IT Security

Anforderungen für den Aufbau eines eIDAS konformen Vertrauensdiensteanbieters

Voraussetzungen einer qualifizierten CA in der EU am Beispiel Österreich

Bachelorarbeit

zur Erlangung des akademischen Grades

Bachelor of Science in Engineering (BSc)

eingereicht von

Paul Lackner

1610410024

im Rahmen des

Studienganges IT Security an der Fachhochschule St. Pölten

Betreuung

Betreuer/in: FH-Prof. Univ.-Doz. Dipl.-Ing. Dr. Ernst Piller

Mitwirkung: -

St. Pölten, 1. Mai 2019 _____ _____

(Unterschrift Verfasser/in) (Unterschrift Betreuer/in)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Bachelorarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Bachelorarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Bachelorarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Ort, Datum *Unterschrift*

Kurzfassung

Die Digitalisierung ist ein oft erwähntes Thema, jedoch werden noch immer ein Großteil der Dokumente händisch unterschrieben. Die EU schuf nun mit der eIDAS ein Rahmenwerk um digitale Unterschriften und Siegel, in weiterer Folge Vertrauensdienste jeglicher Art, EU-weit interoperabel zu gestalten und damit diesen einen größeren Geltungsraum zu verschaffen. Diese Arbeit beschäftigt sich nun mit besagter Verordnung und versucht die Anforderungen für die Anbieter der Vertrauensdienste, sogenannte Vertrauensdiensteanbieter (VDA), am Beispiel Österreich aufzubereiten und darzulegen. Dabei wird die eIDAS, das Signatur- und Vertrauensdienstegesetz und die Signatur- und Vertrauensdiensteverordnung analysiert sowie kommentiert.

Abstract

The digitalization is an often mentioned topic, but still a majority of documents are signed manually. The EU created a framework called eIDAS to arrange digital signatures and seals and all other trust services to be interoperable in the EU. This thesis approaches the topic by analysing the eIDAS, the SVG and the SVV and tries to summaries the requirements of trusted service providers in Austria.

Inhaltsverzeichnis

1 Einleitung

Public Key Infrastructure (PKI) ist ein gängiges Schlagwort nicht nur in der IT-Sicherheit, sondern auch im restlichen, kommerziellen Geschäftsumfeld. Auch staatliche Organisationen haben dies bereits bemerkt und sowohl auf EU, wie auch auf Bundesebene durch Verordnungen und Gesetze reguliert. Seit 1995 existiert mit VeriSign, einer US-amerikanischen Firma, der erste kommerzielle Anbieter digitaler Zertifikate. Dadurch wurde eine Möglichkeit geschaffen, sich auf digitale Art und Weise auszuweisen, Dokumente zu signieren und auch zu verschlüsseln und damit eine vertrauliche Kommunikation zu ermöglichen. Am 19. August 1999 wurde in Österreich das Signaturgesetz (SigG)[1] beschlossen, das am 1.1.2000 in Kraft trat. Österreich war damit das erste Land der EU, das die dementsprechende EG-Richtlinie 1999/93/EG umsetzte. Dann wurde in Österreich das SigG im Jahr 2016 durch das Signatur- und Vertrauensdienstegesetz (SVG)[2] auf Basis der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS)[3] ersetzt. Diese Verordnung und das daraus abgeleitete österreichische Gesetz regelt die elektronische Identifizierung und Rahmenbedingungen für die jeweiligen Vertrauensdienste auf europäischer Ebene beziehungsweise auf Österreich abgeleitet und stellt einen fundamentalen Baustein in der Vision des digitalen Europas dar.

1.1 Struktur der Arbeit

Diese Arbeit wird sich mit den Gegebenheiten für einfache und vor allem qualifizierte Vertrauensanbieter beschäftigen. Welche Unterschiede organisatorischer, technischer und finanzieller Sicht gibt es, welche Einsatzgebiete gibt es für einfache Zertifikate, wofür braucht man rechtlich gesehen qualifizierte Zertifikate? Wie müssen diese Vertrauensdiensteanbieter aufgebaut sein und welche Stellen sind befugt dies zu überprüfen?

[1] Bundeskanzleramt, Signaturgesetz

[2] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz

[3] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS

Die Arbeit versucht zuerst die Grundlagen einer PKI zu erklären. Was für Komponenten gibt es darin und welche Anforderungen gilt es zu bewältigen. Dann werden Definitionen der eIDAS zu den spezfischen Begriffen und erklärt. Der Hauptteil der Arbeit beschäftigt sich mit den Anforderungen an VDA sowie deren angebotenen Dienste und Produkte.

2 Grundlagen

Um die Arbeit verstehen zu können, muss der grundsätzliche Aufbau einer PKI verstanden werden. Es gibt einige Komponenten die jeweils nur von bestimmten Akteuren bedient und benutzt werden. Dazu zählen die Certification Authority (CA), der Zertifikatsserver oder Verteilserver, eine Registrier- und Sperrstelle, ein Zeitstempeldienst (TSA) sowie das Personal Security Environment (PSE).
In weiterer Folge werden die als Beispiel dienenden Kommunikationspartner Alice, Bob und Candace heißen, ein möglicher unerwünschter Teilnehmer (Hacker) Mallory.

2.1 Aufbau einer Public Key Infrastruktur (PKI)

Eine PKI besteht aus einigen Komponenten, die, grob zusammengefasst, das digitale Signieren ermöglichen. Die notwendigen Komponenten und Dienste werden im folgenden Kapitel erklärt.

2.1.1 Digitale Zertifikate

Digitale Zertifikate, in Folge nur mehr „Zertifikat“ genannt, bilden einen fundamentalen Baustein in einer PKI. Mit Zertifikaten können die vier in Abschnitt 2.2 beschriebenen Anforderungen berücksichtigt werden. Ein Zertifikat beinhaltet neben dem öffentlichen Schlüssel, Informationen über den Inhaber (z.B.: Name, E-Mail-Adresse, Arbeitsplatz, Wohnort), sowie eine Seriennummer, Gültigkeitszeitraum, den Verwendungszweck des Schlüssels (Signatur, Verschlüsselung, Authentifizierung) und eine Signatur einer übergeordneten Stelle. Diese übergeordnete Stelle wird „Certification Authority“ genannt. Der genaue Zweck einer CA wird noch erläutert.
Als Beispiel wird in Abbildung 2.1 das persönliche Zertifikat des Autors (in diesem Fall der Common Name (CN)), ausgestellt durch die A-Trust (CA), gezeigt. In diesem Zertifikat sind etliche Detailinformationen hinterlegt, zum Beispiel die Zertifikatsversionsnummer, der verwendete Hash-Algorithmus und die Seriennummer. Die wesentlichen Informationen sind die Antragssteller-Informationen, dessen öffentlicher Schlüssel, die ausstellende CA sowie deren öffentlicher Schlüssel und die Signatur, der Gültigkeitszeitraum

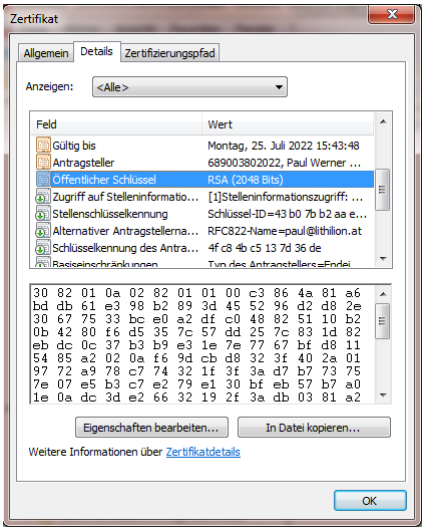

Abbildung 2.1: Zertifikatsansicht der Windows-Konsole. Der ausgewählte Bereich stellt den öffentlichen Schlüssel im Hex-Format dar. Zu sehen sind noch weitere Felder, die über diese Konsole abgefragt werden können.
Bildquelle: Screenshot

sowie der Zugriffspunkt zu den Sperrlisten. Nicht nur natürliche Personen können Zertifikate erhalten, sondern auch Server, Clients und Anwendungen können Zertifikate ausgestellt bekommen. Abbildung 2.2 zeigt das Schema eines Zertifikats.

2.1.2 Signaturen

Digitale Signaturen haben die gleiche Funktion wie handschriftliche Signaturen. Sie sind Authentizitätsbekundungen. Qualifizierte digitale Signaturen sind den handschriftlichen sogar rechtlich gleichgestellt[1][2]. Digitale Signaturen werden aus dem Hash des zu unterzeichnenden Dokumentes sowie einem Zertifikat gebildet. Sie beinhalten daher die zu vergleichende Version des Dokument, das verwendete Zertifikat (bei personenbezogenen Zertifikaten dadurch die Person) und den lokalen Zeitstempel.

2.1.3 Certificate Authority (CA)

Ein Kernelement der PKI ist die Certification Authority. Sie stellt Zertifikate aus und sorgt dafür, dass durch die Ausstellung gewisse Richtlinien eingehalten werden. Weiters verwaltet eine CA auch ihre Sperrliste. Hier können bereits ausgestellte Zertifikate für ungültig erklärt werden. Wichtig zu erwähnen ist noch, dass

[1] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 25 Absatz 2
[2] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §4 Absatz 1

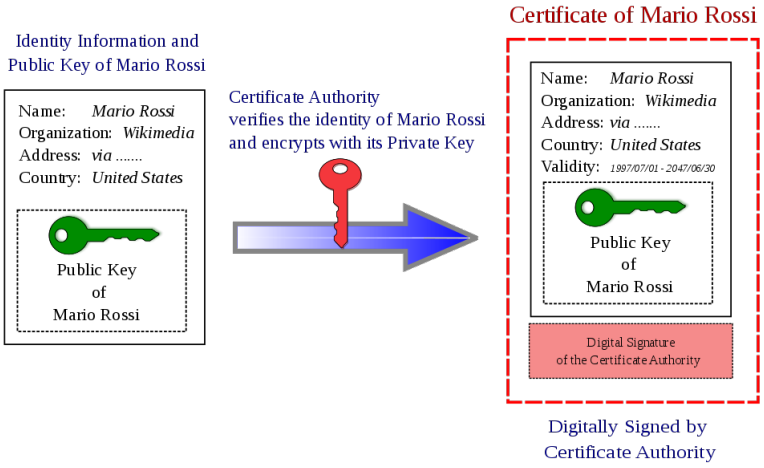

Abbildung 2.2: Das Schema eines Zertifikats. Es zeigt die Weise wie ein Zertifikat aufgebaut ist. Der Benutzer erstellt sich einen Ausweis und fügt seinen öffentlichen Schlüssel hinzu. Dies wird mit dem privaten Schlüssel des VDA signiert.
Bildquelle: Benutzer Giaros auf Wikimedia Commons: `https://commons.wikimedia.org/wiki/File:PublicKeyCertificateDiagram_It.svg`

die CA selbst im alleinigen Besitz ihres eigenen privaten Schlüssels ist. Dieser Schlüssel wird zum Signieren der ausgestellten Zertifikate verwendet. Sollte Mallory in Besitz dieses Schlüssels kommen, ist dadurch die gesamte PKI von dieser CA ausgehend abwärts kompromittiert. Sämtliche von dieser CA ausgestellten Zertifikate sind in diesem Fall als ungültig zu erklären und neu auszustellen. Eine CA kann von jedem betrieben werden, es ist eine Sache des Vertrauens, ob die CA auch akzeptiert wird. Im Falle einer Firma kann es sinnvoll sein eine CA durch die IT-Abteilung betreiben zu lassen. Im Falle eines Staates ist es sinnvoll dies durch das staatliche Rechenzentrum zu betreiben. Weiters ist es aus rechtlicher Hinsicht noch wichtig zu unterscheiden, ob es sich um eine einfache oder qualifizierte CA und damit auch um ein dementsprechendes Zertifikat handelt. Im Fall der österreichischen Bürgerkarte übernimmt dies die Firma *A-Trust*. Sie erzeugt beide Arten von Zertifikaten auf der Smartcard.

