektronisch, medienbruchfrei abgewickelt werden. Unternehmen bieten ihren Kunden diverse elektronische Services an, wie zum Beispiel die Produktbestellung mit digitaler Rechnungsbegleichung oder der selbständigen Servicekonfiguration. Öffentliche Verwaltungen unterstützen die elektronische Anmeldung von Gefahrguttransporten, die Online-Übermittlung der eigenen Steuererklärung oder den standardisierten Austausch von Meldedateninformationen. Nach wie vor liegt jedoch ein großer Teil von Daten und Dokumenten nicht digital vor, nach wie vor finden auch große Teile von Prozessen papierbasiert statt. Dies hat verschiedene Gründe, von kulturell-organisatorischen Pfadabhängigkeiten über gesellschaftlich-wirtschaftliche Barrieren bis zu nicht gelösten technischen Herausforderungen. Um die Teilhabe an elektronischen Prozessen und damit an der wachsenden digitalen Gesellschaft für Bürger, Unternehmen und Verwaltun-

[21] Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme. Vgl. Abrufbar unter: http://www.bundesfinanzministerium.de/nn_314/DE/BMF__Startseite/Service/Downloads/Abt__IV/BMF__Schreiben/015,templateId=raw,property=publicationFile.pdf.

gen mit papierbasierten Daten zu erleichtern, werden rund um den elektronischen Safe Integrationsdienste aufgebaut. Diese ermöglichen die einfache und vertrauenswürdige Digitalisierung analoger Daten.

Mit Hilfe solcher Dienste können verschiedene Hindernisse, die bei der Transformation hin zu einer digitalen Gesellschaft entstehen, verringert werden. Vor dem Hintergrund der Gefahr einer digitalen Spaltung (digital divide) moderner Zivilgesellschaften bieten Digitalisierungsdienste Chancen zur Teilhabe an elektronischen Geschäftsprozessen für Bevölkerungsgruppen, deren Daten überwiegend in Form papierbasierter Unterlagen vorliegen. Für Personengruppen, für die die selbständige Digitalisierung ein Hindernis darstellt, können entsprechende Services angeboten werden.

Ganz allgemein bietet sich mit der vertrauenswürdigen Digitalisierung der eigenen Unterlagen die Möglichkeit, für eventuelle Schadensfälle vorzusorgen. Die zusätzliche Verwahrung wichtiger persönlicher, geschäftlicher und amtlicher Unterlagen in elektronischen Safes beugt einem möglichen Totalverlust bei Unglücken wie Wohnungsdiebstahl, Brand oder Hochwasser vor. Selbst wenn die digitalisierten Unterlagen nicht die gleiche Beweiskraft wie die analogen Originalurkunden aufgrund fehlender elektronischer Signaturen oder gesetzlicher Grundlagen haben sollten, kann die erneute Ausstellung unterstützt werden.

Einmal digitalisierte Daten und Dokumente können sicher im eigenen elektronischen Safe aufbewahrt werden. Durch die Anbindung von Lösungen zur vertrauenswürdigen Archivierung können im Safe vorliegende Daten vergleichsweise einfach in die Langzeitarchivierung überführt werden. Mit der Verwahrung der Daten in elektronischen Safes und anschließender Archivierung nimmt der Bedarf, den Privatpersonen und besonders Organisationen zur Aufbewahrung von Papierunterlagen haben, ab. Vorausgesetzt die digitalisierten Daten können als Ersatz für die jeweilige analoge Vorlage verwendet werden, kann von nicht unerheblichen Einsparpotentialen durch Ansätze zur vertrauenswürdigen Digitalisierung ausgegangen werden. Hierbei kann der Einsatz der qualifizierten elektronischen Signatur für den Verzicht auf papierbasierte Originale die wesentliche Vorbedingung darstellen.

Mit der Digitalisierung erhöht sich auch die Auffindbarkeit spezifischer Daten. Der elektronische Safe bietet Funktionen zur Beschreibung der enthaltenen Daten mit Hilfe von Metadaten. Über eine leistungsfähige Suchfunktion können unter Rückgriff auf die Metadaten und die Volltexte einzelne Unterlagen schnell aufgefunden und eingesetzt werden.

Das Vorliegen der eigenen Daten in digitaler Form vereinfacht es für Safeeigentümer, diese Daten mit Dritten zu teilen. Dabei unterstützt der elektronische Safe die Freigabe von Daten an andere Nutzer auf datenschutzkonforme Art. So können private Daten wie zum Beispiel Fotos anderen Inhabern eines

Safes zur Verfügung gestellt werden, ohne dass Provider diesen Vorgang nachverfolgen können. Im Gegensatz zu vielen Plattformen gerade im Bereich des Web 2.0 wie sozialen Netzwerken bleiben die einmal digitalisierten Daten somit unter der Kontrolle des Safeeigentümers und können nicht von Safeanbietern für eigene Zwecke verwendet werden.

Die Entwicklung des elektronischen Safes als sicherer und vertrauenswürdiger Online-Speicher in der Cloud gewährleistet eine orts- und endgeräteunabhängige Verfügbarkeit der enthaltenen Daten und Dokumente für den Safeeigentümer. Einen Safeclient für das jeweilige System und eine Internetverbindung vorausgesetzt, kann der Safeeigentümer von zu Hause, aus dem Büro, einem Internetcafé, einem Bürgeramt oder von einem Mobilfunkgerät auf die im Safe vorliegenden Daten zugreifen.

Digitalisierte Daten und Dokumente bilden eine wichtige Voraussetzung für die Abwicklung organisationsübergreifender Prozessketten innerhalb von Wirtschaft und Verwaltung und zwischen Einrichtungen dieser Sektoren. Mit Hilfe effizienter und gleichzeitig vertrauenswürdiger Dienste zur Digitalisierung bisher nur analog vorliegender Datensätze können digitale Prozesse ausgeweitet und mit geringerem Aufwand an papierbasierte Vorgänge angeschlossen werden.

Grundsätzlich sind zwei Methoden zur Digitalisierung denkbar:

- Eine reine Bilddigitalisierung digitalisiert physische Dokumente in Pixeldaten. Diese Art der Digitalisierung erzeugt relativ große Datenmengen, welche durch Kompressionsalgorithmen zum Teil verkleinert werden können. Die so digitalisierten Dokumente stehen medienbruchfreien Prozessen als Eingabe zur Verfügung, bedürfen allerdings immer einer menschlichen Interaktion bei der Auswertung ihres Inhaltes.
- Bei einer elektronischen Reinschrift oder Abschrift werden die Informationen des physischen Dokuments in eine elektronische, maschinenlesbare, möglichst standardisierte Form gebracht. Beispiele für diese Standards sind in der XÖV-Welt, den XML-Standards der deutschen öffentlichen Verwaltung, zu finden. Weitere Standards müssen für weit verbreitete physische Dokumentenarten geschaffen werden.

Der besondere Mehrwert elektronischer Reinschriften ergibt sich durch die Möglichkeit zur elektronischen Auswertung ohne menschliche Interaktion. Fachverfahren können so bestimmte Auswertungen oder Berechnungen auf Basis dieser Daten automatisiert ausführen. Weiterhin sind der geringe Speicherbedarf, und die bessere Durchsuchbarkeit prägnante Vorteile gegenüber einer Bilddigitalisierung.

Alternativ kann digitales Bildrohmaterial von physischen Dokumenten mit Texterkennungstechnologien (OCR[22]) verarbeitet werden, um die Inhalte des Dokuments auszulesen. Da je nach Zustand und Lesbarkeit des physischen Dokuments, der optischen Genauigkeit der Digitalisierungseinheit und der eingesetzten Software qualitativ sehr unterschiedliche Ergebnisse geliefert werden, erfordert der Einsatz von Texterkennungstechnologien allerdings eine manuelle Prüfung bzw. Korrektur des Ergebnisses.

Grundsätzlich ist die elektronische Reinschrift der reinen Bilddigitalisierung vorzuziehen, da die daraus entstehenden elektronischen Dokumente flexibler eingesetzt werden können. Ein maschinenlesbares, standardisiertes XML-basiertes Format garantiert darüber hinaus auch eine dauerhafte Verfügbarkeit (im Sinne der Lesbarkeit).

Die Bilddigitalisierung wiederum ist der elektronischen Reinschrift vorzuziehen, wenn der Aufwand zur Erstellung der elektronischen Reinschrift in keinem Verhältnis zum späteren Nutzen steht. Beispiele hierfür wären die Digitalisierung großer Dokumentenarchive, Digitalisierung ausschließlich zur elektronischen Archivierung oder allgemein die Digitalisierung von Dokumenten, die später selten bzw. nie in elektronischen Prozessen verwendet werden. Die Bilddigitalisierung erfolgt dabei ausschließlich unter Verwendung von standardisierten, für langfristige Verfügbarkeit ausgelegten Dokumentenformaten wie PDF/A oder TIFF.

Einfache Digitalisierung

Die Digitalisierung kann, entsprechende Hard- und Software (Scanner, Digitalkamera, Fotobearbeitungssoftware) sowie das nötige technische Verständnis vorausgesetzt, jeder im eigenen Heim erledigen, was größtmögliche Vertraulichkeit garantiert. Optional kann der Eigentümer seine digitalisierten Dokumente elektronisch signieren, um im Falle einer Freigabe die Urheberschaft dieser digitalen Kopie nachzuweisen.

Für eine große Basis digitaler Dokumente auf Seiten der Bürger zur Nutzung in elektronischen Prozessen von Wirtschaft und öffentlicher Verwaltung reicht es nicht aus, auf die Eigeninitiative technisch interessierter Nutzer zu bauen. Vielmehr müssen hierfür Dienstleistungen zur einfachen, vertrauenswürdigen und kostengünstigen Digitalisierung bestehender physischer Dokumente zumindest in einer Übergangszeit etabliert werden, die in eine elektronische Prozessplattform eingebunden werden können

Auch bei der einfachen Digitalisierung muss die Vertraulichkeit der zu digitalisierenden Dokumente gewährleistet werden. Diese Anforderung kann dazu

[22] Optical Character Recognition.

führen, dass beispielsweise (mobile) Selbstbedienungsautomaten für diese Aufgabe etabliert werden müssen. Dritte, etwa Mitarbeiter eines Dienstleisters, bekommen somit die potentiell vertraulichen Dokumente nicht zu sehen. Vergleichbar mit Bankautomaten sind diese Digitalisierungseinheiten geschlossene Systeme und unterliegen höchsten Sicherheitsanforderungen. Sie stellen die digitalisierten Dokumente ohne Zwischenspeicherung direkt in den Posteingang des elektronischen Safes des Eigentümers ein. Auch die Digitalisierung größerer Datenbestände kann, sofern diese nicht selbst vorgenommen wird, über Selbstbedienungsautomaten mit automatischem Einzug erfolgen.

Die höchsten Sicherheitsanforderungen an diese Systeme sind allerdings kein Garant für eine absolute Vertraulichkeit. Aufgrund der physischen Größe, der Verteilung der einzelnen Komponenten (Scaneinheit, Bedienungseinheit etc.) sowie insbesondere dem öffentlichen Zugang zu diesen Systemen kann eine Manipulation faktisch niemals ausgeschlossen werden. Hier muss der Eigentümer auf die organisatorischen Sicherheitsaspekte vertrauen und nur vertrauenswürdige Digitalisierungseinheiten verwenden.

Aus Sicherheitsgründen muss überlegt werden, ob die Digitalisierungseinheiten mit Komponenten zur qualifizierten elektronischen Signatur auszustatten sind. Aufgrund der rechtlichen Stellung der qualifizierten elektronischen Signatur und des damit einhergehenden Missbrauchspotentials aus Sicht des Bürgers müssen besondere Vorkehrungen bei der Nutzung getroffen werden. Öffentlich zugängliche Kiosksysteme mit Komponenten zur qualifizierten elektronischen Signatur müssen entsprechend (erkennbar) zertifizierte, geschlossene Systeme sein. Die Kosten der Einführung entsprechender Digitalisierungseinheiten wären somit höher. In jedem Fall sollten bei der Digitalisierung analoger Datenbestände die zu digitalisierenden Unterlagen von der Digitalisierungseinheit signiert werden (Automatensignatur), um so beispielsweise eine Nachbearbeitung mittels Graphikverarbeitung oder die technische Urheberschaft anzuzeigen. Eine qualifizierte elektronische Signatur des Eigentümers kann bei Übernahmen aus dem Posteingang auf dem sicheren System des Eigentümers (nachträglich) erfolgen.

Digitale Beglaubigungen

Insbesondere zum Nachweis „verbriefter Rechte“ werden physische Dokumente in Form beglaubigter Kopien weitergegeben. Bei der Digitalisierung dieser Dokumente sollte deren Nachweisfunktion erhalten bleiben. Hierzu muss die elektronische Kopie „beglaubigt“ werden. Das Mittel zur Beglaubigung elektronischer Dokumente ist die elektronische Signatur durch eine vertrauenswürdige Instanz. Nach derzeitigem Recht kommen als solche Notare, staatliche Stellen sowie abhängig vom Bundesland einige andere Akteure in Betracht.

Grundsätzlich gelten die gleichen technischen Anforderungen hinsichtlich Sicherheit und Vertraulichkeit wie für die einfache Digitalisierung. Das heißt, dass auch hierfür bei entsprechend autorisierten Instanzen Digitalisierungseinheiten etabliert werden müssen. Im Unterschied zur einfachen Digitalisierung werden diese allerdings nicht vom Eigentümer, sondern von der beglaubigenden Partei bedient. Die digitalisierten Daten und Dokumente werden mit dem Schlüsselmaterial der beglaubigenden Partei elektronisch signiert und vom System ohne Zwischenspeicherung direkt in den Posteingang des elektronischen Safes des Eigentümers der Unterlagen eingestellt. Für die Nachweisfunktion muss die Signatur der beglaubigten, elektronischen Kopie des physischen Dokuments von Dritten verifiziert werden können. Hierzu muss das öffentliche Schlüsselmaterial der beglaubigenden Partei für den Verifizierenden zugänglich sein. Entsprechende PKI-Systeme müssen zur Verfügung stehen.

Zur langfristigen Wahrung der Nachweisfunktion müssen die Grundsätze zur Langzeitsicherung elektronisch signierter Dokumente beachtet werden. Beglaubigte elektronische Dokumente müssen demnach erneut signiert werden, bevor die kryptographischen Algorithmen ihre Sicherheitseigenschaften verlieren[23].