2.1.4 Verteilserver

Der Zertifikatsserver ist optional zu betreiben, aber sehr zu empfehlen, um einen reibungslosen Betrieb der PKI gewährleisten zu können. Der Server stellt die Zertifikate und Sperrlisten anderen Teilnehmern zur Verfügung und sollte daher jedem PKI Teilnehmer zugänglich sein. Meist geschieht dies über einen

Verzeichnisdienst (z.B.: Lightweight Directory Access Protocol (LDAP) oder *Microsoft* Active Directory (AD)). Weiters bietet dieser Server oft auch einen Dienst zur Gültigkeitsprüfung von Zertifikaten an (certificate revocation list (CRL), online certificate status protocol (OCSP)). Dabei sendet ein Client ein zu überprüfendes Zertifikat an den Server, dieser prüft ob das übermittelte Zertifikat noch gültig ist oder widerrufen wurde und sendet eine dementsprechende Antwort zurück. Im Fall der österreichischen Bürgerkarte übernimmt dies die Firma *a-trust*.

2.1.5 Zeitstempeldienst (TSA)

Das Problem einer digitalen Signatur ist, dass der verwendete Zeitstempel, der des gerade benutzten Rechners ist. Da aber bekanntlich die lokale Zeit sehr leicht änderbar ist, ist so ein Zeitstempel recht wertlos. Da kommt ein Zeitstempeldienst (TSA) zum Einsatz. Dieser signiert das Dokument zusätzlich mit seinem eigenen Zeitstempel. Zeitstempel sind dann kritisch, wenn es sich um Urheberschaften von Dokumenten handelt (ist Dokument A zuerst von Alice und später erst eine Kopie davon von Mallory signiert und damit von Mallory gestohlen worden), und wenn es sich um gesperrte Schlüssel handelt (ist Dokument A vor oder nach der Schlüsselsperre signiert worden).

2.1.6 Registrierstelle

Die Registrierungsstelle ist die Anlaufstelle zum Beantragen eines Zertifikates. Dies ist meist das Büro eines Administrators oder eine Filiale eines Trust-Anbieters. Dies ist eine optionale Stelle, immerhin kann Alice auch direkt mit der CA kommunizieren. Außerdem fällt diese Einrichtung bei automatisch erstellten Zertifikaten weg. Im Fall der österreichischen Bürgerkarte übernimmt diese Aufgabe das Magistrat oder eine Bezirkshauptmannschaft.

2.1.7 Sperrstelle

Die Sperrstelle ist die Anlaufstelle zum Sperren verlorener oder gestohlener Zertifikate. Bob ruft eine (meist ohnehin bekannte) Hotline an; der Mitarbeiter trägt Bobs Zertifikat in die Sperrliste ein und erklärt es damit für ungültig. Im Fall der österreichischen Bürgerkarte übernimmt dies die Firma *A-Trust* unter der Nummer 01 715 20 60[3]. Meistens ist diese Nummer rund um die Uhr erreichbar. Betreffend der Bürgerkarte ist dies der Fall.

[3] `https://www.buergerkarte.at/hilfe.html`

2.1.8 Personal Security Environment (PSE)

Die Personal Security Environment (PSE) kann sowohl als Software als auch als Hardware realisiert werden. Meist handelt es sich dabei um den Smartcard-Reader am Arbeitsplatz. Alternativ kann der Schlüssel auch auf einer verschlüsselten Festplatte liegen. Weiters gibt es noch Roaming-PSE. Darunter wird das Konzept verstanden, den privaten Schlüssel von Alice auf einem Server zu speichern. Alice muss daher mit einem Roaming-Client eine Verbindung zu dem Server aufbauen, um den Schlüssel verwenden zu können. Dies ist aber heftig umstritten, da der private Schlüssel jemand anderem anvertraut wird. Im Fall der österreichischen Bürgerkarte ist dies ein eigens beschaffter Smartcard-Reader um die eCard mit den aufgespielten Zertifikaten auslesen zu können.

2.2 Eigenschaften einer PKI

Eine PKI setzt gewisse Eigenschaften und Richtlinien, in Bezug auf Identitäten durch und löst die unten beschriebenen Probleme.

2.2.1 Authentizität der Schlüssel

Asymmetrische Verschlüsselung funktioniert mit einem Schlüsselpaar, einem öffentlichen und einem privaten Schlüssel. Wird zum Beispiel eine E-Mail verschickt, kann sie mit dem öffentlichen Schlüssel des Empfängers verschlüsselt werden. Woher bekommt der Absender aber diesen öffentlichen Schlüssel und wer garantiert, dass dieser öffentliche Schlüssel wirklich dem Empfänger gehört?

2.2.2 Sperrung der Schlüssel

Alice kommt ihr privater Schlüssel abhanden. Dabei ist es völlig irrelevant, ob dieser Schlüssel verloren, gestohlen, kopiert oder anderweitig verschwunden oder in falsche Hände geraten ist. Alice möchte nun ihren Kommunikationspartner (Bob und Candace) mitteilen, dass der früher verwendete Schlüssel ungültig geworden ist. Schreibt sie eine E-Mail mit einem neuen Schlüssel? Dabei muss aber die Authentizität beachtet werden. Schreibt sie eine E-Mail unverschlüsselt? Dabei muss die Verbindlichkeit beachtet werden, außerdem könnte Mallory diese Nachricht abfangen und/oder verfälschen. Weiters wird dies bei vielen Teilnehmern schnell aufwendig.

2.2.3 Verbindlichkeit

Mit einem Schlüsselpaar können Daten auch signiert werden. Dabei muss die Signatur für Verbindlichkeit sorgen. Diese darf nicht im Nachhinein von dem Signatar abgestritten werden können, beispielsweise indem Alice behauptet, der Schlüssel, mit dem unterschrieben wurde, gehöre nicht ihr.

2.2.4 Durchsetzen einer Richtlinie

Es soll eine Richtlinie bezüglich Schlüssellänge und Komplexität durchgesetzt werden. Weiters sollen beispielsweise die Schlüssel zentral registriert werden und jeder Teilnehmer genau ein Schlüsselpaar ausgestellt bekommen.

2.3 Vertrauensmodell

Ein Vertrauensmodell beschreibt die Beziehungen zwischen verschiedenen Teilnehmern und deren Vertrauen untereinander. Dabei wird beachtet, ob ein Teilnehmer dem jeweils anderen vertraut und umgekehrt. Es gibt drei große Vertrauensmodelle (Direct Trust, Web of Trust, Hierarchical Trust), wobei eine mittels CA verwirklichte PKI auf Hierarchical Trust setzt.
Beim Hierarchical Trust werden die Zertifikate nicht selbst ausgestellt, sondern es werden Certificate Signing Requests (CSR) an CAs gesandt und diese wiederum stellen ein von ihnen signiertes Zertifikat aus. Alice und Bob möchten ein Zertifikat bekommen. Sie stellen einen CSR an eine CA. Diese überprüft verschiedene Kriterien, die in einer Richtlinie festgelegt wurden. Anschließend stellt sie den beiden jeweils ein Zertifikat aus, das auch von dieser CA signiert wurde. Jeweils Alice und Bob haben das Zertifikat der CA als vertrauenswürdig auf ihren Rechnern abgelegt und können somit auch die Zertifikate des jeweils anderen überprüfen. So kann Alice auch an Candace problemlos eine Nachricht schicken, da Candace die Nachricht durch Alices Zertifikat verifizieren kann. Alice kann nun auch zusätzlich aus einem möglicherweise angeschlossenen Verzeichnisdienst Candaces Zertifikat laden und diese E-Mail verschlüsselt verschicken. Voraussetzung ist, dass das Zertifikat der CA sich auf dem Computer als vertrauenswürdig eingestuft befindet. Handelt es sich um eine interne CA einer Firma, wird dies höchstwahrscheinlich durch die IT-Abteilung bewerkstelligt. Einige Zertifikate der international bekannten CAs sind mit der Auslieferung des Betriebssystems gleich auf den Rechnern vorinstalliert.
Aber auch der Hierarchical Trust hat je nach Anwendungsfall miteinander kompatible Varianten.

2.3.1 Ein-Stufen-Hierarchie

Dieses Modell kommt oft bei KMUs zum Einsatz. Es gibt eine CA, die sämtliche im Umlauf befindlichen Zertifikate (persönliche Zertifikate, Anwendungszertifikate,...) ausstellt. Alice benötigt dadurch nur den öffentlichen Schlüssel dieser CA und kann alle Zertifikate überprüfen.

2.3.2 Mehr-Stufen-Hierarchie

Ein Konzern oder Staat könnte dies betreiben. Es wird eine Wurzel-CA (Root-CA) bereitgestellt. Diese stellt weiteren, untergeordneten CAs Zertifikate aus. Diese untergeordneten CAs können wiederum weiteren, untergeordneten CAs Zertifikate ausstellen oder die Endzertifikate ausstellen. Das Zertifikat von Bob wäre dann in der Stufe 0, das Zertifikat der ausstellenden CA in Stufe 1 und das der Wurzel-CA in Stufe 2.
Dieses Prinzip kann verwendet werden, um beispielsweise Zertifikate der Mitarbeiter in Europa von Zwischen-CA 1 auszustellen, die Zertifikate der Mitarbeiter in Asien von Zwischen-CA 2 und die Zertifikate der Rechner von Zwischen-CA3. Um all diese Zertifikate überprüfen zu können, muss lediglich das Zertifikat der Wurzel-CA bekannt sein. Vorteil einer solchen Struktur ist einerseits, dass die Vergabe der Zertifikate an verschiedene IT-Abteilungen aufgeteilt werden kann, und andererseits, dass ganze Bereiche wenn nötig schnell und effizient für ungültig erklärt werden können, ohne die PKI ganz austauschen zu müssen. Dieses System wird in Abbildung 2.3 dargestellt.

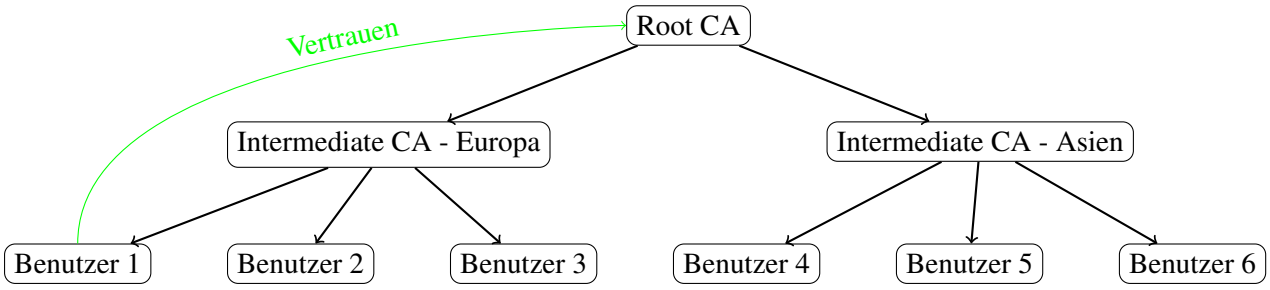

Abbildung 2.3: Mehr-Stufen-Hierarchie. User 1 bekommt sein Zertifikat von Europa ausgestellt, benötigt aber nur das Zertifikat der Root-CA um die Zertifikate aller anderen User (Europa und Asien) zu verifizieren.
Bildquelle: Selbst erstellt mit TikZ

2.4 Rechtliche Grundlagen

Da sich diese Arbeit vor allem mit der eIDAS Verordnung und darüber hinaus mit der EU-Richtlinie 1999/93/EG auseinandersetzt, wird auch ein Grundverständnis darüber sowie über das sich daraus ableitende SigG und das SVG benötigt.

2.4.1 EG-Richtlinie 1999/93/EG

Die EU-Richtlinie zielte darauf ab, gemeinsame Regeln für elektronische Signaturen im Binnenmarkt zu schaffen um das Vertrauen der Mitgliedsstaaten in die einzelnen Vertrauensdiensteanbieter sowie die generelle Akzeptanz in elektronische Authentifizierungsmaßnahmen zu stärken. Generell wird die elektronische qualifizierte Signatur der handschriftlichen Signatur gleichgestellt. Die Richtlinie schreibt auch erstmals vor, eine elektronische Signatur als gerichtliches Beweismittel zuzulassen, jedoch werden die einzelnen zugelassenen Rechtsgebiete von den jeweiligen Nationalstaaten bestimmt. Dabei wird explizit darauf hingewiesen, dass diese Anbieter von öffentlichen Stellen, juristischen und natürlichen Personen betrieben werden können[4]. Diese Rechtsvorschrift ist im Rang einer EG-Richtlinie und daher nicht unmittelbar bindend, sondern muss erst durch nationale Gesetze (in diesem Fall bis 19. Juli 2001) ratifiziert und umgesetzt werden[5][6]. Außerdem schreibt sie auch keine genauen Details vor, sondern lässt die technische und organisatorische Umsetzung Sache der Mitgliedsstaaten sein. Die Richtlinie wurde am 30. Juni 2016 durch die eIDAS Verordnung außer Kraft gesetzt und wird daher in dieser Arbeit nicht mehr behandelt.

2.4.2 eIDAS Verordnung

Die eIDAS Verordnung der EU setzt die EG-Richtlinie 1999/93/EG außer Kraft und ersetzt sie durch neue Regelungen, unter anderem weil die Richtlinie Regelungen festgelegt hat, „ohne einen umfassenden grenz- und sektorenübergreifenden Rahmen für sichere, vertrauenswürdige und einfach zu nutzende elektronische Transaktionen zu schaffen. Die [...] Verordnung stärkt und erweitert die Rechtsvorschriften jener Richtlinie“[7]. Das Europäische Parlament sieht als Mittel zur Vollendung des Binnenmarktes die Notwendigkeit, „dass die Sicherheit elektronischer Dienstleistungen — insbesondere elektronischer Signaturen — wichtig ist und dass auf europäischer Ebene eine Infrastruktur öffentlicher Schlüssel (PKI) geschaffen werden muss, und forderte die Kommission auf, eine Schnittstelle der europäischen Validierungsstellen (European

[4] Europäische Kommission, EG-Richtlinie 1999/93/EG Erwägungsgrund 12
[5] Europäische Union, Verordnungen, Richtlinien und sonstige Rechtsakte
[6] Europäische Union, Durchführungsrechtsakte und delegierte Rechtsakte
[7] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Erwägungsgrund 3

Validation Authorities Gateway) einzurichten, um die grenzüberschreitende Interoperabilität elektronischer Signaturen zu gewährleisten“[8]. Weiters verpflichtet die Verordnung die Mitgliedsstaaten zur Errichtung von einheitlichen Ansprechpartnern und die Anerkennung der Identifizierungsmaßnahmen der jeweils anderen Mitgliedsstaaten. „Eines der Ziele dieser Verordnung ist die Beseitigung bestehender Hindernisse bei der grenzüberschreitenden Verwendung elektronischer Identifizierungsmittel, die in den Mitgliedstaaten zumindest die Authentifizierung für öffentliche Dienste ermöglichen. Diese Verordnung bezweckt keinen Eingriff in die in den Mitgliedstaaten bestehenden elektronischen Identitätsmanagementsysteme und zugehörigen Infrastrukturen.“[9] Die Regelung ist Teil einer Vision, dargestellt in Abbildung 2.4, deren Umsetzung dadurch ermöglicht werden soll. Als EU-Verordnung ist die Regelung rechtlich direkt bindend und muss nicht mehr durch nationale Gesetze ratifiziert werden[10].

2.4.3 Signaturgesetz (SigG)

Das SigG „regelt den rechtlichen Rahmen für die Erstellung und Verwendung elektronischer Signaturen sowie für die Erbringung von Signatur- und Zertifizierungsdiensten“[11]. Das Gesetz war die österreichische Ratifizierung und nationale Umsetzung der EG-Richtlinie 1999/93/EG. Durch die Aufhebung der Richtlinie am 30. Juni 2016 und anschließendem in Kraft treten der eIDAS am 1. Juli 2016 wurde auch dieses Gesetz zeitgleich vom Signatur- und Vertrauensdienstegesetz (SVG) abgelöst. Das SigG wird daher nicht mehr in dieser Arbeit behandelt.

2.4.4 Signatur- und Vertrauensdienstegesetz (SVG)

Das SVG Gesetz trat am 1. Juli 2016 zeitgleich mit der eIDAS Verordnung in Kraft. Es ersetzt das SigG und ergänzt die eIDAS Verordnung. Wesentlich dabei ist die Konzentrierung der Regelung auf qualifizierte Zertifikate und deren Rechtswirkung, sowie deren Aussteller, die Vertrauensdiensteanbieter und deren Voraussetzungen. Das SVG beschreibt Akkreditierungsstellen und deren Aufgaben zur Bestätigung diverser Vertrauensdiensteanbietern. Details dazu werden in der Signatur- und Vertrauensdiensteverordnung (SVV) behandelt.

[8] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Erwägungsgrund 7
[9] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Erwägungsgrund 12
[10] Europäische Union, Verordnungen, Richtlinien und sonstige Rechtsakte
[11] Bundeskanzleramt, Signaturgesetz §1 Abs. 1

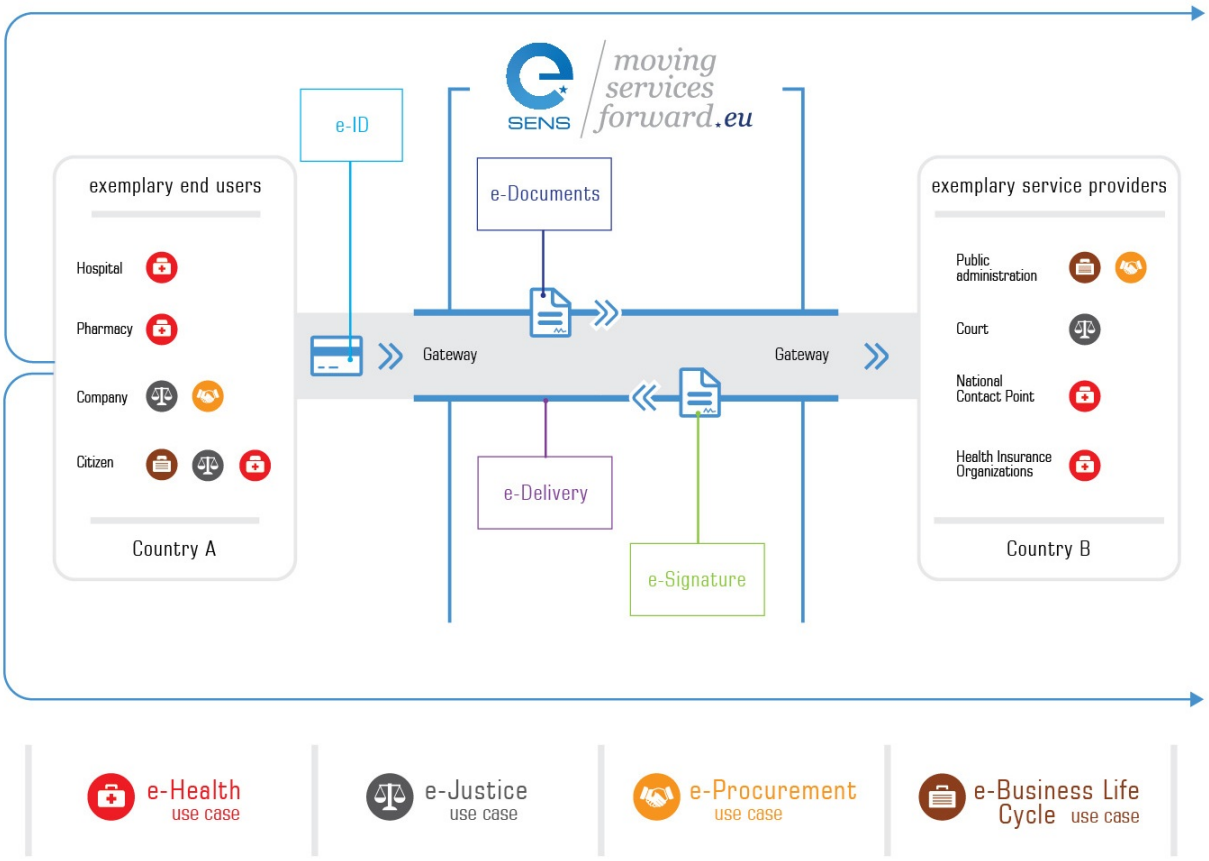

Abbildung 2.4: Digitale Vision der EU, die mit Hilfe der eIDAS umgesetzt werden soll. Bürger, Behörden und Unternehmen sollen digital mittels Vertrauensdiensten ihre Geschäfte erledigen können. Bildquelle: Benutzer FlippyFlink auf `https://commons.wikimedia.org/wiki/File:E-SENS_architecture.jpg`

2.4.5 Signatur- und Vertrauensdiensteverordnung (SVV)

Die SVV fällt in den Zuständigkeitsbereich des Bundeskanzlers[12] und ist laut SVG auf dem aktuellen technischen Stand zu halten. Sie regelt die technischen, organisatorischen und finanziellen Details. Als Verordnung des Bundes ist diese Regelung in der Rechtsordnung unter dem SVG angesiedelt[13].