Anwendungsbeispiele für die vertrauliche Digitalisierung

Die vertrauenswürdige Digitalisierung kann von verschiedenen Einrichtungen als Dienst angeboten werden. Hierfür kommen besonders Organisationen in Betracht, welche nicht selbst als Safeanbieter auftreten. So kann der Verdacht ausgeschlossen werden, dass ein Safeanbieter Einblicke in die zu digitalisierenden Unterlagen eines Kunden aufzeichnet und so über eine Vorstellung der späteren Safeinhalte verfügt.

Digitalisierung kann und wird als Selbstbedienung oder im Auftrag angeboten. Wird sie im Auftrag durchgeführt, bieten sich hierbei vor allem Organisationen an, die bereits heute vertrauensvoll mit sensiblen Daten im Kundenauftrag umgehen. Diese Einrichtungen verfügen bereits über Prozesse, mit denen die Vertraulichkeit ihrer Kundendaten auf einem hohen Niveau sichergestellt werden kann. Solche Organisationen können zum Beispiel Banken, Versicherungen oder Postdienstleistungsunternehmen sein.

Abhängig von der anbietenden Einrichtung wird die vertrauenswürdige Digitalisierung als eigenständige oder inklusive Dienstleistung angeboten. Versicherungsunternehmen könnten dies beispielsweise im Paket mit Hausratversicherungen anbieten. Für Postunternehmen bietet sich hier eher eine separat an-

[23] Vgl. § 17 Verordnung zur elektronischen Signatur.

gebotene Dienstleistung an, da die klassische Briefbeförderung ebenfalls einzeln berechnet wird.

4.2.4 Spezialdienst Trusted Third Party

Zum Schutz vor Verlust des Zugangs zum elektronischen Safe durch Verlust oder Beschädigung entsprechender physischer Zugangsmechanismen kann der Safeeigentümer einen alternativen Zugang für eine vertrauenswürdige dritte Instanz einrichten. Diese sogenannte „Trusted Third Party“ ist dem Safeanbieter bekannt. Im Falle des Verlustes kann sich der Safeeigentümer gemeinsam mit der Trusted Third Party an den Safeanbieter wenden, um den eigenen Zugang wieder herzustellen. Die Wiederherstellung erfolgt dabei im 3-Parteienprinzip. Der Safeanbieter muss sowohl Safeeigentümer als auch Trusted Third Party zweifelsfrei identifizieren, bevor der Zugang für den Safeeigentümer wiederhergestellt wird.

Der Safeeigentümer ist frei in der Wahl seiner Trusted Third Party. Grundsätzlich müssen Ausfallsicherheit und Privacy-Aspekte bei der Wahl berücksichtigt werden. Spezialisierte Dienstleister können eine hohe Ausfallsicherheit garantieren, Gefährdungs- und Missbrauchpotential sind allerdings höher. Notare oder Rechtsanwälte bieten auf Grund ihrer besonderen rechtlichen Stellung und Aufgabe im Verhältnis zum Staat einen höheren organisatorischen Schutz. Bei vertrauenswürdigen Personen aus dem direkten Umfeld des Safeeigentümers ist die Ausfallwahrscheinlichkeit höher.

Die Nutzung eines elektronischen Safes sollte keine Voraussetzung sein, um als Trusted Third Party für andere zu fungieren. Grundsätzlich wird nur ein geeigneter öffentlicher Schlüssel der Trusted Third Party für die Verschlüsselung der Zugangskopie benötigt. Der Dienst kann allerdings mit den Mitteln des elektronischen Safes (Schlüsselmaterial, Safeclient) realisiert werden. Der einfachste und aus Sicht des Safeeigentümers vertrauenswürdigste Fall wäre somit, dass der Safeeigentümer mit dem Schlüsselmaterial eines zweiten Safeaccounts als seine eigene Trusted Third Party auftritt. Hierfür kann er sich einen zweiten Safeaccount einrichten, deren Zugangsmechanismen (z.B. Chipkarte) in einem Bankschließfach oder bei einem Notar vor unberechtigter Einsichtnahme und zum physikalischen Schutz hinterlegt werden.

5. Rechtliche Aspekte

Im Rahmen der rechtlichen Betrachtung stellt sich die Frage, ob die beschriebene Safe-Infrastruktur zur Erhöhung der Akzeptanz, vor allem in der öffentlichen Verwaltung, eines gesetzlichen Rahmens bedarf. Hierzu ist es denkbar, den Safeanbieter selbst zu reglementieren und Anforderungen an den elektronischen Safe zu normieren. Hinzu kommen Rechtsfragen, die aus dem konkreten Einsatz des Safes und seiner Dienste im E-Government und E-Commerce resultieren. Ein Rechtsrahmen muss insbesondere die Aspekte der Datensicherheit, der Datenvertraulichkeit und der Datenverfügbarkeit adressieren. Vorhandene Regelungskomplexe (bspw. BDSG und BSI-Zertifizierungen) sind dazu bereichsspezifisch fortzuentwickeln[24]. Sachgerecht erscheinen darüber hinaus eine eigenständige Akkreditierung vertraulicher Safeanbieter sowie effektive Instrumente einer staatlichen repressiven Kontrolle. Vorhandene Ansätze (bspw. der De-Mail-Gesetzentwurf) sollten dabei aufgegriffen und vor allem um safespezifische Vorgaben ergänzt werden. Angesichts der fehlenden 100-prozentigen Sicherheit informationstechnischer Systeme und elektronischer Safes kann ein Rechtsrahmen der Akzeptanzsteigerung dienen, Rechtsunsicherheiten abbauen und so einen Einsatz auch in und durch die öffentliche Verwaltung forcieren. So kommen beispielsweise der Nachweisbarkeit (elektronischer) Zustellungen, Fragen der Zugangseröffnung und ähnlichem in Verwaltungsverfahren erhebliche Bedeutung zu. Der flächendeckende Einsatz von Safe-Kommunikation, Diensten und übergreifenden Prozessketten ohne eine Anpassung der rechtlichen Grundlagen und – wie heute – ausschließlich basierend auf einzelfallbezogener Rechtsprechung erscheint wenig wahrscheinlich.

5.1 Rechtliche Aspekte des Safeanbieters

Zu Beginn des Projektes stand die Idee, aufgrund der fehlenden Nachvollziehbarkeit technischer Vorgänge eines Safes für den Nutzer, diesen bei einer vertrauenswürdigen Instanz (bspw. Notaren bzw. „Datennotaren“) anzusiedeln oder zumindest überwachen zu lassen. Allerdings wurde seit Projektbeginn die technische Ausgestaltung elektronischer Safes so fortentwickelt, dass von einem neuen Niveau bezüglich Datensicherheit und Datenschutz ausgegangen werden kann, das eine vertrauenswürdige Instanz zwar nicht vollständig entbehrlich macht, aber auch ohne die besondere Stellung eines Notars im privatwirtschaftlichen Raum durch IT-Anbieter und damit auch einer gesteigerten Usability realisiert werden kann. Trotz einer verbesserten technischen Sicherheit kommt der Ausgestaltung der organisatorischen und rechtlichen Rahmenbedingungen weiterhin eine gewisse Bedeutung zu, da kein techni-

[24] S. *Schulz*, DuD 2009, 601 (605); *Warnecke*, MMR 2010, 225 (230).

sches System vollständige Sicherheit gewährleisten kann. Auch unterscheidet sich das bisherige Aufgabenprofil der Notare von der im Rahmen der Studie entwickelten Perspektive, die vielmehr eine Verortung elektronischer Safes im privatrechtlichen Raum bei gleichzeitiger Sicherstellung der Vertraulichkeit und Akzeptanz durch staatliche Reglementierung und Überwachung nahelegt.

Für den Nutzer wird auch weiterhin technisch kaum nachvollziehbar sein, ob der ausgewählte Safeanbieter die ihm anvertrauten Daten tatsächlich sicher und vertraulich behandelt. Neben den beschriebenen technischen Anforderungen können daher gerade gesetzliche Grundlagen in zweifacherweise zur Bildung des notwendigen Vertrauens und so zur Akzeptanzsteigerung beitragen: Zum einen kann dem Nutzer die Auswahl eines geeigneten und vertrauenswürdigen Anbieters erleichtert werden, indem der Staat seiner Infrastrukturverantwortung durch das Aufstellen von Rahmenbedingungen nachkommt, die ein vertrauenswürdiger Anbieter erfüllen muss.[25] Zum anderen kann ein gesetzlicher Rahmen, der unerwünschte Risiken abfedert (z.B. Fragen der Haftung im Falle des Datenverlustes, Zulässigkeit von Vertragsklauseln, allgemeine Rechtsschutzmöglichkeiten) dem Einzelnen ein subjektives Sicherheitsgefühl vermitteln. Da aber ein blinder Glaube an die Schutzpotenziale des Rechts genauso wenig wie an die der Technik zum Ziel führt, bedarf es eines sinnvollen Zusammenspiels beider Komponenten.[26]

Gleichzeitig muss ein gesetzlicher Rahmen den Safeanbietern aber auch hinreichende Flexibilität für attraktive Geschäftsmodelle bieten. So können einige Funktionalitäten und Anforderungen verpflichtend, bspw. im Rahmen einer Regulationsrechtsetzung bzw. eines Zertifizierungsverfahrens zu erbringen sein, andere freiwillig als Ergänzung zu diesem Mindeststandard ausgehend von der Nachfrage der Nutzer hinzutreten. Damit entsteht für den Nutzer ggf. ein Mehrwert, der in der Lage ist, dem Safeanbieter einen Wettbewerbsvorteil gegenüber seinen Mitbewerbern zu verschaffen. Gerade die aufgezeigten Dienste („Apps“) könnten sich außerhalb der staatlichen Reglementierung der eigentlichen Safeinfrastruktur und ihrer Anbieter bewegen und so ausreichend Raum für privatwirtschaftliche Geschäftsmodelle und eine Abgrenzung von Konkurrenten bieten.

---

[25] Dazu im Kontext der Virtualisierung zahlreicher Lebensbereiche *Anika D. Luch/Sönke E. Schulz.* E-Daseinsvorsorge staatliche Schutzpflichten und Sozialstaatsprinzip im Lichte der Virtualisierung des Lebens, in: Hill/Schliesky (Hrsg.), Herausforderung E-Government: E-Volution des Rechts- und Verwaltungssystems, Baden-Baden 2009, S. 305-335; *dies.*, eDaseinsvorsorge – Neuorientierung des überkommenen (Rechts-)Begriffs Daseinsvorsorge im Zuge technischer Entwicklungen?, MMR 2009, S. 19-24; *Sönke E. Schulz*, E-Daseinsvorsorge – der Grundversorgungsauftrag des Staates im Lichte der Virtualisierung zahlreicher Lebensbereiche, in: Vitako aktuell 4/2009, S. 30 f.; *ders.*, E-Daseinsvorsorge für das Leben im Netz, in: Datareport 1/2010, S. 18 f.

[26] *Hornung*, MMR 2004, 3 (7); vgl. dazu auch *Gusy*, DuD 2009, 33 (35); speziell zum Datenschutzrecht *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. II, § 22, Rn. 34 ff.

Notwendig ist daher ein eigenständiges Gesetz, gegebenenfalls in Verbindung mit einer Rechtsverordnung, welches verbindliche Anforderungen an Anbieter elektronischer Safes aufstellt. Denkbar wäre auch eine Fortentwicklung der safespezifischen Bestandteile des De-Mail-Gesetz(entwurfs). Durch darin definierte inhaltliche und organisatorische Vorgaben wie Zulassung, Aufsicht und Kontrolle kann der Staat hohe Anforderungen an Sicherheit, Datenschutz und Funktionen der Angebote definieren. Damit potentielle Nutzer die Vertrauenswürdigkeit eines Anbieters erkennen können, muss die Möglichkeit geschaffen werden, die Erfüllung der Vorgaben durch eine Zertifizierung bestätigen zu lassen und durch ein Gütezeichen nachzuweisen (bspw. ISO 27001). Das Instrument der Zertifizierung basiert auf der Idee, dass derjenige Anbieter einen Marktvorteil erhalten soll, der vordefinierte rechtliche Standards einhält und dieses seinen Kunden gegenüber durch ein Zertifikat nachweisen kann.[27] Besonders bei komplexen und zudem grundrechtsrelevanten Gebieten wie dem elektronischen Daten- und Dokumentensafe kann ein solches Gütesiegel große Bedeutung erlangen, da der Nutzer die technischen Prozesse nicht überschauen kann.

Wichtig bei einem solchen Verfahren ist die Prüfung der Einhaltung dieser Standards durch geeignete Institutionen. In Bezug auf die Informationstechnik bietet sich aufgrund der hohen Fachkompetenz als allgemein anerkannte Instanz das Bundesamt für Sicherheit in der Informationstechnik (BSI) an. Da es heute bereits Prüfungen und Bewertungen für informationstechnische Systeme, Komponenten und Produkte durchführt, könnten zukünftig Prüfungen bzgl. der Zertifizierungsvoraussetzungen der Diensteanbieter hinzukommen. Die Zertifizierung, die in Form eines Verwaltungsaktes i.S.d. § 35 VwVfG vorgenommen wird, bietet einen verlässlichen Nachweis der überprüften Vertrauenswürdigkeit des angebotenen Dienstes, da nur Anbieter, die die strengen Anforderungen erfüllen, das staatliche Gütezeichen erhalten und mit diesem auf dem Markt um das Vertrauen der Kunden werben können. Darüber hinaus könnte das Gütezeichen zum Tragen einer vertrauensstärkenden Bezeichnung, wie etwa „zertifizierter Daten- und Dokumentensafeanbieter“ berechtigen. Durch ein Zertifizierungssystem, welchem sich Anbieter freiwillig anschließen können, kann die Erfüllung von vordefinierten gesetzlichen Standards vorab und danach in regelmäßigen Zeitabständen und ggf. auch bei wesentlichen Änderungen des Dienstes durch das BSI als öffentlich anerkannte fachkundige Stelle umfassend geprüft und bestätigt werden. Die Kombination aus gesetzlichen Rahmenbedingungen und begleitender Qualitätssicherung kann dabei zur Gewährleistung des grundrechtlich gebotenen Schutzniveaus beitragen.

---

[27] *Weichert*, in: Klumpp/Kubicek/Roßnagel/Schulz (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, S. 325; zu Zertifizierungen von Software und Systemen *Quiring-Kock*, DuD 2010, 178 (179); zum sog. Datenschutzaudit vgl. auch *Bizer*, in: Simitis (Hrsg.), BDSG, § 9a Rn. 2 ff; *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. II, § 22, Rn. 164.

Legt man dieses Modell zu Grunde, würde sich der Markt für Safeanbieter differenzieren – nach Durchführung eines (freiwilligen) Zertifizierungsverfahrens wäre man nicht nur zum Führen einer bestimmten Bezeichnung berechtigt, denkbar erscheint es gerade auch bestimmte Funktionalitäten (bspw. den rechtssicheren Austausch mit Behörden, die Gleichstellung elektronischer Safe-Kommunikation mit der Brief- oder De-Mail-Kommunikation) ausschließlich auf Anbieter, die einen „sicheren Safe“ im oben beschriebenen Verständnis anbieten, zu begrenzen. Eine Anpassung des Verwaltungszustellungsgesetzes, wie im Rahmen des De-Mail-Gesetzes beabsichtigt, könnte diese Besserstellung rechtlich abbilden. Daneben bestünde weiterhin ein Markt „freier“ Anbieter, die bspw. die schon heute denkbaren und vorhandenen Services einer Online-Festplatte anbieten könnten. Der Nutzer ist dann in die Lage versetzt, ausgehend von seinen persönlichen Anforderungen eine Entscheidung zu treffen. Hinzu käme ein Markt für Safedienste („Apps“), die soweit sie die Vertraulichkeit der eigentlichen Safeinfrastruktur nicht beeinträchtigen, ebenfalls unreglementiert angeboten werden können. Die zertifizierten Safeanbieter könnten – gesetzlich oder im Rahmen der Vertragsbeziehung – verpflichtet werden, ausschließlich solche Apps zu akzeptieren und einzubinden, die diese Voraussetzung erfüllen.

5.2 Regelungsinhalt eines einfach-gesetzlichen Rechtsrahmens elektronischer Daten- und Dokumentensafes

Voraussetzungen der Zertifizierung

Inhaltlich erfordert der Rechtsrahmen zunächst die Voraussetzungen der Zertifizierung. Als solche sind die technischen Anforderungen an Safeanbieter zu formulieren. Die Art der Speicherung muss dabei die Datensicherheit, Datenintegrität, Datenvertraulichkeit sowie die Datenverfügbarkeit sicherstellen. Für den Bereich des Postfach- und Versanddienstes enthält das De-Mail-Gesetz entsprechende Vorgaben, die im Detail zwar Kritik herausfordern, jedoch als Leitlinie zur Sicherstellung der Vertraulichkeit geeignet erscheinen. Demgegenüber sind safespezifische Regelungen bisher nur rudimentär angelegt; unklar bleibt auch, ob Safes nur bei Erfüllung der übrigen Vorgaben angeboten werden dürfen und ob diese entsprechend übertragen werden können. Insoweit kann der De-Safe-Dienst allenfalls als „Online-Festplatte“ und nicht als „Safe“ bezeichnet werden – problematisch ist insbesondere der Umstand, dass eine Verschlüsselung nur auf Seiten des Anbieters vorgesehen ist, Ver-

traulichkeit der Daten ihm gegenüber aber nur durch eine clientseitige Verschlüsselung erreicht werden kann.[28]

Der Aspekt der **Datensicherheit** wird durch technisch-organisatorische Maßnahmen, bspw. den Betrieb eines den Anforderungen des BSI genügenden Rechenzentrums gewährleistet. Gleiches gilt für die erforderliche fachliche Qualifikation, persönliche Integrität und Fachkunde des Betreibers und seiner im Rechenzentrum tätigen Mitarbeiter. Zudem hat der Anbieter durch entsprechende Zeugnisse nachzuweisen, dass bei Gestaltung und Betrieb des Angebots Aspekte der IT-Sicherheit berücksichtigt wurden. Ob und inwieweit derartige Vorgaben für Safeanbieter im Rahmen einer Regulierungsgesetzgebung gefordert werden, ist abhängig davon, welches Schutzniveau für erforderlich gehalten wird und ob man die bestehenden Regelungen – bspw. auch aus dem BDSG – die ohne ein Zertifizierungs-, Akkreditierungs- oder Auditierungsverfahren Geltung beanspruchen, für ausreichend erachtet.

Der Aspekt der IT-Sicherheit wird jedoch zunehmend an Bedeutung gewinnen. So werden auch in privatrechtlichen Vertragsverhältnissen die Vorgaben des Bundesverfassungsgerichts zur Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, in dessen Schutzbereich auch elektronische Safes bzw. deren Inhalte fallen, Beachtung finden müssen. Gleiches gilt für die Ausführungen in der Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung, in dem der Gesetzgeber verpflichtet wird, für den Fall, dass er Speicherpflichten der Anbieter vorsieht, diese zugleich auch auf bestimmte Vorgaben an IT-Sicherheit und Datensicherheit zu verpflichten (Leitsatz 4: „Hinsichtlich der Datensicherheit bedarf es Regelungen, die einen besonders hohen Sicherheitsstandard normenklar und verbindlich vorgeben. Es ist jedenfalls dem Grunde nach gesetzlich sicherzustellen, dass sich dieser an dem Entwicklungsstand der Fachdiskussion orientiert, neue Erkenntnisse und Einsichten fortlaufend aufnimmt und nicht unter dem Vorbehalt einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten steht“).[29]

Die **Datenvertraulichkeit** muss sowohl gegenüber externen als auch internen Zugriffen gesichert werden. Vorgaben zur Datenintegrität und Datenvertraulichkeit enthält vor allem das BDSG, welches auch Geltung beansprucht, wenn keine gesonderten Zertifizierungs-, Akkreditierungs- oder Auditierungsverfahren für Safeanbieter eingeführt werden.

Danach hat der Anbieter nachzuweisen, dass bei Gestaltung und Betrieb des Angebots die datenschutzrechtlichen Anforderungen eingehalten werden. Da-

[28] Vgl. auch *Lapp*, DuD 2009, 651 (655), der aus dem Umstand der fehlenden Vorgaben im Bürgerportal-Gesetz allerdings den Schluss zieht, dass § 8 ersatzlos gestrichen werden sollte.

[29] BVerfG, 1 BvR 256/08 v. 2.3.2010.

zu gehören insbesondere die Anforderungen des § 9 BDSG, wonach bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten die erforderlichen technischen und organisatorischen Maßnahmen zu treffen sind, um die informationelle Selbstbestimmung der Nutzer zu gewährleisten.

Problematisch könnte – auch im Kontext von elektronischen Safes – der Einsatz von Cloud-Technologien werden. Kommt es bei der Nutzung cloudbasierter Dienste nämlich zur Verarbeitung personenbezogener Daten (§ 3 Abs. 1 BDSG), ist im Verhältnis zwischen dem Safeanbieter und weiteren an der Cloud-Infrastruktur beteiligten Unternehmen von einer Auftragsdatenverarbeitung i.S.d. § 11 BDSG auszugehen. Der Auftraggeber bleibt datenschutzrechtlich verantwortlich; er ist gem. § 11 Abs. 2 Satz 1 u. 4 BDSG zur sorgfältigen Auswahl und Überwachung des Anbieters verpflichtet. Entsprechende Aufträge sind schriftlich zu erteilen, wobei Verarbeitungsprozesse, technische und organisatorische Maßnahmen sowie etwaige Unterauftragsverhältnisse detailliert festzulegen sind. Gerade durch die exzessive Nutzung derartiger Unterauftragsverhältnisse treten Gefahren für den Schutz der personenbezogenen Daten auf – sie ist aber gerade für eine Cloud-Infrastruktur typisch und prägend, zumal auch ein Safeanbieter in der Regel zumindest in Zeiten einer Höchstauslastung zum Zukauf externer Server-, Rechen- und Softwarekapazitäten gezwungen ist. Hinzu kommt, dass personenbezogene Daten nicht ohne weiteres in Drittstaaten außerhalb der Europäischen Union übermittelt werden dürfen. Eine solche Übermittlung ohne Einschränkungen in Staaten außerhalb der Europäischen Union bzw. des Geltungsbereichs der Richtlinie 95/46/EG ist nur gem. § 4b Abs. 2 u. 3 BDSG statthaft, wenn in den einbezogenen Drittstaaten ein angemessenes Datenschutzniveau sichergestellt ist. Scheidet eine Auftragsdatenverarbeitung also in der Regel aus, käme eine Datenübermittlung in Betracht, die jedoch ebenfalls nur beim Vorliegen einer konkreten Einwilligung oder unter den strengen Voraussetzungen der §§ 28 ff. BDSG zulässig ist. Das Kostensparinteresse des Safeanbieters wird wohl keine Rechtfertigung geben können.

In diesem Kontext ist – abhängig von der technischen Ausgestaltung – zu klären, ob und inwieweit die im elektronischen Safe gespeicherten Daten bspw. im Fall einer Aufteilung auf unterschiedliche Safeanbieter überhaupt als personenbezogene Daten einzuordnen sind. In jedem Fall müssen die Vorgaben des BDSG gewahrt werden, wenn beim Safeanbieter diese Dateien in unverschlüsselter oder entschlüsselbarer Form vorliegen – selbst wenn eine sichere Erstanmeldung beim Safeanbieter (bspw. durch Nutzung des neuen Personalausweises) nicht vorgeschrieben ist. Allerdings setzt das Vertragsverhältnis zwischen Safeanbieter und Safeeigentümer in der Regel eine Identifizierung der Vertragspartner voraus.

Spezielle Vorgaben zur **Datenverfügbarkeit** enthält das nationale Recht derzeit nicht. Diese ist im Rahmen des zivilrechtlichen Vertrages zwischen Safee-

igentümer und Safeanbieter zu konkretisieren. Grundsätzlich sind keine rechtlichen Besonderheiten im Vergleich zu bestehenden Angeboten ersichtlich; der Vertragstyp ist abhängig vom gewählten Geschäftsmodell. In der Regel wird es sich um einen typengemischten Vertrag (miet-, dienst- und werkvertragliche Elemente) handeln. Auch etwaige Leistungsstörungen – also bspw. die Nichtverfügbarkeit der Daten – können grundsätzlich unter Rückgriff auf vergleichbare Angebote (E-Mail-Postfächer; Online-Festplatten) beurteilt werden. Lediglich dann, wenn der elektronische Safe zur Kommunikation mit staatlichen Stellen oder im Rechtsverkehr eingesetzt wird, ist zu beachten, dass sich solche Leistungsstörungen ggf. auch nachteilig auf das Verwaltungsverfahren auswirken können. Denkbare Leistungsstörungen sind bspw. die Nichterreichbarkeit des Safes, der Verlust oder Missbrauch der Daten im Safe, die Nichtzustellung von Freigaben, Fehler beim Einstellen von Dokumenten und Fehler bei der Protokollfunktion.

Die Datenverfügbarkeit muss durch technisch-organisatorische Maßnahmen gewährleistet werden, die gesetzlich vorgegeben werden. Der Anbieter sollte dazu angehalten sein, eine zuvor definierte Verfügbarkeitsgarantie zu gewährleisten. Auch wenn sich eine hundertprozentige Verfügbarkeit nicht sicherstellen lässt, muss die Verfügbarkeitsquote der Verfügbarkeit vergleichbarer Dienste entsprechen (Service Level Agreement).

Besondere Relevanz erhält der Grundsatz der (langfristigen) Datenverfügbarkeit vor allem im Kontext gesetzlicher Aufbewahrungsvorschriften und bei besonderen Nutzergruppen (Unternehmen, Anwälte, Ärzte etc.). Diese bleiben unverändert; soweit schon heute eine digitale Speicherung zulässig ist. Dies gilt auch für den Einsatz eines elektronischen Safes. Da ein Zugriff des Providers und damit eine „Kontrolle“ der Fristen durch ihn ausscheidet, liegt dies ausschließlich in der Verantwortungssphäre des Safeeigentümers, was durch geeignete Dienste im oben beschriebenen Sinne („Apps“) unterstützt werden kann.

Für den Bereich der Datenverfügbarkeit käme es ebenfalls in Betracht, den Safeanbieter, der eine Zertifizierung als vertraulicher Anbieter begehrt, gesetzlich auf bestimmte technische und organisatorische Maßnahmen zu verpflichten. Um diese – ebenfalls wie im Bereich Datensicherheit und -schutz – effektiv abzusichern, erscheint es denkbar, neben präventiven und repressiven staatlichen Instrumentarien auch besondere gesetzliche Haftungstatbestände (bspw. Garantiehaftung) zu schaffen und den Nachweis einer geeigneten Deckungsvorsorge zu verlangen.

Daneben sind die beschriebenen **Funktionalitäten des elektronischen Safes** als Mindeststandard vom Anbieter gesetzlich zu fordern. Insbesondere durch die Möglichkeit der Festlegung von Zugriffsrechten müssen dem Nutzer technische Hilfsmittel angeboten werden, die unterschiedliche Qualitätsstufen

hinsichtlich der Sicherheit ihrer Informationen eröffnen. Durch die Freigabe- und Protokollfunktion kann eine hinreichende Absicherung der Kontrollmöglichkeiten gewährleistet werden. Die Provider sollten ebenfalls verpflichtet werden, Mittel zur Verschlüsselung und zur Erstellung einer digitalen Signatur standardmäßig bereitzustellen. Gleichzeitig muss ein gesetzlicher Rahmen den Safeanbietern aber auch hinreichende Flexibilität für attraktive Geschäftsmodelle bieten. So können einige Funktionalitäten und Anforderungen verpflichtend zu erbringen sein, andere freiwillig als Ergänzung zu diesem Mindeststandard ausgehend von der Nachfrage der Nutzer hinzutreten. Gerade die aufgezeigten Dienste („Apps“) könnten sich außerhalb der staatlichen Reglementierung der eigentlichen Safeinfrastruktur und ihrer Anbieter bewegen und so ausreichend Raum für privatwirtschaftliche Geschäftsmodelle und eine Abgrenzung von Konkurrenten bieten.

Organisatorische Vorgaben

Darüber hinaus sind weitere zwingende Elemente der regulatorischen Ausgestaltung für eine grundrechtskonforme Ausgestaltung erforderlich.