[12] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz § 17 Abs. 1

[13] Richtervereinigung, Stufenbau der Rechtsordnung

3 Begriffsdefinition nach eIDAS

Diese Arbeit beschäftigt sich mit dem Aufbau einer eIDAS-konformen CA. Daher wird der Gesetzestext der eIDAS im Mittelpunkt dieser Arbeit stehen. Die Verordnung versucht den elektronischen Transaktionen im Binnenraum einen gesetzlichen Rahmen zu verleihen und zu reglementieren. Schwerpunkte dabei sind die elektronische Identifizierung, einfache, fortgeschrittene und qualifizierte Signaturen, einfache und qualifizierte Zertifikate, einfache und qualifizierte Vertrauensdiensteanbieter, einfache, fortgeschrittene und qualifizierte Siegel sowie einfache und qualifizierte Zeitstempel. Weiters wird auch explizit die Website-Authentifizierung über elektronische Identifizierungsmittel angesprochen.

3.1 Begriffsklärung

Die zuvor aufgezählten Begriffe werden nun nach eIDAS erklärt.

3.1.1 Elektronische Identifizierung

„‚Elektronische Identifizierung' ist der Prozess der Verwendung von Personenidentifizierungsdaten in elektronischer Form, die eine natürliche oder juristische Person oder eine natürliche Person, die eine juristische Person vertritt, eindeutig repräsentieren."[1] Diese Definition bezeichnet noch keinerlei Verfahren kryptographischer Art.

3.1.2 Signaturen

Die eIDAS-Verordnung unterscheidet zwischen einfachen, fortgeschrittenen und qualifizierten Signaturen. „‚Elektronische Signatur' sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet."[2] Auch hier gibt es keine weitere Definition zu Eindeutigkeit und Unverfälschbarkeit. Einfache elektronische Si-

[1] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 1

[2] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 10

gnaturen fallen aber auch nicht in den Anwendungsbereich der eIDAS bzw. sämtliche durch die eIDAS geregelten Authentifizierungsmöglichkeiten benötigen zumindest fortgeschrittene Signaturen, weswegen die einfachen Signaturen auch nicht weiter behandelt werden.

„‚Fortgeschrittene elektronische Signatur' ist eine elektronische Signatur, die die Anforderungen des Artikels 26 erfüllt."[3] Der Artikel 26 legt fest, dass die fortgeschrittene Signatur, „eindeutig dem Unterzeichner zugeordnet"[4] werden kann (Eindeutigkeit), „die Identifizierung des Unterzeichners"[5] ermöglicht (Identität), „der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann"[6] (Vertraulichkeit) und „eine nachträgliche Veränderung der Daten erkannt werden kann"[7] (Integrität).

„‚Qualifizierte elektronische Signatur' ist eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht."[8] Als Signaturerstellungseinheit wird die entsprechende Software und/oder Hardware zum Erstellen einer Signatur bezeichnet. Im Fall der österreichische Bürgerkarte ist dies die Bürgerkartensoftware, sowie das Kartenlesegerät und die eCard. Eine qualifizierte Signaturerstellungseinheit muss die Vertraulichkeit der Daten während des Signiervorgangs sicherstellen, sowie für geeignete Zufallszahlen sorgen, die Signatur vor Fälschungen schützen und die Signaturerstellungsdaten vor dem Zugriff anderer schützen (PIN).[9]

3.1.3 Zertifikate

„‚Zertifikat für elektronische Signaturen' ist eine elektronische Bescheinigung, die elektronische Signaturvalidierungsdaten mit einer natürlichen Person verknüpft und die mindestens den Namen oder das Pseudonym dieser Person bestätigt."[10] Das Zertifikat ist damit ein elektronischer Datensatz mit zumindest ID-Daten auf eine Datenbank mit dort hinterlegten personenbezogenen Daten. Deswegen ist laut eIDAS die Richtlinie 95/46/EG anzuwenden. Diese Richtlinie wurde bereits am 28. Mai 2018 durch die DSGVO ersetzt.[11]

„‚Qualifiziertes Zertifikat für elektronische Signaturen' ist ein von einem qualifizierten Vertrauensdienstean-

[3] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 11
[4] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 26 Buchstabe a
[5] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 26 Buchstabe b
[6] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 26 Buchstabe c
[7] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 26 Buchstabe d
[8] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 12
[9] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Anhang II
[10] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 14
[11] Europäische Kommission, Verordnung (EU) 2016/679 - DSGVO Artikel 94

bieter ausgestelltes Zertifikat für elektronische Signaturen, das die Anforderungen des Anhangs I erfüllt.“[12] Anhang I besagt, dass das qualifizierte Zertifikat als solches gekennzeichnet sein muss und eine Angabe des Mitgliedstaats, des VDA, sowie des Namens der Person oder Firma und dessen Registriernummer enthalten muss. Desweiteren muss auch der Name oder zumindest ein eindeutig zuordenbares Pseudonym des Unterzeichners enthalten sein. Das qualifizierte Zertifikat muss eine Gültigkeitsdauer besitzen und diese auch vorweisen können, eine dem VDA eindeutige ID enthalten und mit der fortgeschrittenen Signatur oder Siegel des qualifizierten VDAs signiert sein. Außerdem muss das Zertifikat die URL des Verteilservers, sowie „den Ort der Dienste, die genutzt werden können, um den Gültigkeitsstatus des qualifizierten Zertifikats zu überprüfen“[13] (CRL, OCSP, Certificate Transparency) bekanntgeben.

3.1.4 Siegel

„‚Elektronisches Siegel‘ sind Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen.“[14]
„‚Fortgeschrittenes elektronisches Siegel‘ ist ein elektronisches Siegel, das die Anforderungen des Artikels 36 erfüllt.“[15]
„‚Qualifiziertes elektronisches Siegel‘ ist ein fortgeschrittenes elektronisches Siegel, das von einer qualifizierten elektronischen Siegelerstellungseinheit erstellt wird und auf einem qualifizierten Zertifikat für elektronische Siegel beruht.“[16]
Siegel sind technisch mit Signaturen vergleichbar. Signaturen sind eher für natürliche Personen gedacht um Willenserklärung abzugeben. Siegel stehen in erster Linie Institutionen bzw. juristischen Personen zur Verfügung um einen Herkunftsnachweis (Authentizität) zu erbringen.[17] Ein Siegel ist juristisch gesehen, im Gegensatz zu einer Signatur, keine Einverständniserklärung zum zugrundeliegenden Dokument!

3.1.5 Signaturerstellungseinheit

„‚Elektronische Siegelerstellungseinheit‘ ist eine konfigurierte Software oder Hardware, die zum Erstellen eines elektronischen Siegels verwendet wird“[18]. „‚Qualifizierte elektronische Siegelerstellungseinheit‘ ist

[12] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 15
[13] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Anhang I
[14] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 25
[15] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 26
[16] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 27
[17] Bundesamt für Sicherheit in der Informationstechnik, Elektronische Signaturen, Siegel und Zeitstempel
[18] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 31

eine elektronische Siegelerstellungseinheit, die die Anforderungen des Anhangs II sinngemäß erfüllt“[19]. Der Anhang II stellt fest, dass die qualifizierten Signaturerstellungseinheiten die Vertraulichkeit, Einzigartigkeit und Fälschungssicherheit der Daten, sowie gegen eine Verwendung durch Dritte verlässlich schützen können muss[20].

3.1.6 Zeitstempel

„‚Elektronischer Zeitstempel‘ bezeichnet Daten in elektronischer Form, die andere Daten in elektronischer Form mit einem bestimmten Zeitpunkt verknüpfen und dadurch den Nachweis erbringen, dass diese anderen Daten zu diesem Zeitpunkt vorhanden waren.“[21]
„‚Qualifizierter elektronischer Zeitstempel‘ ist ein elektronischer Zeitstempel, der die Anforderungen des Artikels 42 erfüllt.“[22] Der Artikel 42 besagt, dass durch den qualifizierten Zeitstempel die „Möglichkeit der unbemerkten Veränderung der Daten nach vernünftigem Ermessen ausgeschlossen ist“[23], er „auf einer korrekten Zeitquelle, die mit der koordinierten Weltzeit verknüpft ist“[24] beruht (GPS, GALILEO, Funk- und Atomuhr und weitere) und dass er „mit einer fortgeschrittenen elektronischen Signatur unterzeichnet oder einem fortgeschrittenen elektronischen Siegel des qualifizierten Vertrauensdiensteanbieters versiegelt“[25] wird.

3.1.7 Vertrauensdiensteanbieter

„‚Vertrauensdiensteanbieter‘ ist eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt.“[26] Ein qualifizierter Vertrauensdiensteanbieter erbringt nur qualifizierte Vertrauensdienste und wurde von einer Aufsichtsstelle akkreditiert[27]. Ein Vertrauensdienst besteht aus der „Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln, und Diensten für die Zustellung elektronischer Einschreiben sowie von diese Dienste betreffenden Zertifikaten“[28], sowie der „Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung“[29] und der „Bewahrung

[19] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 32
[20] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Anhang II Absatz 1
[21] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 33
[22] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 34
[23] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 42 Absatz 1 Buchstabe a
[24] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 42 Absatz 1 Buchstabe b
[25] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 42 Absatz 1 Buchstabe c
[26] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 19
[27] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 20
[28] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 16 Buchstabe a
[29] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 16 Buchstabe b

von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten“[30]. Ein qualifizierter Vertrauensdienst erfüllt die Anforderungen der eIDAS.[31]

[30] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 16 Buchstabe c

[31] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 17

4 Aufbau eines Vertrauensdiensteanbieter (VDA)

Die eIDAS erlässt Regelungen für (gewöhnliche) VDA sowie zusätzliche Regelungen für qualifizierte VDA. Daraus leiten sich dann wie bereits in Kapitel 3 beschrieben normale, fortgeschrittene und qualifizierte Zertifikate, Siegel und Signaturen ab. Dabei wird versucht die PKI, die als staatliche Infrastruktur (meist qualifizierte VDA) benutzt wird von firmeninternen PKIs (fast ausschließlich einfache oder fortgeschrittene VDA) abzugrenzen. Die eIDAS bedient sich einiger Normen, unter anderem der ISO 29115 und der EN 319 411 um die technischen Voraussetzungen dafür zu schaffen.