Auflösung und Sperrung /„Umzug“

Wichtig ist die Möglichkeit des Nutzers, seinen Datensafe aufzulösen sowie die damit verbundene Verpflichtung des Anbieters keine Daten wie etwa Sicherungskopien des Nutzers nach der Auflösung des Kontos mehr vorzuhalten. Ob neben dem Safeeigentümer weiteren Personen diese, wie auch andere, Rechte eingeräumt werden, bedarf einer eigenverantwortlichen Entscheidung des Eigentümers, der dann ggf. auch das Risiko eines Missbrauchs im Innenverhältnis trägt.

Eine Sperrmöglichkeit des Datensafes seitens des Anbieters darf indes aufgrund der Bedeutung des Safes für den Nutzer nur in äußerst begrenztem Maße zugelassen werden, etwa wenn seitens des Nutzers gegen Vertragspflichten verstoßen wurde.

Für den Fall, dass der Anbieter seinen Dienst einstellt, hat er den Nutzer unverzüglich darüber zu informieren. Zugleich muss der Anbieter dazu verpflichtet werden, die im Safe gespeicherten Daten für einen angemessenen Zeitraum nach Benachrichtigung für den Nutzer abrufbar zu halten. Aufgrund der erheblichen Bedeutung der Daten muss dem Nutzer ausreichende Zeit zur Verfügung gestellt werden, die Daten anderweitig zu sichern oder zu einem anderen Anbieter zu wechseln. Dabei muss ein möglichst barrierefreier „Umzug“ von einem Safeanbieter zu einem anderen sichergestellt werden. Insbesondere muss durch rechtliche Vorgaben die Interoperabilität zwischen den

Anbietern gewährleistet sein, so dass die Möglichkeit besteht, den Inhalt von einer Plattform direkt auf eine andere zu übertragen.

Bußgeldvorschriften

Um eine wirksame Durchsetzung der gesetzlichen Vorschriften zu ermöglichen, bedarf es darüber hinaus Bußgeldvorschriften. Zur Wahrung des Grundsatzes der Verhältnismäßigkeit sind diese als mildere Maßnahme im Vergleich zu anderen Aufsichtsmaßnahmen der zuständigen Behörde (wie z.B. Untersagung des Betriebes) erforderlich. Mit Bußgeld müssen insbesondere solche Verstöße belegt werden, die Auswirkungen auf die Sicherheit des Angebots haben können und denen (zivilrechtliche) Haftungsregeln für den Schadensfall nicht gerecht werden. Elementar für die Grundrechte des Nutzers ist die Verpflichtung des Anbieters, die vom Nutzer gelöschten Daten tatsächlich rückstandslos zu löschen und nicht etwa weitere Sicherungskopien vorzuhalten. Gleiches gilt für das Nichteinhalten der gesetzlich definierten Datenvorhaltepflicht nachdem die Einstellung des Dienstes angekündigt wurde. Da ein Verstoß gegen die gesetzlichen Vorschriften von unterschiedlicher Schwere und Bedeutung sein kann, sollte die Ermächtigung zur Auferlegung von Bußgeldern als Ermessensvorschrift ausgestaltet werden.

Einer ausdrücklich normierten Möglichkeit des Nutzers, die Einhaltung der rechtlichen Standards zu überprüfen, bedarf es indes nicht. Dies soll dem Nutzer durch die Einführung des Zertifizierungsverfahrens und der damit verbundenen Überprüfung seitens der zuständigen Stelle abgenommen werden. Damit sind den Anbietern freiwillige Maßnahmen, die zur Erhöhung der Transparenz interner Abläufe beitragen und dadurch das Kundenvertrauen steigern können, indes nicht verwehrt.

Zugriffsmöglichkeiten staatlicher Stellen

Elementare Voraussetzung für eine grundrechtskonforme Ausgestaltung des Rechtsrahmes eines virtuellen Speicherplatzes ist die Möglichkeit und der Umfang, in dem staatlichen Stellen die Befugnis eingeräumt wird, auf den Inhalt zuzugreifen. Der Gesetzgeber ist bei Erlass neuer Rechtsnormen zu einer abwägenden Gestaltung der infrage stehenden Rechtsgüter aufgerufen. Jedem Nutzer elektronischer Safes muss bewusst sein, dass es sich bei dem Safe nicht um ein absolut sicheres Versteck handelt, was jedem staatlichen Zugriff stets ausgeschlossen wäre. In engen, genau festgelegten Situationen kann es geboten sein, den staatlichen Ermittlungsbehörden Zugriff auf die im Safe gespeicherten Daten zu gewähren. Diese müssen jedoch technisch begrenzbar und beherrschbar sein. Aufgabe des Rechts ist es, dies sicherzustellen, so dass einfach-gesetzlich festgelegt ist, unter welchen Vorausset-

zungen ein Zugriff auf die Daten im Safe zulässig ist.[30] Es bedarf daher hinreichend normenklarer Regelungen hinsichtlich der Voraussetzungen des Zugriffs, der Datenverwendung, der Transparenz und des Rechtsschutzes, die sich an den insbesondere vom Bundesverfassungsgericht in mehreren Entscheidungen[31] herausgearbeiteten Grundsätzen zu orientieren haben. Dabei ist insbesondere beachtlich, dass der Zugriff auf die Daten durch die Inanspruchnahme der Safeanbieter einen Grundrechtseingriff in das Fernmeldegeheimnis des Safeeigentümers darstellen kann[32]. So könnten die Ermittlungsbehörden bspw. eine Sicherstellung und ggf. Beschlagnahme der betreffenden Daten nach den §§ 94 ff. StPO anordnen. Dieses Vorgehen erfolgt heutzutage bereits bei lokalen Festplatten, bspw. im Rahmen einer Hausdurchsuchung. Beachtet werden muss in diesem Zusammenhang unterdessen, dass die beschlagnahmten Daten für die Ermittlungsbehörden nur für den Fall Wert haben werden, wenn sie nicht verschlüsselt sind. Aufgrund des hier beschriebenen Modells des Safes, bei dem auch dem Safeanbieter das Auslesen der Daten nicht möglich ist, wird auch den Ermittlern eine Entschlüsselung in realistischen Zeiträumen nicht gelingen.[33] In diesem Fall müssten die Behörden wissen, welche Verschlüsselungsmethoden angewendet wurden und über die entsprechenden Zugangscodes verfügen. Wird das Passwort vom Beschuldigten nicht freiwillig herausgegeben, besteht aufgrund des Verbots der Selbstbelastung keine rechtliche Möglichkeit den Täter zur Herausgabe zu verpflichten. Daher können die Ermittlungsbehörden nur versuchen, mit einer Durchsuchung oder Beschlagnahme oder über strafprozessuale Mitwirkungspflichten, z.B. Zeugenaussage oder Herausgabeverlangen des § 95 StPO gegenüber unbeteiligten Dritten an den geheimen Schlüssel zu gelangen.[34] Anderenfalls wird es den Ermittlungsbehörden kaum möglich sein, sichergestellte Informationen auszuwerten.

Sollten Zugriffe des Safeanbieters auf die gespeicherten Daten jedoch nicht vollständig ausgeschlossen sein, erscheint es vorzugswürdig die staatlichen Zugriffsrechte abschließend, normklar und bereichsspezifisch zu normieren, da ansonsten das allgemeine Regime des Strafverfolgungs- und Gefahrenabwehrrechts zur Anwendung gelangt, welches weit weniger geeignet ist, das besondere Schutzniveau elektronischer Safes abzubilden.

---

30 So allgemein bereits *Gusy*, DuD 2009, 33 (35).

31 Zu denken ist hier insbesondere an die Entscheidungen bzgl. Möglichkeit der Beschlagnahme von Daten beim Betreiber, der Online-Durchsuchung sowie der Vorratsdatenspeicherung.

32 Zu Ermittlungen im Internet *Sönke E. Schulz/Christian Hoffmann*, Grundrechtsrelevanz staatlicher Beobachtungen im Internet – Internet-Streifen der Ermittlungsbehörden und das Autorisierungskonzept des BVerfG“, CR 2010, S. 131-136.

33 Vgl. zur Problematik der Verschlüsselung im Rahmen der Strafverfolgung: *Rux*, JZ 2007, 285 (286); *Buermeyer*, HRRS 2007, 154 (159); *Fox*, DuD 2007, 827 (828); *Bär*, in: Wabnitz/Janovsky (Hrsg.), Handbuch Wirtschafts- u. Steuerstrafrechts, 3. Aufl. 2007, Rn. 110; *Gercke*, CR 2007, 245 (247).

34 *Bär*, in: Wabnitz/Janovsky (Hrsg.), Handbuch Wirtschafts- u. Steuerstrafrecht, 25. Kap., Rn. 50, 113.

Auskunftspflichten

Denkbar ist auch ein Auskunftsanspruch für Dritte zur Verfolgung von Rechtsansprüchen. Danach wäre der Safeanbieter bspw. verpflichtet, dem Dritten Auskunft über Namen und Anschrift des Eigentümers zu erteilen, wenn der Dritte glaubhaft darlegt, dass er die Auskunft zur Verfolgung eines Rechtsanspruches gegen den Eigentümer braucht und das Verlangen nicht offensichtlich rechtsmissbräuchlich ist. Vor allem wenn der pseudonyme Einsatz des Safes zur Kommunikation mit Dritten ermöglicht wird, kommt einer solchen Auskunft entscheidende Bedeutung zu.

Zu bezweifeln ist aber, ob bspw. der in § 16 De-Mail-Gesetz ursprünglich vorgesehene sehr weitgehende Auskunftsanspruch grundrechtlichen Anforderungen gerecht wird. Erforderlich ist es vielmehr, detaillierte Voraussetzungen in eine entsprechende Norm aufzunehmen, wozu v.a. gehört, wer einen derartigen Auskunftsanspruch geltend machen kann. Während bspw. gem. § 14 Abs. 2 SigG die Identität eines Signatur-Schlüssel-Inhabers lediglich zuständigen Stellen unter bestimmten Voraussetzungen sowie Gerichten auf Anordnung im Rahmen anhängiger Verfahren übermittelt werden darf, ist im De-Mail-Gesetz generell von „Dritten“, die einen Rechtsanspruch geltend machen, die Rede. Eine Regelung zu Auskunftsrechten bedarf daher in der Weise einer Einschränkung, dass die anfragenden Stellen eingegrenzt werden und detailliert festgelegt wird, unter welchen Voraussetzungen ein Auskunftsanspruch zulässig ist.[35] Zudem ist der Betroffene über die Aufdeckung so früh wie möglich zu informieren.[36] Anleihen können hier an § 14 Abs. 2 SigG oder § 14 Abs. 2 TMG genommen werden. Schließlich ist auch die geringe Schutzbedürftigkeit Dritter, die sich auf eine anonyme oder pseudonyme Kommunikation eingelassen haben, zu berücksichtigen.

Schwierig zu regeln ist in jedem Fall die Prüftiefe des Safeanbieters. Als Ausgleich sind in jedem Fall Dokumentations- und Benachrichtigungspflichten gegenüber dem Safeeigentümer vorzusehen. Hinsichtlich der Schwelle für derartige Zugriffe ist zudem zu berücksichtigen, dass es keinen Unterschied macht, ob der Grundrechtseingriff aufgrund eines staatlichen Auskunftsverlangens oder aufgrund eines Auskunftsverlangens eines Privaten ergeht. In jedem Fall ist das Grundrecht auf informationelle Selbstbestimmung betroffen, in das nur unter qualifizierten Voraussetzungen eingegriffen werden darf.

---

[35] So muss bspw. festgelegt sein, was unter einem „Rechtsanspruch“ i.S.d. Norm zu verstehen ist.

[36] Auf eine derartige Informationspflicht des Anbieters wurde verzichtet, da sie ihm angeblich Aufgaben auferlegen würde, „zu deren Bewältigung er nicht sachgemäß gerüstet wäre“, BT-Drs. 16/12598, S. 22.

Sonstige Inhalte

Schließlich ist dem Diensteanbieter die Pflicht aufzuerlegen, den Nutzer über die mit der Nutzung des Safes verbundenen Sicherheitsrisiken zu informieren. Dazu zählen insbesondere Informationen zu Maßnahmen, die notwendig sind, um einen unbefugten Zugriff auf den Safe zu verhindern (wie z.B. das sichere Anmelden, Verschlüsselung, etc.) und den Verlust der Zugangsmechanismen zu vermeiden. Demgegenüber erscheint eine über einen Mindeststandard und die zur Vertraulichkeit erforderlichen technischen und organisatorischen Maßnahmen hinausgehende gesetzliche Regelung, bspw. von Diensten („Apps“) weder grundrechtlich gefordert, noch sachgerecht.

Kompetenzfragen

Was die Gesetzgebungskompetenz für eine Ausgestaltung der rechtlichen Rahmenbedingungen elektronischer Safes anbelangt, könnte als Kompetenztitel für den Bund auf die konkurrierende Gesetzgebungskompetenz des Art. 74 Abs. 1 Nr. 11 GG (Recht der Wirtschaft) abgestellt werden. Das Recht der Wirtschaft wird von der Rechtsprechung sehr weit als alle Normen, die das wirtschaftliche Leben und die wirtschaftliche Betätigung regeln, definiert.[37] Von den einzelnen in der Klammer aufgeführten Wirtschaftszweigen kommt das „Gewerbe“ in Betracht. Darunter versteht man die selbstständige, nicht verbotene, auf Erwerb gerichtete Tätigkeit mit Ausnahme der Urproduktion und der höheren Berufsarten.[38] Darunter wird auch die Tätigkeit von Safeanbietern fallen, die eine Infrastruktur zur Ablage von Dokumenten im Internet zur Verfügung stellen.