4.1 (Gewöhnlicher) VDA

Gewöhnliche CAs sind berechtigt normale und fortgeschrittene Zertifikate auszustellen. Aufgrund dessen sind die daraus entstehenden Signaturen und Siegel niemals höher zu bewerten als fortgeschrittene Signaturen und Siegel. Ein normales Zertifikat hat keinerlei Anforderungen zu Personenbindung oder ähnliches und werden daher meist als reine E-Mail-Zertifikate, Maschinen- und PC-Zertifikate verwendet. Ein fortgeschrittenes Zertifikat zeichnet sich durch seine Personenbindung[1] aus. Die Authentizität der Identität der Person muss natürlich überprüft werden[2] und wird durch den Registration Officer übernommen. Dies wird im Firmenkontext meistens durch die IT-Abteilung übernommen. Diese VDA müssen auch Prozesse implementieren um gegebenenfalls Sicherheitsverletzungen und -vorkommnisse erkennen zu können und auch darauf reagieren zu können. Deshalb muss immer auch der Stand der Technik berücksichtigt werden[2]. Weiters müssen sie auch den jeweils zuständigen Aufsichtsbehörden und Datenschutzbehörden innerhalb von 24 Stunden nach Kenntnisnahme die Vorfälle melden[3].

[1] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 26
[2] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 19 Absatz 1
[3] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 19 Absatz 2

4.2 Qualifizierter VDA

Qualifizierte VDA sind der zentrale Punkt des eIDAS Vertrauenssystem (dargestellt in Abbildung 4.1). Sie erbringen die dargestellten Dienste. Die bereits bei den (gewöhnlichen) VDA beschriebenen Anforderungen gelten auch für qualifizierte VDA. Die zuständige Behörde für österreichische VDA ist die Telekom-Control-Kommission (TKK)[4]. Die TKK ist eine weisungfreie Kollegialbehörde[5] die laut Telekommunikationsgesetz (TKG) [6] von der Rundfunk und Telekom Regulierungs-GmbH (RTR) geleitet wird. Weiters werden qualifizierte VDA mindestens alle 24 Monate auf eigene Kosten von einer Konformitätsbewertungsstelle[7] (in Österreich z.B. die RTR[8] oder das Zentrum für sichere Informationstechnologie - Austria (A-SIT)[9]) geprüft. Die Aufsichtsstelle (Telekom-Control-Kommission) kann zusätzlich jederzeit einen Konformitätsbericht von einer Konformitätsbewertungsstelle (RTR) über einen VDA auf Kosten des VDA[10] anfordern.

4.2.1 Beginn der Tätigkeit als qualifizierter VDA

Um als VDA qualifizierte Zertifikate ausgeben zu können, muss der qualifizierte Status zuerkannt werden. Dazu legt der VDA der Aufsichtsstelle einen von der Konformitätsbewertungsstelle ausgestellten Konformitätsbewertungsbericht vor und erklärt die Absicht qualifizierte Vertrauensdienste erbringen zu wollen[11][12]. Sobald der qualifizierte Status der VDA zugewiesen wurde, kann dieser beginnen qualifizierte Zertifikate auszustellen[13]. Der qualifizierte VDA wird dann in eine Vertrauensliste aufgenommen[14][15]. Diese Vertrauensliste wird in Österreich auch von der RTR geführt[16]. Mit der Ausweisung eines VDAs in der Vertrauensliste ist dieser dazu berechtigt das EU-Vertrauenssiegel zu verwenden[17]. Qualifizierte VDA, die ein solches Siegel (Abbildung 4.2) verwenden, müssen auf ihrer Website auf die Vertrauensliste verlinken[18].

[4] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz § 12 Absatz 1
[5] RTR, Telekom-Control-Kommission – die weisungsfreie Kollegialbehörde
[6] Bundeskanzleramt, Telekommunikationsgesetz §116
[7] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 20 Absatz 2
[8] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz § 12 Absatz 2
[9] A-SIT, Konformitätsbewertungsstelle
[10] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 20 Absatz 2
[11] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 21 Absatz 1
[12] Servida, Beginn der Tätigkeit als qualifizierter VDA.
[13] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 21 Absatz 3
[14] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 22 Absatz 1
[15] Europäische Kommission, Durchführungsbeschluss (EU) 2015/1505
[16] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §12 Absatz 1
[17] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 23 Absatz 1
[18] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 23 Absatz 2

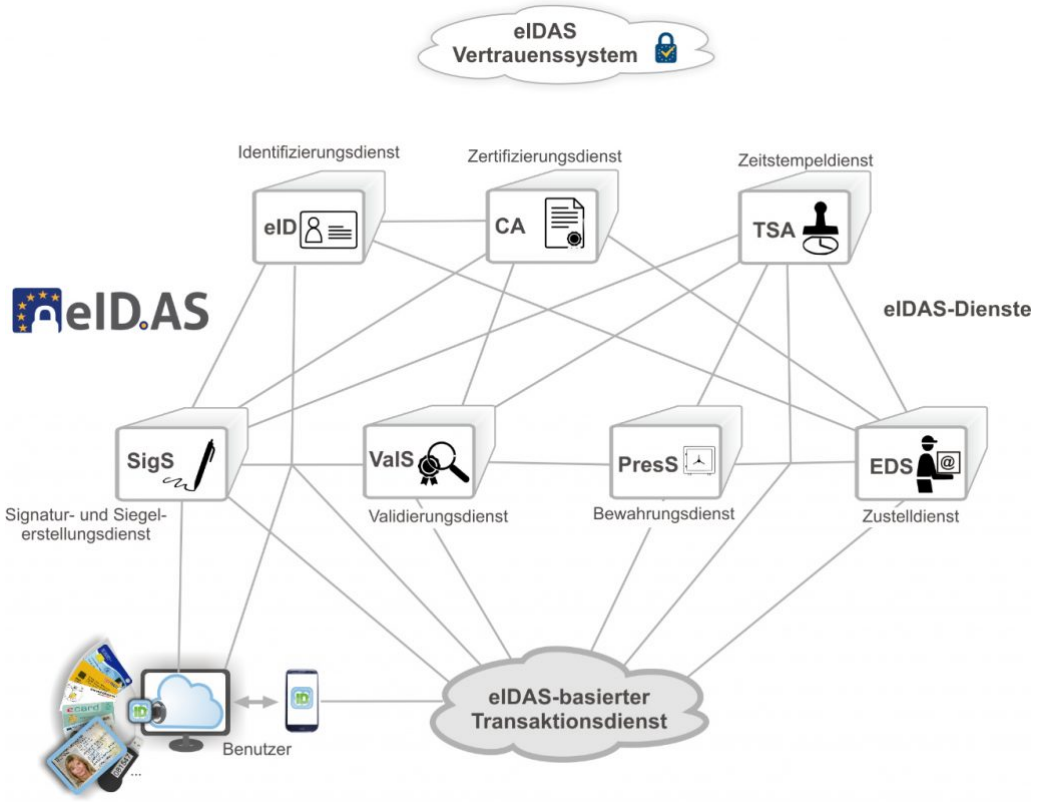

Abbildung 4.1: Eine Übersicht über die Vertrauensdienste, die die eIDAS behandelt. Diese werden noch innerhalb der Arbeit beschrieben.
Bildquelle: `https://blog.eid.as/de/eidas-oekosystem/`

4.2.2 Anforderungen an qualifizierte VDA

„Bei der Ausstellung eines qualifizierten Zertifikats für einen Vertrauensdienst überprüft der qualifizierte Vertrauensdiensteanbieter anhand geeigneter Mittel und im Einklang mit dem jeweiligen nationalen Recht die Identität und gegebenenfalls die spezifischen Attribute der natürlichen oder juristischen Person, der das qualifizierte Zertifikat ausgestellt wird.“[19] Der VDA kann die Identität durch die persönliche Anwesenheit der Person, ein elektronisches Identifizierungsmittel, das zuvor bereits durch persönliche Anwesenheit geprüft ausgestellt wurde, sowie eine qualifizierte Signatur, oder andere gleichwertige, national anerkannte Mittel prüfen[20]. Persönlich anwesende Personen benötigen zur Identifizierung einen amtlichen Lichtbildausweis oder einen gleichwertigen Nachweis[21]. Vertreter juristischer Personen müssen auch eine Vertre-

[19] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 24 Absatz 1
[20] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 24 Absatz 1 Buchstabe a-d
[21] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §3

Abbildung 4.2: Das EU-Vertrauenssiegel, welches berechtigte VDA tragen dürfen.
Bildquelle: Benutzer FlippyFlink auf Wikimedia Commons: `https://commons.wikimedia.org/wiki/File:Eu-trustmark-logo-eIDAS.jpg`

tungsbefugnis vorlegen[22]. Ein qualifizierter VDA muss die Aufsichtsstelle (TKK) über alle Änderungen und Einstellung ihrer Vertrauensdienste informieren[23].

Anforderungen an Personal und Unterauftragsnehmer

Sowohl das Personal, wie auch Unterauftragsnehmer müssen über erforderliches Fachwissen, Zuverlässigkeit, Erfahrung und Qualifikation verfügen. Weiters müssen sie die Vorschriften zum Schutz personenbezogener Daten kennen und können auf europäisch oder international anerkannten Normen basierende Verwaltungs- und Managementverfahren anwenden[24]. Als dementsprechende Normen eignen sich vor allem die Normen der ISO 27000 Familie, beispielsweise die Norm ISO 27001 (IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen) sowie die Norm ISO 27005 (Informationsicherheit Risikomanagement). Das erforderliche Fachwissen muss abgesehen von der allgemeinen EDV-Ausbildung unter anderem auch Wissen in den Bereichen Sicherheitstechnologien, Kryptographie, PKI und diversen einschlägigen Vorschriften beinhalten[25]. Dieses Fachwissen kann durch den Besuch einer einschlägigen HTL oder einer einschlägigen FH, sowie durch ein einschlägiges Studium oder eine fachlich einschlägige Tätigkeit von zumindest drei Jahren erworben werden[26]. „Die Zuverlässigkeit ist jedenfalls bei Personen nicht gegeben, die wegen einer mit Vorsatz begangenen strafbaren Handlung zu einer Freiheitsstrafe von mehr als einem Jahr oder wegen strafbarer Handlungen gegen das Vermögen oder gegen die Zuverlässigkeit von Urkunden und Beweiszeichen zu einer Freiheitsstrafe von mehr als drei Monaten verurteilt wurden“[27]. Der VDA stellt sicher, dass personenbezogene Daten gemäß der Verordnung (EU) 2016/679 des Europäi-

[22] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §8 Absatz 1
[23] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 24 Absatz 2 Buchstabe a
[24] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 24 Absatz 2 Buchstabe b
[25] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §2 Absatz 5
[26] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §2 Absatz 6
[27] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung § 2 Absatz 4

schen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO) behandelt werden[28].