Gem. Art. 72 Abs. 2 GG hat der Bund auf dem Gebiet des Art. 74 Abs. 1 Nr. 11 GG jedoch nur dann die Gesetzgebungskompetenz, wenn und soweit die Herstellung gleichwertiger Lebensverhältnisse im Bundesgebiet oder die Wahrung der Rechts- oder Wirtschaftseinheit im gesamtstaatlichen Interesse eine bundesgesetzliche Regelung erforderlich macht. Es wird sich in Bezug auf eine Safeinfrastruktur begründen lassen, dass bundeseinheitliche Regelungen zur Wahrung der Rechtseinheit im gesamtstaatlichen Interesse liegen, da ansonsten eine Rechtszersplitterung mit problematischen Folgen droht, „die im Interesse sowohl des Bundes als auch der Länder nicht hingenommen werden kann“.[39]

Auch wird sich eine bundesgesetzliche Regelung zur Wahrung der Wirtschaftseinheit im gesamtstaatlichen Interesse begründen lassen. Normen des Landesgesetzgebers werden hier regelmäßig zu Nachteilen für die Gesamt-

---

37 BVerfGE 55, 274 (308); 68, 319 (330); 116, 202 (215 f.).

38 *Pieroth*, in: Jarass/Pieroth, Art. 74, Rn. 23.

39 So die Anforderungen des BVerfG in BVerfGE 106, 62 (145).

wirtschaft führen.[40] Insbesondere ist zu befürchten, dass unterschiedliche landesrechtliche Behandlungen, z.B. unterschiedliche Anforderungen an die Zertifizierung von Anbietern, Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten. Die Benutzung der Datensafes zeichnet sich vor allem durch einen ortsunabhängigen und damit länderüberschreitenden Bezug aus. Auch die Anknüpfung von Rechtsfolgen an die Vorabprüfung des Dienstes verlangt schließlich einheitliche Rahmenbedingungen. Damit ist der Bund für ein derartiges Gesetzesvorhaben zuständig. Es bedarf nicht der Zustimmung des Bundesrates.

Um aus technischer Sicht notwendige Änderungen möglichst schnell umsetzen zu können, ohne stets ein aufwändiges Gesetzgebungsverfahren durchlaufen zu müssen, sollte zudem die Möglichkeit zum Erlass einer Rechtsverordnung nach Art. 80 Abs. 1 S. 1 GG berücksichtigt werden. Dabei müssen gem. Art. 80 Abs. 1 S. 2 GG jedoch Inhalt, Zweck und Ausmaß der erteilten Ermächtigung im Gesetz bestimmt werden (Bestimmtheitsgrundsatz). Das Bundesverfassungsgericht trennt nicht immer scharf zwischen Inhalt, Zweck und Ausmaß, sondern hat zu deren Auslegung verschiedene Formeln entwickelt.[41] So fehle die nötige Beschränkung jedenfalls dann, wenn die Ermächtigung so unbestimmt ist, dass nicht mehr vorausgesehen werden kann, in welchen Fällen von der Ermächtigung Gebrauch gemacht wird und welchen Inhalt die Verordnung haben wird. Zumindest die grundsätzlichen technischen und organisatorischen Anforderungen bzgl. des Sicherheitsniveaus, der Vertraulichkeit oder des Speicherortes der Daten müssen daher in das Gesetz selbst aufgenommen werden.

5.3 Rechtliche Betrachtung anhand eines Lebenszyklus

Nachfolgend sollen anhand eines Lebenszyklus rechtliche Aspekte der Nutzung elektronischer Daten- und Dokumentensafes skizziert werden. Ziel dieser stichwortartigen Übersicht ist es dabei vor allem, diejenigen Fragen zu identifizieren, die einer eingehenden Untersuchung bedürfen und deren juristisch korrekte Beantwortung den Rahmen dieser Untersuchung sprengen würde.[42] Der Schwerpunkt der Überlegungen ist dabei der Einsatz im E-Government – bspw. in staatlichen Antragsverfahren; zivilrechtliche Fragestellungen (insbesondere zu den Nutzungsbedingungen etc.) werden nur einbezogen, soweit diese auch Relevanz für die elektronische Behördenkommunikation besitzen. Weitgehend ausgeblendet bleiben datenschutzrechtliche Aspekte, zumal keine Besonderheiten sowohl bei der Datenverarbeitung durch

---

40 So die Anforderungen des BVerfG in BVerfGE 106, 62 (147); 112, 226 (249).

41 Dazu bspw. *Mann*, in: Sachs, GG, Art. 80, Rn. 27; *Pieroth*, in: Jarass/Pieroth, Art. 80, Rn. 11.

42 So dass an dieser Stelle auf die ausführliche Betrachtung der Rechtsfragen in Schliesky (Hrsg.), Rechtsfragen des Identitätsmanagements, i.E. verwiesen sei.

den Safeanbieter als auch durch die Behörde beim Einsatz im E-Government bestehen, die nicht unter Rückgriff auf bestehende Angebote bzw. das geltende BDSG-Regime gelöst werden könnten. Hinsichtlich der Besonderheiten oder einer etwaigen Regulierungsgesetzgebung kann daher auf die Ausführungen im Abschnitt 5.2 verwiesen werden.

Hinsichtlich der behandelten Fragestellungen wird analysiert, ob diese (weitgehend) unter Rückgriff auf bestehende Strukturen und Angebote (Webhosting-Verträge, E-Mail-Postfächer, Online-Festplatten o.ä.) zu lösen sind, oder ob es sich um Neuerungen handelt, die eine neue, andere rechtliche Beurteilung erfordern. Der Lebenszyklus elektronischer Safes wird dabei in acht grobe Phasen bzw. Einsatzmöglichkeiten und Funktionalitäten unterteilt, denen sich die rechtlich relevanten Aspekte grob zuordnen lassen:

- Vorvertragliche Phase
- Eröffnung eines Safes durch einen Safeeigentümer
- Leistungsstörungen
- Hochladen von Daten und Dokumenten in den elektronischen Safe
- Einstellen von Dokumenten durch Safenutzer in den Posteingangsbereich des Safes
- Freigabe von Dokumenten im Safe an Safenutzer
- Besonderheiten bei der Kommunikation mit / von Anwälten, Notaren und Gerichten
- Beendigung des Vertragsverhältnisses

Als wesentliche Funktionen und Neuerungen gegenüber bestehenden Systemen und Angeboten sind das Einstellen von Dokumenten durch Safenutzer in den Freigabebereich sowie die Freigabe von Daten und Dokumenten zu nennen. Nachfolgend werden Safeeigentümer (natürliche oder juristische Person, die mit dem Safeanbieter ein Vertragsverhältnis eingeht und die primäre Verfügungsgewalt über die gespeicherten Daten und Dokumente besitzt), andere (dritte) Safenutzer (die nach einer Freigabe, freigegebene Daten und Dokumente aus dem Safe beziehen) und der Safeanbieter unterschieden.

Vorvertragliche Phase (Werbung/Kommunikation/Vertragsanbahnung)		
	Rechtliche Aspekte	**Anmerkungen**
1) **Geschäftsmodell** (unentgeltliches Angebot wie Webmail?, Entgeltzahlung durch den Safeeigentümer oder insbesondere im Behördenkontakt durch den Safenutzer)	• Grundsätzlich keine rechtlichen Vorgaben / Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten) • De-Mail-Gesetz enthält keine Vorentscheidung; gesetzliche Vorgaben sind nicht erforderlich • auch die Unentgeltlichkeit von Angeboten entbindet nicht von den besonderen Vorgaben, wenn das Akkreditierungsverfahren durchlaufen werden soll	• die Wahl des Geschäftsmodells hat ggf. Auswirkungen auf den Einsatz im E-Government bzw. die Ausgestaltung der Safe-Nutzung in diesem Kontext (kann der Safenutzer Zustellung der Verwaltung in den Safe verlangen, wenn diese dafür „E-Porto“ zahlen muss?)
2) Werbung durch den Safeanbieter	• Grundsätzlich keine rechtlichen Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten) • Sollte eine Akkreditierung geschaffen werden, ist ausschließlich diesen Safeanbietern ein Verweis auf diese besondere Eigenschaft gestattet	
3) Vertragsanbahnung	• Grundsätzlich keine rechtlichen Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten)	
4) **Vorvertragliche Pflichten**	• Grundsätzlich keine rechtlichen Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten)	
5) Verträge mit Dritten (Sicherstellung der Leistungsfähigkeit)	• Grundsätzlich keine rechtlichen Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten) • Aber: ggf. sind bei der Einschaltung Dritter (bspw. zum Zukauf externer Speicherkapazitäten) datenschutzrechtliche Besonderheiten (vor allem beim perspektivischen Ausbau zum weltweiten Cloud Computing) zu beachten	• Rechtsfragen des Cloud Computing (und des Einsatzes im E-Government) bedürfen einer gesonderten Betrachtung (Datenschutzrecht, Organisation etc.[43])

[43] S. dazu *Schulz*, VM 2010, 36 ff.; *ders.*, MMR 2010, 75 ff.

Eröffnung eines elektronischen Safes durch den Safeeigentümer		
	Rechtliche Aspekte	**Anmerkungen**
1) Vertragsschluss	• Grundsätzlich keine rechtlichen Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten)	• Vertragstyp abhängig vom gewählten Geschäftsmodell (insbesondere Unterschiede bei Unentgeltlichkeit für den Safeeigentümer) • es handelt sich um einen typengemischten Vertrag (miet-, dienst- und werkvertragliche Elemente)
2) Formerfordernisse	• Grundsätzlich ist der Abschluss eines „Safe-Vertrages“ formfrei (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten)	
3) Authentisierung	• De-Mail-Gesetz schreibt eine sichere Erstregistrierung vor (bspw. durch E-Personalausweis)	• auch bei „isolierten“ Datensafes empfiehlt sich eine sichere Erstregistrierung um eine erhöhte Beweiskraft sicherzustellen
4) Einbeziehung allgemeiner Geschäftsbedingungen	• Grundsätzlich keine rechtlichen Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten) • Wichtig: genaue Beschreibung der Vertragspflichten (insb. für **Protokoll-, Bestätigungs- und Freigabefunktionen**, um Beweiskraft sicherzustellen, Gebührenmodelle und die **Abbildung unterschiedlicher Sicherheits- und Authentisierungsniveaus**)	• hinsichtlich der Protokollfunktionen etc. und den Authentisierungsniveaus empfiehlt sich auch bei „isolierten“ Safes (s.o.) eine Orientierung an den Vorgaben des De-Mail-Gesetzes • in jedem Fall ist ein Widerspruch zwischen AGB / Service Level Agreements zu gesetzlichen Vorgaben zu vermeiden • gesetzliche Vorgaben zu Datenschutz, Datenverfügbarkeit und Datensicherheit sind nicht disponibel
5) Aushändigung von Software	• Grundsätzlich keine rechtlichen Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: i.d.R. Kaufvertrag über Gegenstand und/oder Nutzungsrecht)	• da nur eine clientbasierte Verwaltung des Safe-Inhaltes die erforderliche Sicherheit gewährleistet, ist diese grds. erforderlich

Leistungsstörungen		
	Rechtliche Aspekte	**Anmerkungen**
	• Grundsätzlich keine rechtlichen Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten) • aber: wird der Safe zur Kommunikation mit staatlichen Stellen eingesetzt, können sich Leistungsstörungen ggf. auch nachteilig auf das Verwaltungsverfahren auswirken	• abhängig vom Vertragstyp bzw. dem betroffenen Element (denkbare Leistungsstörungen sind bspw. Nichterreichbarkeit des Safes, Verlust oder Missbrauch der Daten im Safe, Nichtzustellung von Freigaben, Fehler beim Einstellen von Dokumenten, Fehler bei der Protokollfunktion)

Hochladen von Dokumenten durch den Safeeigentümer		
	Rechtliche Aspekte	**Anmerkungen**
1) Authentisierung	• Grundsätzlich keine rechtlichen Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten) • aber: De-Mail-Gesetz sieht verschiedene Anmeldeniveaus vor, in deren Abhängigkeit die Funktionalitäten stehen	• auch bei „isolierten“ Safes sollte bei jedem Anmelde- und Hochladevorgang eine Authentisierung verlangt werden (ggf. unterschiedliche Niveaus und Kennzeichnung der Dateien, mit welchem Niveau zugefügt) • clientbasierter Safe bildet das erforderliche Sicherheitsniveau ab
2) Dateiformate / Standards	• Grundsätzlich keine rechtlichen Vorgaben / Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten)	• im Verhältnis zum Staat bestehen ggf. Vorgaben zu Austauschformaten • Probleme können hinsichtlich des Zugangs / der Zustellung (s.u.) entstehen, wenn Verwaltung oder Bürger Dateien nicht öffnen können (weil i.d.R. Protokolle nur bescheinigen können, dass eine bestimmte Datei übermittelt wurde, nicht deren Inhalt und schon gar nicht, ob diese vom Gegenüber zu lesen war)
3) Digitale Signatur	• Grundsätzlich keine rechtlichen Vorgaben / Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten)	• es besteht grundsätzlich keine Notwendigkeit, Dateien im Safe zu signieren • beim Einsatz im E-Government muss Dokument vor Übermittlung an den Staat (bei Schriftformerfordernis) digital signiert werden • derartige Funktionen können integraler Bestandteil des Safes

		sein oder über „Apps“ integriert werden
4) Verschlüsselung	• Grundsätzlich keine rechtlichen Vorgaben / Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten)	• client- oder providerseitige Verschlüsselungen sind denkbar und rechtlich unproblematisch; relevant nur für die Freigabefunktion an Safenutzer • die Safeanbieter sollten verpflichtet werden, clientbasierte Safes und damit eine Verschlüsselung auf dem lokalen System anzubieten
5) Digitalisierung „analoger“ Dokumente	• könnte perspektivisch als sog. „Integrationsdienst“ eingebunden werden	• vor allem bei Nutzung der Safes durch Behörden oder Anwälte ist zu klären, welche Beweiskraft eingescannten Dokumenten zukommt
6) Schnittstellen zu E-Mail- und De-Mail-Postfächern		• Sicherzustellen ist, dass ein Transfer von Dateien und Dokumenten aus E-Mail- und De-Mail-Postfächern in den Safe möglich ist

Einstellen von Dokumenten durch Dritte/Safenutzer in den Posteingangsbereich des Safes		
	Rechtliche Aspekte	**Anmerkungen**
1) Verhältnis zu E-Mail-Postfächern	• es stellt sich vor allem die Frage nach dem Verhältnis zum De-Safe nach dem Bürgerportal-Gesetz • es soll ein „direkter“ Zugriff in Form von Einstellen von Dokumenten ermöglicht werden (s.o.)	• Mehrwert des direkten Zugriffs auf fremde Safes ist, dass der „Umweg“ über ein unsicheres E-Mail bzw. De-Mail-Postfach vermieden wird (s.o.)
2) Kennzeichnung der Safes /Adressen/ Verzeichnisse		• Insbesondere im Kontext von Verwaltungsverfahren (Zugangseröffnung s.u.) ist zu klären, wie sichergestellt wird, dass alle Behörden von generellen Freigaben und von der Existenz elektronischer Safes Kenntnis haben
3) Authentisierung	• ein Einstellen durch den Safenutzer darf nur möglich sein, wenn er die gleichen Anforderungen erfüllt und so die Vertraulichkeit der Safe-Infrastruktur nicht beeinträchtigt	• Sichere Authentisierung, wenn der Dritte Unternehmen / Behörde ist (und daher kein E-Personalausweis zur Verfügung steht) • Abhilfe könnte De-Mail Adresse schaffen (Zustellung Freigabe-Link an De-Mail mit hohem Authentisierungsniveau stellt sicher, dass der

		Einstellende berechtigt ist), problematisch bleiben „isolierte“ Safes
4) Vertragsverhältnis zum Safenutzer	• Abhängig vom gewählten Geschäftsmodell	• zahlt der Safenutzer für die „Zustellung“ in den Safe ein Entgelt (E-Porto), entsteht hier ein Vertragsverhältnis (Vergleich mit der herkömmlichen Post!) • dies wirkt sich ggf. auf ein „Recht zur elektronischen Kommunikation“ (bspw. aus der EU-DLR) und auf die Verwaltungsgebühren und -auslagen aus
5) Benachrichtigung (Eingang Dokument im Safe)	• muss automatisch versendet werden • über verschiedene Apps erscheint es denkbar, diese nicht nur an den Safeclient, sondern auch per E-Mail, SMS o.ä. zu versenden	• Beweiskraft derartiger Zugangsbestätigungen zweifelhaft • Bürgerportal-Gesetz schafft Abhilfe, allerdings nur beim „Umweg“ über den Postfach- und Versanddienst; Regelungen zum Safe fehlen
6) Zugangseröffnung	• In Anlehnung an die Rechtsprechung zum Einsatz von E-Mails im E-Government ist zu klären, ob und wann ein Bürger durch Nutzung eines Safes sein Einverständnis zu diesem Weg der Kommunikation gegeben hat	• Klärungsbedarf, da die Vergleichbarkeit von E-Mail- und Safe-Kommunikation nicht zwingend gegeben ist • Vor allem sind derzeit Änderungen des Verwaltungszustellungsgesetzes nur für die De-Mail, nicht elektronische Safes vorgesehen
7) Zugang	• Zu klären ist, wann ein Dokument nach der Ablage im Safe zugegangen ist und damit Rechtswirksamkeit entfalten kann	• Klärungsbedarf, da die Vergleichbarkeit von E-Mail- und Safe-Kommunikation nicht zwingend gegeben ist
8) Beweiskraft	• Zu klären ist, ob und inwieweit den automatisch versendeten Bestätigungen Beweiskraft für den Zugang zukommen kann.	• Die Beweiskraft ist insbesondere fraglich, wenn „isolierte“ Safes realisiert werden, für die die gesetzliche Regelung des De-Mail-Gesetzes keine Vorgaben enthält
9) Förmliche Zustellungen /Einschreiben	• Zu klären ist, ob Safe-Systeme in Anlehnung an die Funktionalitäten des Postfach- und Versanddienstes der Bürgerportale auch besondere Zustellformen abbilden sollen • In Anlehnung an die herkömmliche Post können solche freiwillig angeboten werden • Förmliche Zustellungen nach den Zustellungsgesetzen sind nur bei gesetzlicher Beleihung möglich	• Eine Beleihung ist nach dem De-Mail-Gesetz zwar vorgesehen, der Regelungssystematik kann aber nicht entnommen werden, ob diese ganz allgemein für die Anbieter gilt oder nur für bestimmte Dienste (den Postfach-und Versanddienst)

10) Zustellungsrecht	• Verwaltungszustellungsgesetz und Auswirkungen der beabsichtigten Änderungen durch das De-Mail-Gesetz	• Es ist zu klären, ob eine „Zustellung“ in Safes nach der derzeitigen Rechtslage überhaupt zulässig ist und wie sich der Erlass des De-Mail-Gesetzes auf diese auswirkt (besteht eine überschießende Exklusivität, so dass nur noch die vom De-Mail-Gesetz vorgesehenen Zustellungen zulässig sind?)

Freigabe von Dokumenten im Safe an Safenutzer		
	Rechtliche Aspekte	**Anmerkungen**
1) Digitales Rechte-Management	• Ein digitales Rechte-Management lässt sich ohne rechtliche Besonderheiten realisieren • Problematisch sind die Interoperabilität und die verwendeten Standards beim Einsatz zum E-Government; aber: gewisse Parallelen zum Einsatz von E-Mails • Digitales Rechte-Management muss die Möglichkeiten der herkömmlichen Kommunikation abbilden (Bsp.: nicht jedes Dokument muss ausgehändigt werden, also auch nicht im elektronischen Verkehr, Einsicht reicht u.U. aus)	• anhand einzelner Verfahren ist zu klären, welche konkrete „Art“ der Freigabe notwendig ist und wie diese elektronisch abgebildet werden kann (bspw. nur Lesen, auch Speichern zur Dokumentation, Referenz auf die Daten im Safe)
2) Freigabeanforderungen	• Beim Einsatz im E-Government muss sichergestellt werden, dass bei automatisierten Verfahren immer konkrete Freigabeanforderungen an den Safe gesendet und vom Safeeigentümer bestätigt werden (Zweckbindung und Datensparsamkeit)	
3) Versand von Benachrichtigungen	• Die Beweiskraft von Benachrichtigungen über Freigaben muss vor allem bei isolierten Safes geklärt werden	• Klärungsbedarf besteht insbesondere, wenn die Vorlage / Aushändigung von Dokumenten an die Behörde rechtliche Folgen auslöst (Fristen oder Vollständigkeit von Unterlagen)
4) Zugangseröffnung / Zugang / Beweiskraft	• In Anlehnung an die E-Mail-Kommunikation ist zu klären, wann die Behörde diesen Zugangskanal eröffnet hat , welche Modalitäten gelten und vor allem, wann und ob Zugang bei der Behörde gegeben ist	• Klärungsbedarf, da die Vergleichbarkeit von E-Mail- und Safe-Kommunikation nicht zwingend gegeben ist • Insbesondere, wenn die Etablierung übergreifender Prozessketten beabsichtigt ist, besteht rechtlicher An-

		passungsbedarf (zumindest fachbezogen denkbar)
5) Recht auf „Safe-Kommunikation“	• Fraglich ist, ob bei rechtlichen E-Government-Verpflichtungen diese auch zugleich eine Safe-Kommunikation einbeziehen	
6) Ersetzen der Unterschrift durch elektronischen Identitätsnachweis	• Fraglich ist, ob das Erfordernis der Unterschrift auf einem Antrag etc. durch ein Dokument, welches unter Nutzung des elektronischen Identitätsnachweises des E-Personalausweis übermittelt wird, ersetzt werden kann	• Auch im Anwendungsbereich des De-Mail-Gesetzes (Postfach- und Versanddienst) noch nicht geklärt
7) Authentisierung	• Auf Seiten des Safeeigentümers bieten sich unterschiedliche Sicherheitsniveaus an, die der Behörde auch übermittelt werden, damit sie entscheiden kann, ob sie freigegebenen Dokumenten vertraut • Auf Seiten der Behörde stellt sich das Problem der Authentisierung in gleicher Weise, wie beim Einstellen in den Safe (s.o.)	• Es ist sicherzustellen, dass nur der zuständigen Behörde, ggf. nur einem bestimmten Behördenteil die Freigabe erteilt wird und sich diese sicher authentisiert

Besonderheiten bei der Kommunikation mit / von Anwälten, Notaren und Gerichten		
	Rechtliche Aspekte	**Anmerkungen**
1) Anwälte/ Notare	• Zu klären ist, ob eine Nutzung der Safes durch Anwälte oder Notare besondere Sicherheitsmechanismen oder Funktionalitäten benötigt • Ggf. sind Schnittstellen zu den besonderen Kommunikationsformen des elektronischen Handelsregisters oder Grundbuchs vorzusehen	
2) Verwaltung	• In Betracht kommt auch, dass Behörden selbst als Safeeigentümer auftreten, in die dann seitens der Bürger Dokumente eingestellt werden können (zu den Problemen s.o.)	• Inwieweit ein solcher Einsatz sachgerecht und rechtlich zulässig ist, muss gesondert geprüft werden
3) Gerichte	• Aufgrund der Besonderheiten des gerichtlichen Verfahrens bestehen Einschränkungen beim Einsatz elektronischer Kommunikation • Um auch hier eine Akzeptanz zu erreichen, muss auf die Interoperabilität mit eingesetzten Systemen (bspw. EGVP) geachtet werden • Perspektivisch sollte man aber über die Zustellung von Gerichtspost in Safes (evtl. nur solcher von Anwälten) nachdenken	

Beendigung des Vertragsverhältnisses		
	Rechtliche Aspekte	**Anmerkungen**
1) nachvertragliche Pflichten	• Grundsätzlich keine rechtlichen Vorgaben / Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten) • Aufgrund der Bedeutung der Safe-Dokumente müssen allgemeine Geschäftsbedingungen aber Regelungen zur Speicherung nach Vertragsbeendigung enthalten, die beiden Seiten gerecht werden	• Das De-Mail-Gesetz enthält auch für Safe-Inhalte eine entsprechende Regelung; das Verhältnis zu allgemeinen Geschäftsbedingungen müsste geklärt werden
2) Vererblichkeit von Safe-Inhalten	• Grundsätzlich keine rechtlichen Vorgaben / Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten) • Allerdings bisher auch bei E-Mail-Postfächern etc. kaum geklärt; Probleme liegen eher im faktischen Bereich (Nachweis etc.)	
3) Umzug des Safe-Inhaltes auf Wunsch des Safe-eigentümers	• Grundsätzlich keine rechtlichen Vorgaben / Besonderheiten im Vergleich zu bestehenden Angeboten (**Vergleichbarkeit**: E-Mail-Postfächer; Online-Festplatten) • Vertragliche Regelungen müssen aber einen „einfachen“ Transfer zu einem anderen Safe ermöglichen • In Anlehnung an die herkömmliche Post wäre über die technische (und vertragliche) Abbildung von „Nachsendeanträgen“ etc. nachzudenken	
4) Insolvenz o.ä. des Safeanbieters	• Wie bei digitalen Signaturen und im De-Mail-Gesetz wäre eine Pflicht zur Übernahme durch andere Anbieter wünschenswert	• Gesetzliche Regelung fehlt bisher, wenn isolierte Safes betrieben werden

Als Zwischenfazit der rechtlichen Prüfung kann festgehalten werden, dass sich ein großer Teil der Rechtsfragen im Rahmen des Lebenszyklus eines elektronischen Safes für Daten und Dokumente unter Rückgriff auf die Regelungen und die Rechtsprechung zu bereits bestehenden Angeboten bewältigen lässt. Einer genaueren Analyse bedurften insbesondere:

- Safe-Einsatz im E-Government, wenn gesetzliche Regelungen fehlen (Akzeptanz und Verbreitung lässt sich nur bei Verbindlichkeit der Safe-Kommunikation erreichen)
- Verhältnis von „isolierten" Safes zum De-Mail-Konzept (bzw. bei dessen fehlender Realisierung grundsätzlich die Frage, wie Verbindlichkeit im Kontext von Behördenkommunikation gewährleistet werden kann)
- Rechtsfragen der neuartigen Funktionen (Freigabe und Einstellen von Daten und Dokumenten), da die Vergleichbarkeit zur E-Mail hier fraglich ist (u.a. Zugangseröffnung, Zugang und Beweiskraft)

Weitere Rechtsfragen sollten im Kontext einer regulierenden Gesetzgebung geregelt werden. Insoweit könnte sich der Rechtsrahmen für elektronische Safes weitestgehend an die Vorgaben des De-Mail-Gesetzes zum Postfach- und Versanddienst anlehnen, wäre jedoch auch um safespezifische Aspekte zu ergänzen. Diese vollständig dem Verordnungsgeber zu überlassen, erscheint der grundrechtlichen Relevanz der Safes nicht gerecht zu werden.

Weitergehender Regelungsbedarf, der nicht in einem De-Mail-Gesetz oder einem Rechtsrahmen für Safes und Safeanbieter zu verorten ist, entstammt dem Komplex „Zustellung, Zugangseröffnung und Nachweisbarkeit". Denkbar wäre es, diesen in einem E-Government-Gesetz (des Bundes[44]), einer Fortentwicklung des Verwaltungsverfahrensgesetzes oder Verwaltungszustellungsgesetzes aufzugreifen. Dabei ist eine Begrenzung auf bestimmte Infrastrukturen und Dienste (bspw. Postfach- und Versanddienst i.S.d. De-Mail-Gesetzes) zu vermeiden, sondern eine Lösung zu realisieren, die auch zukünftige Entwicklungen (bspw. auch i.S.d. M-Government) hinreichend berücksichtigt.

[44] Zur Landesebene *Sönke E. Schulz*, Können E-Government-Gesetze den IT-Einsatz erfassen?, eGovernment Review Nr. 5 (2010), S. 22 f.; *ders*., Macht Art. 91c Grundgesetz E-Government-Gesetze der Länder erforderlich?", in: DÖV 2010, S. 225-229; *ders*., Ein eGovernment-Gesetz für Schleswig-Holstein – Angriff auf die kommunale Selbstverwaltung?, Die Gemeinde SH 2008, S. 272-278.

6. Elektronische Safe-Dienste am Beispiel potentieller Anwendergruppen

Im folgenden Kapitel wird anhand von drei verschiedenen Szenarien aufgezeigt, wie elektronische Safes und damit verbundene Dienste in unterschiedlichen Zusammenhängen eingesetzt werden können. Es wird die Verwendung von elektronischen Safes im Verlauf von Grundstückskäufen, der Bereitstellung von Unterlagen im Zuge einer Antragstellung über den Einheitlichen Ansprechpartner für Dienstleistungsunternehmen und bei der Erfüllung von Arbeitgebermeldepflichten beschrieben.