Haftung und Absicherung der Systeme

Der VDA muss über entsprechendes Kapital verfügen um Schäden gemäß Artikel 13 der eIDAS begleichen zu können. Es wird empfohlen eine Haftpflichtversicherung abzuschließen[29]. Die Haftung eines VDA kann im Vorhinein weder ausgeschlossen noch beschränkt werden[30]. Der VDA verwendet „vertrauenswürdige Systeme und Produkte, die vor Veränderungen geschützt sind“[31]. Weiters werden diese Systeme „für die Speicherung der ihnen übermittelten Daten in einer überprüfbaren Form“ verwendet. Sie gewährleisten, dass die Daten nur mit Zustimmung der betreffenden Person öffentlich sind, nur befugte Personen Daten erstellen und verändern können und die Daten auf Echtheit geprüft werden können[32]. Der VDA ergreift auch „Maßnahmen gegen Fälschung und Diebstahl von Daten“[33]. Dies kann durch den Einsatz einer CA Software mit 4-Augen-Prinzip erfolgen. Dabei müssen immer mindestens zwei Mitarbeiter die Eingabe bestätigen. Das Vorgehen schützt so weitgehend vor Fehlern und vorsätzlichem Diebstahl und Veränderung. Die SVV sieht auch vor, die technischen Einrichtungen, die zur Erbringung von Vertrauensdiensten notwendig sind, von anderen Einrichtungen, Funktionen und Anwendungen zu trennen[34] (Sandboxing). Auch hat der VDA seine Einrichtungen vor unbefugtem Zutritt zu schützen[35]. Dies kann durch einen Wachdienst oder Alarmanlage erfolgen, aber auch durch Käfigbereiche im Rechenzentrum und Eintrittsprotokollierung.

Zertifikatsdatenbank

Der VDA erstellt und wartet eine Zertifikatsdatenbank[36]. Die Zertifikatsdatenbank muss in einem Format erstellt sein das für die Weiterführung durch die Aufsichtsstelle geeignet ist. Dieses Format darf auch nachträglich nicht verändert werden. Die Datenbank muss allgemein frei, unentgeltlich und ohne Identifizierung zugänglich sein. Durch die Datenbank muss es möglich sein, zu eruieren ob ein Zertifikat zu einem ge-

[28] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 24 Absatz 2 Buchstabe j - Die Richtlinie 95/46/EG wurde durch die DSGVO aufgehoben und ersetzt.
[29] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 24 Absatz 2 Buchstabe c
[30] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §11 Absatz 1
[31] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 24 Absatz 2 Buchstabe e
[32] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 24 Absatz 2 Buchstabe f
[33] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 24 Absatz 2 Buchstabe g
[34] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §2 Absatz 2
[35] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §2 Absatz 3
[36] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 24 Absatz 2 Buchstabe k

wissen Zeitpunkt widerrufen war[37]. Der VDA stellt seinen Signataren und Siegelerstellern eine geeignete Möglichkeit des Zertifikatswiderrufs zur Verfügung[38]. Dies geschieht meistens, wie in Unterabschnitt 2.1.7 erklärt, durch eine Hotline. „Die Zertifikatsdatenbank muss vor Fälschung, Verfälschung und unbefugtem Zugriff ausreichend geschützt sein“[39]. Die Aktualisierung hat zu Arbeitszeiten innerhalb von drei Stunden ab Bekanntwerden eines Widerrufs aktualisiert zu werden, außerhalb der Arbeitszeiten automatisiert innerhalb von sechs Stunden[40]. Die Zertifikatsdatenbank muss verlässlich verfügbar sein. Ein Ausfall von mehr als 30 Minuten ist als Störfall zu dokumentieren. Für geplante Ausfälle muss ein Ersatzsystem bereitgestellt werden. Fällt das Ersatzsystem aus muss innerhalb von einem Tag die Aufsichtsbehörde benachrichtigt werden[41]. Der VDA muss auf Ansuchen der Behörden und Gerichte diesen Zugang gewähren[42].

Beendigungsplan

Der VDA verfügt über einen fortlaufend aktualisierten Beendigungsplan[43]. Dieser ist notwendig, um im Falle einer Einstellung der Dienste des VDA dessen Dienstleistungen durch die Aufsichtsstelle (TKK) geordnet fortzuführen oder einstellen zu können[44]. Der VDA hat im Fall der Einstellung seiner Tätigkeiten dies der Aufsichtsstelle (TKK) mindestens drei Wochen im Vorraus mitzuteilen[45]. Der VDA kümmert sich darum, dass die Zertifikatsdatenbank von einem anderen qualifizierten VDA weitergeführt wird. Passiert dies nicht, wird die Datenbank von der Aufsichtsstelle weitergeführt. Die bereits ausgegeben Zertifikate werden, sollte dies im öffentlichen Interesse sein[46], widerrufen[47]. Weiters sind die Signataren und Siegelersteller unverzüglich zu informieren[48]. Im Fall einer Übernahme durch die Aufsichtsstelle dürfen die Angaben und Inhalte eines qualifizierten Zertifikats nachträglich geändert werden, sofern dies unbedingt notwendig ist[49].

[37] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §5 Absatz 1
[38] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §5 Absatz 2
[39] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §5 Absatz 3
[40] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §5 Absatz 4
[41] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §5 Absatz 5
[42] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §10 Absatz 1
[43] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 24 Absatz 2 Buchstabe i
[44] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 17 Absatz 4 Buchstabe i
[45] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §9 Absatz 1
[46] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §9 Absatz 3
[47] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §9 Absatz 2
[48] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §9 Absatz 4
[49] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §4 Absatz 3

Gebühren der VDA an die Aufsichtsstelle

Die SVV schreibt explizit Gebühren vor, die der VDA an die Aufsichtsstelle für folgende Tätigkeiten zu entrichten hat: Die Analyse der Konformitätsbewertungsberichte, die Überprüfung des qualifizierten VDA mit Unterscheidung ob dies durch einen sicherheitsrelevanten Anlassfall geschehen ist oder nicht, die Verleihung sowie der Entzug des Qualifikationsstatus, die Erteilung von Auflagen, die Überprüfung von Beendigungsplänen, die Weiterführung der Zertifikatsdatenbank, sowie die Führung der Vertrauensliste[50]. „Die Gebühren sind von der Aufsichtsstelle mit Bescheid vorzuschreiben“[51].

Dokumentation

Qualifizierte VDA „zeichnen alle einschlägigen Informationen über die von dem qualifizierten Vertrauensdiensteanbieter ausgegebenen und empfangenen Daten auf und bewahren sie so auf, dass sie über einen angemessenen Zeitraum, auch über den Zeitpunkt der Einstellung der Tätigkeit als qualifizierten Vertrauensdiensteanbieters hinaus, verfügbar sind, um insbesondere bei Gerichtsverfahren entsprechende Beweise liefern zu können und die Kontinuität des Dienstes sicherzustellen. Die Aufzeichnung kann in elektronischer Form erfolgen“[52]. Diese Dokumentation muss auf Anfrage Behörden und Gerichten zugänglich gemacht werden[53]. Die Dokumentation ist vom VDA 30 Jahre ab dem Ende der Gültigkeit eines qualifizierten Zertifikats zu speichern[54].

4.2.3 Interoperabilität

Ein vom Mitgliedsstaat bei der EU notifizierter VDA muss interoperabel sein[55]. Dazu muss zuerst geklärt werden ob man der Sicherheitsstufe *niedrig*, *substanziell*, oder *hoch* angehören möchte[56]. „Das Sicherheitsniveau ‚niedrig‘ bezieht sich auf ein elektronisches Identifizierungmittel im Rahmen eines elektronischen Identifizierungssystems, das ein begrenztes Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Überprüfungen — deren Zweck in der Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung besteht — gekennzeichnet ist“[57]. Sinnge-

[50] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §1 Absatz 1
[51] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §1 Absatz 2
[52] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 24 Absatz 2 Buchstabe h
[53] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §10 Absatz 1
[54] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §10 Absatz 3
[55] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 12 Absatz 1
[56] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 8 Absatz 1
[57] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 8 Absatz 2 Buchstabe a

mäßes gilt für die Stufen *substanziell* und *hoch*[58]. Die Durchführungsverordnung (EU) 2015/1502 legt im Detail die jeweiligen technischen Anforderungen zur Identifizierung natürlicher und juristischer Personen zu deren Verknüpfung mit elektronischen Systemen, die Validierung der Daten und Widerrufsmöglichkeiten fest[59]. Weiters bezieht sich die eIDAS auf die ISO 29115 um die technischen Anforderungen zu diesen Niveaus umsetzen zu können, sowie auf das Pilotprojekt STORK[60], ein Projekt zur Erprobung der eID. Um Interoperabel zu sein muss der VDA mit dem Knoten des jeweiligen Mitgliedsstaates kommunizieren können. „‚Knoten' ist ein Anschlusspunkt, der als Teil der Interoperabilitätsarchitektur für die elektronische Identifizierung an der grenzüberschreitenden Authentifizierung von Personen mitwirkt und der Datenübertragungen erkennen und verarbeiten oder an andere Knoten weiterleiten kann; er ermöglicht damit über eine Schnittstelle die Verbindung zwischen der nationalen elektronischen Identifizierungsinfrastruktur eines Mitgliedstaats und der nationalen elektronischen Identifizierungsinfrastruktur eines anderen Mitgliedstaats"[61]. Knotenbetreiber in Österreich ist das Bundesministerium für Inneres (BMI)[62]. Weitere Angaben bezüglich Interoperabilität finden sich in der eIDAS[63], der Durchführungsbeschlüssen 2015/1502[64] und 2015/1506[65], sowie im E-Government-Gesetz (E-GovG)[66].

4.3 Zertifikate und Signaturen

Digitale Signaturen sind ein von digitalen Zertifikaten abgeleitetes gewolltes Produkt. Die Signaturen bekunden Willenserklärungen und stellen die Authentizität und Integrität eines Dokuments sicher. Sie sind daher integraler Bestandteil einer PKI und auch in der eIDAS geregelt.

4.3.1 Rechtswirkung elekronischer Signaturen

„Eine qualifizierte elektronische Signatur hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift"[67]. „Eine qualifizierte elektronische Signatur erfüllt das rechtliche Erfordernis der Schriftlichkeit im Sinne des §886 ABGB"[68]. Das Allgemein bürgerliche Gesetzbuch (ABGB) schreibt dazu: „Ein Vertrag, für

[58] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 8 Absatz 2 Buchstabe b und c
[59] Europäische Kommission, Durchführungsverordnung (EU) 2015/1502 Anhang
[60] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Erwägungsgrund 16
[61] Europäische Kommission, Durchführungsbeschluss (EU) 2015/1506 Artikel 2 Absatz 1
[62] `https://eidas.bmi.gv.at/ms_connector/`
[63] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 12
[64] Europäische Kommission, Durchführungsverordnung (EU) 2015/1502.
[65] Europäische Kommission, Durchführungsbeschluss (EU) 2015/1506.
[66] Bundeskanzleramt, E-Government-Gesetz.
[67] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 25 Absatz 2
[68] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §4 Absatz 1

den Gesetz oder Parteiwille Schriftlichkeit bestimmt, kommt durch die Unterschrift der Parteien oder, falls sie des Schreibens unkundig oder wegen Gebrechens unfähig sind, durch Beisetzung ihres gerichtlich oder notariell beglaubigten Handzeichens oder Beisetzung des Handzeichens vor zwei Zeugen, deren einer den Namen der Partei unterfertigt, zustande“[69]. Dies bedeutet, dass eine digitale Signatur gleichwertig zu einer handschriftlichen Unterschrift ist und dadurch auch für Vertragsunterzeichnung verwendet werden kann. Weiters sind die qualifizierten elektronischen Signaturen eines in einem EU-Mitgliedstaat ausgestellten Zertifikats in allen anderen EU-Mitgliedsstaaten anerkannt[70]. Die eIDAS erklärt aber auch, dass eine Signatur nicht unbedingt qualifiziert sein muss um Rechtswirkung zu erlangen[71].

4.3.2 Anforderungen an elektronische Signaturen

Die eIDAS behandelt nur fortgeschrittene elektronische Signaturen, sowie qualifizierte Signaturen. Eine fortgeschrittene Signatur zeichnet sich dadurch aus, dass sie „dem Unterzeichner zugeordnet“ ist sowie dessen Identifizierung unterstützt, „unter Verwendung elektronischer Signaturerstellungsdaten erstellt [wird], die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann“ , und so mit den „unterzeichneten Daten verbunden [ist], dass eine nachträgliche Veränderung der Daten erkannt werden kann“[72]. Eine fortgeschrittene elektronische Signatur hat eine Personenbindung. Die qualifizierte Signatur zeichnet sich dadurch aus, dass sie, zusätzlich zu den vorigen Kriterien, noch von einem qualifizierten Zertifikat abgeleitet und von einer qualifizierten Signaturerstellungseinheit erstellt worden ist[73].

4.3.3 Anforderungen an qualifizierte Zertifikate

Qualifizierte Zertifikate müssen als qualifiziertes Zertifikat gekennzeichnet sein und eine Kennung des VDA und des Mitgliedstaats enthalten, den Namen der beantragenden Person, bei juristischen Personen zusätzlich die Registriernummer, den Namen oder ein eindeutiges Pseudonym des Unterzeichners, elektronische Signaturvalidierungsdaten, Beginn und Ende der Gültigkeitsdauer, die Seriennummer des Zertifikats, den Ort des Zertifikatsverteilservers, sowie die Orte der Validierungsstellen (u.a. CRL, OCSP, Certificate Transparency) enthalten[74]. Wird ein Pseudonym verwendet, gibt der VDA einem Dritten, der berechtigtes Interesse

[69] Bundeskanzleramt, Allgemein bürgerliches Gesetzbuch § 886
[70] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 25 Absatz 3
[71] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 25 Absatz 1
[72] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 26
[73] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 12
[74] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Anhang I

an der Identität glaubhaft machen konnte, die Identität preis[75]. Die eIDAS schließt aber explizit weitere Anforderungen an einen VDA aus[76]. Sollte das Zertifikat weitere Attribute besitzen, dürfen diese die Interoperabilität und die Anerkennung qualifizierter Signaturen nicht beeinflussen[77]. Sollte ein VDA neben qualifizierte Zertifikaten auch andere Zertifikate ausstellen, müssen für qualifizierte Zertifikate eigene Signatur- und Siegelerstellungsdaten verwendet werden[78]. „Bis zum Ablauf der Gültigkeit eines qualifizierten Zertifikats ist es zulässig, mit Ausnahme der Gültigkeitsdauer und der eindeutigen Kennung, dieselben Inhalte samt denselben Signatur- oder Siegelvalidierungsdaten neu zu zertifizieren und auf diese Weise ein neues Zertifikat auszustellen“[79]. Es wird ein neues, gültiges Zertifikat mit Hilfe des alten ausgestellt. Dies bedeutet unter anderem auch, dass der Besitzer eines Zertifikats die Zertifikatsverlängerung durchführen kann.

Widerrufung und Aussetzung von Zertifikaten

Die Widerrufung eines Zertifikats muss sofort in der Zertifikatsdatenbank registriert werden und spätestens 24 Stunden nach Einlagen des Ersuchens veröffentlicht werden. Dies gilt auch an Wochenenden und Feiertagen. Nach der Veröffentlichung ist der Widerruf sofort wirksam[80]. Ein widerrufenes Zertifikat ist ab diesem Zeitpunkt unumkehrbar ungültig zu machen[81]. Sofern ein Zertifikat nicht widerrufen wird, hat der VDA noch eine andere Möglichkeit um ein Zertifikat für ungültig zu erklären: Die Aussetzung. Der VDA muss davon Gebrauch machen wenn, „der Signatar, Siegelersteller oder sonstiger Berechtigter dies verlangt, die Aufsichtsstelle [...] die Aussetzung des Zertifikats anordnet, der qualifizierte VDA Kenntnis vom Ableben des Signatars, der Beendigung des Bestehens des Siegelerstellers oder sonst von der Änderung im Zertifikat bescheinigter Umstände erlangt, das Zertifikat auf Grund unrichtiger Angaben erwirkt wurde oder die Gefahr einer missbräuchlichen Verwendung des Zertifikats besteht“[82]. Die Aussetzung ist analog zur Widerrufung gleich vorzunehmen und innerhalb von 24 Stunden zu veröffentlichen[83]. Ein Zertifikat ist auch während seiner Aussetzung ungültig[84]. Die Dauer einer Aussetzung ist in der Zertifikatsdatenbank deutlich anzugeben[85]. Dieser Zeitraum darf nicht länger als zwei Wochen andauern[86]. Sollte ein Zertifikat ausgesetzt

[75] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §10 Absatz 2
[76] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 28 Absatz 2
[77] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 28 Absatz 3
[78] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §4 Absatz 1
[79] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §4 Absatz 2
[80] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 24 Absatz 3
[81] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 28 Absatz 4
[82] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §6 Absatz 1
[83] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §6 Absatz 2
[84] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 28 Absatz 5 Buchstabe a
[85] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 28 Absatz 5 Buchstabe b
[86] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §6 Absatz 3

werden, muss der Signatar oder Siegelersteller sofort verständigt werden. Wird die Aussetzung aufgehoben bleibt das Zertifikat weiter gültig, ansonsten wird es widerrufen[87]. Ein widerrufenes Zertifikat darf unter keinen Umständen wieder für gültig erklärt werden[88]. Der VDA muss den Aussetzungszeitraum dauerhaft in der Zertifikatsdatenbank vermerken und muss dies „elektronisch jederzeit allgemein zugänglich [...] veröffentlichen“[89]. Der VDA muss den Teilnehmern auch Informationen zu den jeweiligen widerrufenen und ausgesetzten Zertifikaten zur Verfügung stellen[90].

4.3.4 Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten

„Qualifizierte elektronische Signaturerstellungseinheiten müssen die Anforderungen des Anhang II erfüllen“[91]. Dieser Anhang besagt, wie bereits im Abschnitt „Signaturerstellungseinheit“ erwähnt, dass die Einheiten die Vertraulichkeit, Einzigartigkeit, Fälschungssicherheit der Signaturen gewährleisten und angemessen gegen eine Verwendung der Zertifikate durch Dritte schützen soll[92]. Diese Signaturerstellungseinheiten müssen die zu unterzeichnenden Daten vor dem Signieren dem Unterzeichner anzeigen und sie dürfen diese Daten nicht verändern[93]. „Das Erzeugen oder Verwalten von elektronischen Signaturerstellungsdaten im Namen eines Unterzeichners darf nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt werden“[94]. Dies ist beispielsweise bei der Handysignatur der Firma *a-trust* der Fall[95]. Weiters dürfen die VDA auch die Signaturerstellungsdaten verwenden um Sicherungskopien (Backup) zu erstellen sofern, diese Kopien das gleiche Sicherheitsniveau wie die Echtdaten aufweisen und nicht mehr als unbedingt notwendige Sicherheitskopien vorhanden seien[96]. Die Signaturerstellungseinheiten können sowohl vom VDA wie auch anderen Firmen erstellt werden (vgl. Bürgerkartensoftware von *a-trust*[97] und trustDesk basic von *IT Solution*[98]).

[87] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §5 Absatz 7
[88] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 28 Absatz 4
[89] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §6 Absatz 4
[90] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 24 Absatz 4
[91] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 29 Absatz 1
[92] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Anhang II Absatz 1
[93] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Anhang II Absatz 2
[94] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Anhang II Absatz 3
[95] A-SIT, Hintergrundinformationen
[96] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Anhang II Absatz 4
[97] `https://www.a-trust.at/de/signaturkarten/asign-premium`
[98] `https://www.itsolution.at/digitale-signatur-produkte/desktop/trustDesk.html`

Zertifizierung der qualifizierten elektronischen Signaturerstellungseinheiten

„Die Konformität qualifizierter elektronischer Signaturerstellungseinheiten mit den Anforderungen des Anhangs II wird von geeigneten, von den Mitgliedstaaten benannten öffentlichen oder privaten Stellen zertifiziert“[99]. Diese Firmen prüfen dann anhand entsprechender Normen[100] ob die Signaturerstellungseinheit den Status qualifiziert erhalten darf[101]. Eine Liste dieser öffentlichen und privaten Stellen stellen die Mitgliedsstaaten der EU-Kommission zur Veröffentlichung zur Verfügung[102]. Eine qualifizierte Signatureinheit wird durch einen Mitgliedsstaat von der EU-Kommission veröffentlicht[103].

4.3.5 Validierung der qualifizierten elektronischen Signaturen

Die „Gültigkeit einer qualifizierten elektronischen Signatur wird bestätigt, wenn“ das verwendete Zertifikat ein den Anforderungen des Anhangs I entsprechendes qualifiziertes Zertifikat, gültig und von einem qualifizierten VDA ausgestellt war, „die Signaturvalidierungsdaten den Daten entsprechen, die dem vertrauenden Beteiligten bereitgestellt werden,“ die Personenbindung dem Überprüfer korrekt dargestellt wird, ein etwaiges Pseudonym dem Überprüfer als solches angezeigt wird, die Signatur von einer qualifizierten Signaturerstellungseinheit erstellt wurde, der zu überprüfende Hashwert der Daten mit den Daten übereinstimmt, sowie dass eine Personenbindung und ein an die Signatur angehängter Hashwert überhaupt existierten[104]. Das zur Validierung verwendete System muss das korrekte Ergebnis der Überprüfung anzeigen und auch etwaige Sicherheitsprobleme anzeigen[105].

Qualifizierter Validierungsdienst für qualifizierte Signaturen

„Qualifizierte Validierungsdienste für qualifizierte elektronische Signaturen können nur von qualifizierten Vertrauensdiensteanbietern erbracht werden, die [...] eine Validierung gemäß Artikel 32 Absatz 1 durchführen und [...] es vertrauenden Beteiligten ermöglichen, das Ergebnis des Validierungsprozesses automatisch in zuverlässiger und effizienter Weise mit Bestätigung durch die fortgeschrittene elektronische Signatur oder das fortgeschrittene elektronische Siegel des Anbieters des qualifizierten Validierungsdienstes zu erhalten“[106]. Dies bedeutet sie müssen die Validierung nach den im vorigen Absatz erwähnten Kriterien

[99] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 30 Absatz 1
[100] Europäische Kommission, Durchführungsbeschluss (EU) 2016/650
[101] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 30 Absatz 3 Buchstabe a
[102] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 30 Absatz 2
[103] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 31 Absatz 1 und 2
[104] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 32 Absatz 1
[105] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 32 Absatz 2
[106] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 33 Absatz 1

durchführen und das Ergebnis signiert an den Anfragenden übermitteln. Um die Interoperabilität der Signaturen und Siegel im Binnenmarkt gewährleisten zu können, wurde ein Durchführungsbeschluss erlassen, der weitere detaillierte Angaben zu Signaturformaten und Validierungsmöglichkeiten gibt[107].