Abwicklung eines Grundstückskaufs mit Unterstützung von elektronischen Safe-Diensten

Der Kauf eines Grundstücks erfordert die Einbindung verschiedener Akteure und Unterlagen. Neben Käufer und Verkäufer des Grundstücks ist zumindest ein Notar involviert, ebenso wie finanzierende Banken und die jeweilige grundbuchführende Stelle der öffentlichen Verwaltung. Zur Abwicklung des Vorgangs werden von den einzelnen Parteien unterschiedliche Unterlagen eingebracht, bearbeitet und abgelegt. Ein Vertrag über den Kauf eines Grundstücks bedarf nach § 311b Abs. 1 BGB der Beurkundung durch einen Notar. Der Vorgang der Beurkundung eines Grundstückskaufs stellt sich im Allgemeinen wie folgt dar:

Zu Beginn nimmt der Notar Einsicht in das Grundbuch, um sich über den aktuellen Stand zu informieren und eine bessere Beratung durchführen zu können. Diese Einsicht ist Personen gestattet, die ein berechtigtes Interesse an der Einsicht haben, wozu auch Notare, welche im Auftrag handeln, zu zählen sind. Die Einsichtnahme ist nach §§ 133 n.F. GBO per elektronischem Datenabruf möglich.

Im Anschluss an die Verkaufsabwicklung muss der Käufer als neuer Eigentümer in das Grundbuch eingetragen werden. Hierzu wird ein entsprechender Antrag an das Grundbuchamt gestellt. Dieser Antrag muss von einem Notar gestellt werden. Dabei kann der Notar die Anträge der beteiligten Akteure an das Grundbuchamt weiterleiten oder im Auftrag der Beteiligten einen Antrag stellen.

Der Notar ist auch für die sogenannte Auflassungserklärung zuständig. Mit dieser Erklärung bestätigen Verkäufer und Käufer eines Grundstückes ihre Übereinkunft, das Grundstück zu übereignen. Die Auflassung erfolgt dabei in Anwesenheit des Notars. Dieser unternimmt in der Regel eine Beurkundung des Vorgangs. Für den Notar besteht nach § 18 des Grunderwerbssteuerge-

setzes ferner die Pflicht, der Finanzverwaltung Vorgänge anzuzeigen, in die Grundstücke involviert sind.

Mit dem „Gesetz zur Einführung des elektronischen Rechtsverkehrs und der elektronischen Akte im Grundbuchverfahren“ (ERVGBG)[45] ist ein rechtlicher Rahmen für die elektronische Abwicklung von Prozessen mit Bezug zum Grundbuch etabliert. Angestrebt wird mit dem Gesetz, dass zukünftig die Bestellung der Grundschuld zwischen den involvierten Institutionen und mit dem Grundbuchamt elektronisch abgewickelt wird. Ziel ist dabei ein möglichst medienbruchfreier Prozessablauf. Daten der Akteure werden zu Beginn digital erfasst und mit Hilfe eines vertrauenswürdigen Systems an den zu beauftragenden Notar übermittelt. Dieser erzeugt daraus die Grundschuldurkunde als Entwurfsversion. Hieraus erfolgt die papierbasierte Beurkundung der Grundschuld. Erfolgen im Laufe des Vorgangs der Beurkundung Aktualisierungen, so können diese über ein spezielles Programm in den zugehörigen Datensatz übertragen werden. Einmal fertiggestellt, kann der Notar ein digitales Abbild der Urkunde erzeugen. Die Beglaubigung dieser Version erfolgt mit Hilfe einer qualifizierten elektronischen Signatur nach § 39a Beurkundungsgesetz (BeurkG). Anschließend versendet der Notar die beglaubigte Abschrift inklusive generierter Strukturdaten und stellt den Antrag beim Grundbuchamt auf Eintrag des Vorgangs. Erhält der Notar vom Grundbuchamt eine Mitteilung darüber, dass der Vorgang im Grundbuch eingetragen wurde, so leitet er diese elektronisch weiter.

Für die Einbindung des elektronischen Safes in die digitale Abwicklung eines Grundstückskaufs bieten sich verschiedene Optionen an. Elektronische Safes stellen dabei eine Ergänzung vorhandener Systeme zur digitalen Langzeitarchivierung dar, da sie im Vergleich zu diesen stärker auf die sofortige Verfügbarkeit der in ihnen enthaltenen Daten ausgelegt sind. Gegenüber Systemen zum sicheren E-Mail-Versand weisen elektronische Safes in der zu Beginn definierten Ausprägung eine höhere Sicherheit und Vertraulichkeit der in ihnen gelagerten Daten auf.

Elektronische Safes können im Szenario des Grundstückskaufs zur Bereitstellung und dauerhaften Verfügbarmachung benötigter Unterlagen eingesetzt werden. Die Kernfunktionalität elektronischer Safes, die sichere Aufbewahrung von Daten, ermöglicht es den beteiligten Akteuren, sich gegenseitig die notwendigen Informationen auf digitalem Weg zuverlässig zur Verfügung zu stellen. Elektronische Grundbuchabfragen könnten um signierte strukturierte Informationen ergänzt und im elektronischen Safe des Notars hinterlegt werden. Aus diesem heraus gibt er die Daten für die weiteren Beteiligten des

[45] Bundesgesetzblatt (17.8.2009): Gesetz zur Einführung des elektronischen Rechtsverkehrs und der elektronischen Akte im Grundbuchverfahren. Version vom 11.8.2009. Abgerufen von: http://www.bmj.de/files/-/3907/Gesetz_elektr_Rechtsverkehr_Grundbuchverfahren_Bundesgesetzblatt.pdf.

Grundstückskaufs zur Übernahme frei oder stellt sie direkt in deren Safes ein. Einmal in strukturierter Form vorliegend, können die Grundbuchdaten so dann einfach in weitere Verfahren übernommen werden. Die Beurkundung des Grundstückskaufs durch den Notar muss auch in Zukunft weiter in Anwesenheit aller Beteiligten erfolgen. Neben dem Papieroriginal der Urkunde könnte jedoch eine elektronische Kopie, die qualifiziert signiert wird, vom Notar über seinen elektronischen Safe bereitgestellt werden. So können auch Änderungen, die während des Beurkundungstermins vorgenommen werden, noch in den digitalen Datensatz übernommen werden.

Bereitstellung notwendiger Unterlagen für den einheitlichen Ansprechpartner und zuständige Behörden im Zuge einer Antragstellung nach der EU-Dienstleistungsrichtlinie

In der seit Ende des Jahres 2009 in nationales Recht umgesetzten EU-Dienstleistungsrichtlinie ist der elektronische Austausch von Daten und Dokumenten zwischen Verwaltung und Antragsteller vorgesehen. Mit der Richtlinie soll es für Dienstleistungsunternehmen leichter werden, innerhalb der Grenzen der Europäischen Union ihrer Tätigkeit nachzugehen. Hierzu wurden die Mitgliedstaaten verpflichtet, die Antragstellung für Angelegenheiten der Dienstleistungsunternehmen im EU-Ausland aus der Ferne und auf elektronischem Wege zu ermöglichen.

Ohne geeignete Werkzeuge bei Verwaltung und Antragsteller wird der Austausch der notwendigen elektronischen Daten und Dokumente unnötig erschwert. Auf Seiten der Behörden und Gebietskörperschaften sind u.a. Systeme zum Wissensmanagement, Fallbearbeitung, Identitätsmanagement, Fachverfahren und weitere Basiskomponenten notwendig. Für die Dienstleistungsunternehmen sind Werkzeuge zur Antragstellung und -verwaltung hilfreich. Für die beteiligten Akteure ermöglichen elektronische Safes einen sicheren, vertraulichen sowie strukturierten und einfachen Austausch der notwendigen Daten[46].

Im Fall einer Antragstellung begibt sich das Dienstleistungsunternehmen auf das Internetportal des einheitlichen Ansprechpartners. Dort können die unterschiedlichen Anträge in Form von elektronischen Antragsassistenten aufgerufen und bearbeitet werden. Gleich zu Beginn besteht die Möglichkeit, ein Generalformular mit grundlegenden Daten auszufüllen. Hier kann der Antragsteller auch die Adresse seines elektronischen Safes hinterlegen. Beginnt er an-

[46] Breitenstrom, Christian; Eckert, Klaus-Peter; Lucke, Jörn von; Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS; Interdisziplinäre Studien zu Politik, Recht, Administration und Technologie e.V. (ISPRAT) (Hrsg.) (2008): IT-Umsetzung der EU-Dienstleistungsrichtlinie - Gestaltungsoptionen, Rahmenarchitektur, technischer Lösungsvorschlag - White Paper Version 2.0. Stuttgart: Fraunhofer IRB-Verl. (FOKUSbasic), S. 33 ff.

schließend die für seinen Antrag notwendigen digitalen Formulare auszufüllen, so besteht immer wieder die Möglichkeit, Formulardaten aus dem elektronischen Safe des Dienstleistungsunternehmens zu beziehen. Hierzu teilt der Antragsteller dem intelligenten Antragsassistenten an der geeigneten Stelle mit, die benötigten Daten aus dem elektronischen Safe zu übernehmen. Über das System des Antragsassistenten werden Freigabeanforderungen zu den benötigten Daten und Dokumenten generiert und an die angegebene Adresse des elektronischen Safes übermittelt. Der Safe-Client des Dienstleistungsunternehmens signalisiert das Eintreffen neuer Anforderungen. Sein Benutzer loggt sich ein und kann in der Übersicht der Freigabeanforderungen einfach erkennen, auf welche Daten der Antragsassistent Zugriff benötigt. Nach Erteilung der notwendigen Zugriffsrechte durch die Bestätigung der Freigabeanforderungen wird das jeweilige Online-Formular mit den entsprechenden Daten vorausgefüllt. Elektronische Dokumente werden der zuständigen Behörde ebenfalls freigegeben.

In diesem Szenario werden Dienstleistungsunternehmen durch den elektronischen Safe-Dienst in die Lage versetzt, ihre elektronischen Daten und Dokumente den zuständigen Behörden strukturiert zur Verfügung zu stellen. Die Antragsteller behalten dabei die Verantwortung für ihre Daten, da die öffentlichen Einrichtungen nur auf speziell für sie freigegebene Inhalte Zugriff erhalten.

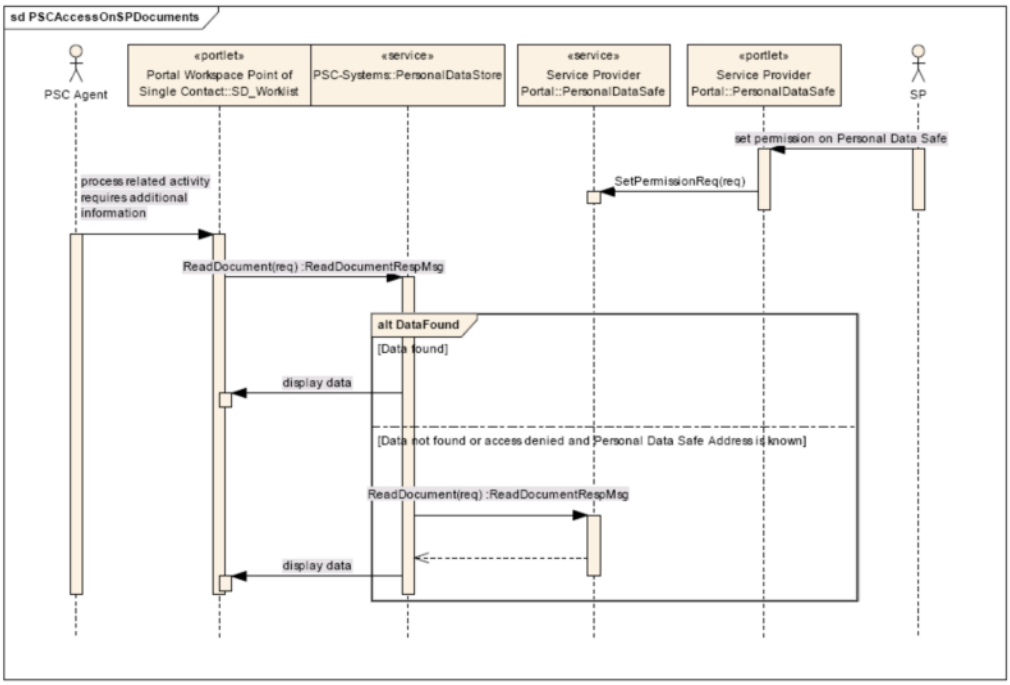

Abbildung 12: Kommunikationsablauf des Zugriffs eines EA-Mitarbeiters auf Daten des Dienstleistungserbringers[47] .

[47] Breitenstrom, Christian; Eckert, Klaus-Peter; Lucke, Jörn von; Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS; Interdisziplinäre Studien zu Politik, Recht, Administration und Technologie e.V. (ISPRAT) (Hrsg.) (2008): IT-Umsetzung der EU-

Automatisierte Unterstützung der Arbeitgeber bei der Erfüllung ihrer Meldepflichten

Zur Erfüllung ihrer Informations- und Meldepflichten obliegt es sämtlichen privaten und öffentlichen Arbeitgebern in Deutschland, in regelmäßigen Abständen Daten an unterschiedliche Stellen der öffentlichen Verwaltung zu übermitteln. Im Zuge der Einführung des Standardkostenmodells in Deutschland zur Ermittlung der Bürokratiekosten wurden die Informationspflichten erhoben. Im Dezember 2006 existierten demzufolge circa 10.000 verschiedene Informations- und Meldepflichten für Arbeitgeber. Abhängig von der jeweiligen Pflicht können Arbeitgeber unterschiedliche Optionen zur Übermittlung der jeweiligen Informationen in Anspruch nehmen.

Verschiedene Meldepflichten können bereits auf elektronischem Wege erfüllt werden. Hierzu zählen beispielsweise Informationen zu ausgewählten Umweltdaten, die im Rahmen der betrieblichen Umweltdatenberichterstattung mit BUBE online[48] übertragen werden können. Mit der Umsetzung des elektronischen Einkommensnachweises (ELENA) können Daten über die Verdienste der Arbeitnehmer automatisiert an die zuständigen Behörden übermittelt werden. Weiter bietet zum Beispiel das Statistische Bundesamt den Service eStatistik.core an, über den statistische Meldepflichten einfacher abgewickelt werden können. Neben den genannten Services existieren diverse weitere elektronische Angebote zur Meldung von Arbeitgeberinformationen. Über diese digitalen Lösungen zur Umsetzung von Informationspflichten sind nach wie vor etliche papierbasierte Informationsprozesse feststellbar.

Im Rahmen des Forschungsauftrags "Entwicklung von Prozessketten zwischen Wirtschaft und Verwaltung“ in den Jahren 2008/2009 durch das Bundesministerium des Innern wurde von Fraunhofer FOKUS und weiteren Projektpartnern ein Ansatz zur automatisierten Erfüllung der Arbeitgebermeldepflichten entwickelt[49]. Ein wesentliches Element dieses Ansatzes stellt der elektronische Safe als unternehmensweite Datendrehscheibe dar.

Auf Basis des elektronischen Safes als Dienst könnten weitere Teile der Informations- und Meldepflichten mit IT-Unterstützung automatisiert abgewickelt werden. Unternehmen setzen in diesem Szenario elektronische Safes ein, um regelmäßig von den öffentlichen Einrichtungen verlangte Daten gesichert organisationsintern abzulegen und möglichst medienbruchfrei zu übertragen (siehe Abbildung 13). Grundannahme ist, dass viele Meldungen an Behörden zwar in ihrer Gesamtheit unterschiedlich, in den Details aber vergleichbar auf-

---

Dienstleistungsrichtlinie - Gestaltungsoptionen, Rahmenarchitektur, technischer Lösungsvorschlag - White Paper Version 2.0. Stuttgart: Fraunhofer IRB-Verl. (FOKUSbasic).

48 Betriebliche Umweltdatenberichterstattung (BUBE online): https://www.bube.bund.de.

49 Bundesministerium des Innern (Hrsg.) (2009): „Machbarkeitsstudie zum Forschungsauftrag "Entwicklung von Prozessketten zwischen Wirtschaft und Verwaltung". Los 3 "Informations- und Meldepflichten für Arbeitgeber“.

gebaut sind. So werden in den entsprechenden Unterlagen gewisse Daten wie die Stammdaten immer wieder verwendet. Mit einem sicheren Speicherort wie dem elektronischen Safe können solche Daten zukünftig unternehmensweit an zentraler Stelle abgelegt werden. Bei der Generierung von Meldungen an die Behörden wird dann automatisiert auf die im elektronischen Safe vorgehaltenen Daten zurückgegriffen. Auf diese Weise werden Meldungen schnell zusammengestellt und elektronisch übermittelt.

Der elektronische Safe in seiner oben beschriebenen Funktionalität wird hierfür um Komponenten zur automatisierten Ablage und regelbasierten Verarbeitung und Aufbereitung der Daten erweitert. Relevante Daten werden aus vorhandenen Fachverfahren bzw. Enterprise-Ressource-Planning-Systemen des jeweiligen Unternehmens regelmäßig in ihren elektronischen Safe importiert. Entsprechend den Anforderungen aus den Informations- und Meldepflichten werden die im elektronischen Safe feingranular vorliegenden Daten jeweils passend zusammengefügt. So können aus den importierten Daten alle erforderlichen Meldungen erstellt und bereitgehalten werden.

Der elektronische Safe steht in diesem Szenario in jedem Fall unter der vollen Kontrolle des jeweiligen Unternehmens. Nur so ist eine hinreichende Akzeptanz des Ansatzes überhaupt denkbar. Für eine erfolgreiche Realisierung müssen jedoch gleichzeitig Betriebsmodelle entwickelt werden, welche die Nutzung elektronischer Safes im beschriebenen Rahmen auch kleinen und mittleren Unternehmen ermöglichen.

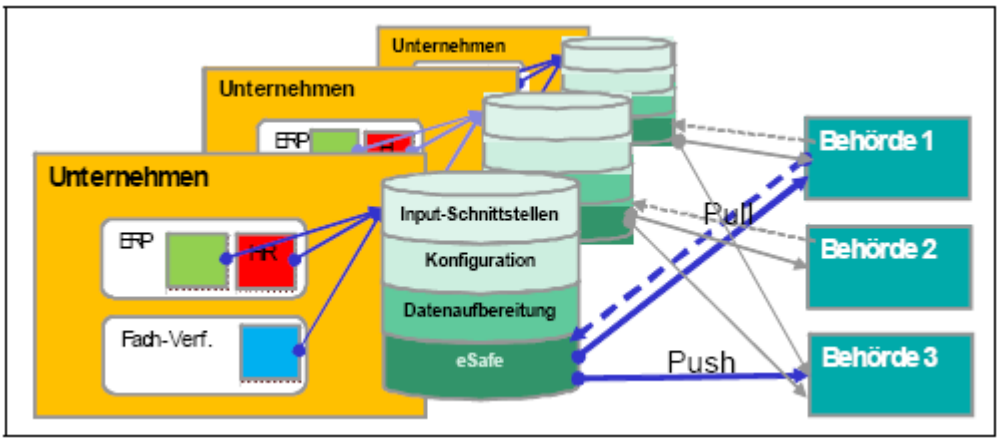

Abbildung 13: Der erweiterte elektronische Safe übermittelt Informationen zwischen Unternehmen und Behörden[50].

Die Informations- und Meldepflichten können mit Hilfe des elektronischen Safes im Push- oder im Pull-Verfahren verbreitet werden. Bei der ersten Variante teilt die jeweilige Behörde die Adresse ihrer digitalen Eingangsstelle mit. Zu dieser Stelle übermittelt der elektronische Safe die notwendigen Meldungen in

[50] Bundesministerium des Innern (Hrsg.) (2009): „Machbarkeitsstudie zum Forschungsauftrag "Entwicklung von Prozessketten zwischen Wirtschaft und Verwaltung". Los 3 "Informations- und Meldepflichten für Arbeitgeber“.

verschlüsselter Form. Bei der zweiten Variante stellt das Unternehmen über den elektronischen Safe verschlüsselte Meldungen zum Abruf bereit. Beteiligte öffentliche Einrichtungen greifen auf diese Daten selbständig zu.

Arbeitgeber sind verpflichtet, neben allgemeinen Meldungen auch jene Meldungen auszustellen, die sich auf einzelne Mitarbeiter beziehen. Arbeitnehmer benötigen für Dritte wie Behörden oder Banken entsprechende Bescheinigungen. Mit Hilfe des elektronischen Safes können diese individualisierten Unterlagen vereinfacht aufbereitet und den Mitarbeitern zur Verfügung gestellt werden. Dabei erfolgt die Bereitstellung in Form einer Freigabe im elektronischen Safe des Unternehmens. Der jeweilige Mitarbeiter kann auf diese Bescheinigung mit seinem eigenen elektronischen Safe zugreifen oder sich bei dem elektronischen Safe des Unternehmens ohne eigenen Safe registrieren.

7. Fazit

Der Einsatz elektronischer Safes zur sicheren und vertraulichen Aufbewahrung von Daten und Dokumenten bietet die Chance, digitale Geschäftsprozesse nutzerorientiert auszurichten. Safeeigentümer bleiben im Besitz ihrer Daten und können leichter nachvollziehen welche Daten wo Verwendung finden. Benötigen Dritte zur Durchführung ihrer Prozesse Daten eines Safeeigentümers, so können sie diese mittels Freigabenachrichten anfordern, die die Safeeigentümer über ihren Safe zum Zugriff freigeben können. Dabei stehen ihnen Möglichkeiten zur genauen Definition der jeweiligen Freigabe im Hinblick auf Dauer, Häufigkeit und Zugriffsberechtigte zur Verfügung. Wird eine Freigabe langfristig erteilt, so stehen dem Safenutzer die hier enthaltenen Daten entsprechend der jeweiligen Frist zur Einbindung in die eigenen Vorgänge zur Verfügung. Jeder Zugriff wird dabei protokolliert.

Die wesentliche Herausforderung aus technisch-organisatorischer Perspektive liegt in der großflächigen Etablierung von vertrauenswürdigen Infrastrukturen und der notwendigen Überzeugungsarbeit für den Einsatz hochsicherer Mechanismen für die Aufbewahrung und Bereitstellung der digitalen Werte von Bürgern, Unternehmen und Verwaltung. Bei der Überzeugungsarbeit geht es darum, hervorzuheben, dass elektronische Safes, wie sie hier beschrieben wurden, ein höheres Datenschutz- und Sicherheitsniveau bieten, als zum Beispiel Online-Festplatten (zur Abgrenzung siehe auch Kapitel 3.3). Dem Privacy by Design-Ansatz folgend wurden entsprechende Aspekte von vornherein bei der Konzeption elektronischer Safes mitgedacht. Darüber hinaus ist zur Realisierung elektronischer Safes ein möglichst breites Einsatzspektrum eine wichtige Voraussetzung.

Mit Hilfe der beschriebenen Dienste auf Basis elektronischer Safes können Safeeigentümer unter Wahrung ihrer Privatsphäre weitere Funktionen nutzen. Dies bedeutet, sie erhalten zum Beispiel die Möglichkeit, Auswertungen ihrer eigenen Daten vorzunehmen, Datentransformationen durchzuführen oder die Aufbereitung für bestimmte Fachverfahren anzustoßen. Die dargestellten Integrationsdienste erlauben eine möglichst einfache Ausweitung der digitalen Datenbasis. Je mehr elektronische Daten im Safe abgelegt werden können, desto größer stellt sich das Anwendungsspektrum und der daraus resultierende Nutzen des Safeeinsatzes dar. Die weiteren externen Dienste auf Grundlage elektronischer Safes unterstützen die unverkettbare und unbeobachtbare Informationsweitergabe aus dem Safe heraus.

Im Kontext der Rechtsfragen zur Nutzung eines elektronischen Safes ist derzeit in Deutschland die Zukunft des De-Mail-Gesetzes bzw. das Verhältnis von Safes zu den dortigen Vorgaben eines Postfach- und Versanddienstes nicht

geklärt. Selbst wenn sich Safeanbieter an den gesetzlichen Vorgaben (Versandbestätigungen, Sicherheitsniveaus etc.) orientieren, ist nicht gewährleistet, dass Behörden dies als vergleichbar „sicher“ akzeptieren, Bestätigungen o.ä. (mangels gesetzlicher Regelungen) vergleichbare Beweiskraft zugemessen wird und eine Gleichstellung der Safe-Kommunikation mit dem Postfach- und Versanddienst im Sinne des Zustellungsrechts akzeptiert wird. In jedem Fall würden den Safes bestimmte Funktionen gänzlich fehlen (bspw. förmliche Zustellung). Der Unterschied zwischen „isolierten“ Safes und den Bürgerportalen besteht darin, dass das Bürgerportal-Konzept darauf basiert, dass auf beiden Seiten eine sichere Kommunikation (gesetzlich) gewährleistet ist. Dies ist bei „isolierten“ Safes gerade nicht garantiert, so dass zu klären wäre, wie Safes als De-Safes ausgestaltet oder an diese angebunden werden können. Gegebenenfalls bedarf es in diesem Kontext einer Prüfung, ob nicht gesetzliche Regelungen auch zu den Safes (in Entsprechung zum Postfach- und Versanddienst) sachgerecht sind, zumal so der Mehrwert der Freigabe- und Einstellfunktionen gegenüber den klassischen Postfächern realisiert werden könnte.

Insofern hat die rechtliche Betrachtung folgende Ergebnisse und Handlungsempfehlungen hervorgebracht:

- Die Einbindung einer sicheren Instanz („Datennotar“), die den elektronischen Safe betreibt oder zumindest überwacht, ist aufgrund der technischen Ausgestaltung elektronischer Safes, die ein neues Niveau bezüglich Datensicherheit und -schutz garantieren kann, nicht erforderlich und angesichts des bisherigen Aufgabenprofils der Notare nicht sachgerecht.

- Eine Verortung elektronischer Safes im privatrechtlichen Raum bei gleichzeitiger Sicherstellung der Vertraulichkeit und Akzeptanz durch staatliche Reglementierung und Überwachung erscheint naheliegend, aber auch erforderlich.

- Ein ausgewogenes Verhältnis zwischen (teil-) reguliertem Markt und freiem Wettbewerb, bspw. im Kontext der Safedienste, sichert das zur breiten Akzeptanz erforderliche Vertrauen der Nutzer einerseits, lässt zugleich aber auch Investitionen der Safeanbieter aufgrund der erzielbaren Gewinne erwarten.

- Die erforderliche Regulierungsgesetzgebung kann in weiten Teilen in Anlehnung an die Vorgaben für die De-Mail-Anbieter erfolgen.

- Sie ist jedoch zwingend um safespezifische Regelungen zu ergänzen.

- Dem Einsatz elektronischer Safes stehen keine unüberbrückbaren rechtlichen Schranken entgegen, zumal zahlreiche Rechtsfragen ent-

weder durch die Regulierung gelöst werden oder unter Rückgriff auf bestehende und vergleichbare Angebote sachgerecht bewältigt werden können.

- Die zunehmende Digitalisierung erfordert aber weitergehende Reaktionen, um ein elektronisches Verwaltungsverfahren und übergreifende Prozessketten zu ermöglichen. Sowohl im Kontext der De-Mail als auch für den Einsatz elektronischer Safes ist ein E-Government-Gesetz zu schaffen, das Rechtsfragen der elektronischen Zustellung, Zugangseröffnung und Nachweisbarkeit behandelt, oder das Verwaltungsverfahrens- und Zustellungsrecht ist entsprechend fortzuentwickeln. Gleiches gilt für das Datenschutzrecht.

Auch wenn das technisch erreichbare Sicherheitsniveau elektronischer Safes hoch ist, stellen organisatorisch-rechtliche Maßnahmen weiterhin eine sinnvolle Ergänzung dar. Zum einen kann die technische Ausgestaltung kaum 100% Sicherheit bieten. Zum anderen können nicht-technische Maßnahmen zur Vertrauensbildung von entscheidender Bedeutung sein. So bietet die Akkreditierung von Safeanbietern eine leicht verständliche Hilfestellung für die individuelle Entscheidung, zukünftig elektronische Safes zu nutzen.

Elektronische Safes für Bürger, Unternehmen und die öffentliche Verwaltung bieten zukünftig eine sichere und vertrauenswürdige Infrastruktur zum Austausch digitaler Daten und Dokumente. Dienste auf Basis dieser Safes vergrößern die Chancen auf umfassende Vernetzung und Realisierung medienbruchfreier Prozesse. Elektronische Safes und ihre Dienste stellen somit einen Beitrag zur Erreichung der digitalen Gesellschaft dar.