4.3.6 Anforderungen an einen qualifizierten Bewahrungsdienst

Ein Bewahrungsdienst wird weder in der eIDAS, noch im SVG definiert. Jedoch definiert die eIDAS einen VDA als Dienst, der zur „Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten“[108] herangezogen werden kann. „Ein qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen kann nur von qualifizierten Vertrauensdiensteanbietern erbracht werden, die Verfahren und Technologien verwenden, die es ermöglichen, die Vertrauenswürdigkeit der qualifizierten elektronischen Signatur über den Zeitraum ihrer technologischen Geltung hinaus zu verlängern“[109]. Dabei handelt es sich um einen Dienst der gewährleisten soll, dass Signaturen, die mit einem mittlerweile als unsicher geltenden Algorithmus erstellt wurden, weiters durch den VDA zwiebelartig signiert werden, um eine Authentizität der Dokumente sicherzustellen[110]. Weiters wurde mir mit einer persönlichen, authentischen Nachricht mitgeteilt, dass sich, aufgrund fehlender Normen und einer Durchführungsrechtsakte, die „praktische Anwendung und Relevanz dieses qualifizierten Dienste (sic!) in sehr engen Grenzen halten“ wird[111].

4.4 Elektronische Siegel

Die Anforderungen an elektronische Siegel, Siegelerstellungseinheiten, Bewahrung und Validierung sind analog zu den qualifizierten elektronischen Signaturen zu sehen. Der Artikel über Siegelerstellungseinheiten verweist auf die jeweiligen Artikel zu den Signaturerstellungseinheiten[112], der Artikel über Bewahrung und Validierung der Siegel verweist genauso auf die jeweiligen Artikel[113]. Die Artikel zu Rechtswirkung[114], Anforderung an fortgeschrittene Siegel[115] und qualifizierte Zertifikate für elektronische Siegel[116], sowie der

[107] Europäische Kommission, Durchführungsbeschluss (EU) 2015/1506
[108] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 3 Absatz 16 Buchstabe c
[109] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 34 Absatz 1
[110] Vogt, Auswirkungen der eIDAS-Verordnung auf das Records Management der öffentlichen Verwaltung in Deutschland, Kapitel 5.5.5, Die Gesetze beziehen sich auf deutsches Recht, die technischen Abläufe sind aber generell anwendbar.
[111] Kustor, Bewahrungsdienst laut eIDAS
[112] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 39
[113] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 40
[114] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 35
[115] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 36
[116] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 38

verwiesene Anhang[117] weisen sogar den gleichen Wortlaut auf. Lediglich wurde „qualifizierte elektronische Signatur“durch „elektronisches Siegel“ ersetzt. Interessanterweise wird im SVG ein Abschnitt „Elektronische Signaturen und elektronische Siegel“ genannt, jedoch wird im entsprechenden Paragraphen nur die Rechtswirkung qualifizierter elektronischer Signaturen geregelt, die Siegel werden gar nicht erwähnt[118].

4.5 Elektronischer Zeitstempeldienst

Die Artikel zur Rechtswirkung ist bereits wie bei den elektronischen Siegeln mit dem exakt gleichen Wortlaut geschrieben[119]. Der Zeitstempeldienst bezieht seinen Zeitstempel von „einer korrekten Zeitquelle, die mit der koordinierten Weltzeit verknüpft ist“[120]. Der Zeitstempel muss derart mit den Daten verknüpft sein, dass ein Ändern bemerkt werden muss[121](Hashing) und wird mit einer fortgeschrittenen elektronischen Signatur oder dem Siegel eines qualifizierten VDA verknüpft[122].

4.6 Zustellung elektronischer Einschreiben

Die Rechtswirkung ist analog zur Rechtswirkung der qualifizierten elektronischen Signaturen zu sehen[123]. Qualifizierte Dienste für die Zustellung müssen von qualifizierten VDA erbracht werden[124]. Weiters stellt der VDA die Identität des Absenders und Empfängers vor der Übermittlung fest[125]. Der VDA signiert oder versiegelt die zu übermittelnden Daten mit einer qualifizierten elektronischen Signatur oder Siegel und zeigt Daten, die notwendigerweise vor der Übermittlung geändert werden müssen, deutlich an[126]. Sämtliche Zeitangaben der Übermittlung (Absenden, Empfangen, Ändern) werden durch qualifizierte Zeitstempel erbracht[127].

[117] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Anhang III
[118] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §4
[119] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 41
[120] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 42 Absatz 1 Buchstabe b
[121] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 42 Absatz 1 Buchstabe a
[122] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 42 Absatz 1 Buchstabe c
[123] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 43
[124] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 44 Absatz 1 Buchstabe a
[125] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 44 Absatz 1 Buchstabe b und c
[126] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 44 Absatz 1 Buchstabe d und e
[127] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 44 Absatz 1 Buchstabe f

4.7 Zertifikate für Website-Authentifizierung

„Qualifizierte Zertifikate für die Website-Authentifizierung müssen die Anforderungen des Anhangs IV erfüllen“[128]. Anhang IV ist analog zu Anhang I betreffend qualifizierte Zertifikate für elektronische Signaturen und Anhang III betreffend qualifizierte Zertifikate für elektronische Siegel[129].

[128] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Artikel 45 Absatz 1
[129] Europäische Kommission, Verordnung (EU) Nr. 910/2014 - eIDAS Anhang IV

5 Conclusio

Die Voraussetzungen und das Regelwerk zu elektronischen Authentifizierungsmaßnahmen mit Zertifikaten wird in der EU grundsätzlich über die eIDAS getroffen. Weiters gibt es einige Durchführungsrechtsakte dazu, jedoch hat die EU noch nicht alle Durchführungsrechtsakte beschlossen, die auch in der Verordnung vorgesehen wären. Hier gibt es noch Handlungsspielräume. Weiters gibt es auch noch nationale Gesetze und Verordnungen, im Fall von Österreich das SVG und die SVV.

Die Verordnung behandelt sämtliche Prozesse recht oberflächlich. Die spezifischeren Durchführungsrechtsakten, Gesetze und weiteren Verordnungen gehen zwar technisch in die Tiefe, jedoch wird organisatorisch recht wenig geregelt. Dies geschieht vor allem durch die angegebenen Normen.

Eine PKI zeichnet sich durch ihre Integrität aus. Diese muss natürlich an allen Stellen der Prozesse gewährleistet sein. Dabei zeichnet sich ab, dass die technischen Prozesse relativ sicher sind, wohl aber Zertifikate durch menschliche Fehler oder absichtliche Irreführung in falsche Hände geraten können (Alice beantragt als Bob ein Zertifikat). Ein Staat mit einem qualifizierten VDA, sowie eine großer Konzern muss dabei auf die Fälschungssicherheit der physischen Ausweise vertrauen. Kleinere Firmen haben hier, obwohl sie nur fortgeschrittene elektronische Zertifikate ausstellen, einen Vorteil, da sich die Mitarbeiter meist persönlich kennen und der Registration Officer bei der Zertifikatsausstellung nicht zwingend auf Ausweise vertrauen muss.

Die elektronischen Siegel sind ein Versuch elektronische Signaturen und Authentizität auch in den Unternehmensbereich zu bringen. Dabei wurde versucht die alten Wachsstempel nachzubilden. Die elektronischen Konstrukte beinhalten Vertretungsbefugnisse einer Firma oder Institution und können somit auch von Unternehmen eingesetzt werden. Allerdings werden die Siegel im SVG so gut wie nicht behandelt, was entweder auf fehlendes Verständnis zu den Siegeln oder fehlendes Interesse schließen lässt.

Die Interoperabilität ist laut eIDAS kein unbedingt notwendiges Kriterium für einen qualifizierten VDA. Die Interoperabilität wird erst notwendig, sollte der Mitgliedsstaat diesen VDA der EU notifizieren und darüber seine eID abwickeln wollen.

Ein österreichisches Unikum betrifft auch die TKK und die RTR. Die Aufsichtsstelle laut eIDAS ist die

weisungsfreie TKK, eine Konformitätsbewertungsstelle ist unter anderem die RTR. Der RTR kommt laut SVG und SVV auch weiterführende Aufgaben in diesem Bereich zu[1][2]. Interessant ist aber der Umstand, dass die Geschäftsführung der TKK (Aufsichtsstelle) der RTR (Konformitätsbewertungsstelle) obliegt[3].

5.1 Weiterführende Arbeiten

Die Arbeit beschreibt die Anforderungen an einen qualifizierten VDA laut eIDAS, wobei keine Rücksicht genommen wird, ob dieser VDA interoperabel sein soll oder nicht. Weiterführend können daher die Anforderungen an einen zwingend interoperabel arbeitenden VDA bzw. die Anforderungen an das eID System auf staatlicher Ebene untersucht werden. Weiters wäre die stärkere Einbeziehung der angegebenen Normen angebracht um eine detaillierte Übersicht zu diesem Thema zu bekommen.

[1] Bundeskanzleramt, Signatur- und Vertrauensdienstegesetz §§ 13 bis 14

[2] Bundeskanzleramt, Signatur- und Vertrauensdiensteverordnung §1 Absatz 4

[3] Bundeskanzleramt, Telekommunikationsgesetz §116 Absatz 2

Abbildungsverzeichnis

Glossar

A-SIT Zentrum für sichere Informationstechnologie - Austria

ABGB Allgemein bürgerliche Gesetzbuch

AD Active Directory

AES Advanced Encryption Standard

BMI Bundesministerium für Inneres

BSI Bundesamt für Sicherheit in der Informationstechnik

CA Certification Authority

CP Certificate Policy

CRL certificate revocation list

DES Data Encryption Standard

DSGVO Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG

E-GovG E-Government-Gesetz

eIDAS Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

OCSP online certificate status protocol

PKI Public Key Infrastructure

RA registration authority

RTR Rundfunk und Telekom Regulierungs-GmbH

SigG Signaturgesetz

SVG Signatur- und Vertrauensdienstegesetz

SVV Signatur- und Vertrauensdiensteverordnung

TKG Telekommunikationsgesetz

TKK Telekom-Control-Kommission

TSA Zeitstempeldienst

VDA Vertrauensdiensteanbieter

Literatur

A-SIT. *Hintergrundinformationen*. URL: https://www.buergerkarte.at/hintergrund-informationen.html. letzter Zugriff: 2019-04-10.

– *Konformitätsbewertungsstelle*. URL: https://www.a-sit.at/bestaetigung-evaluierung/konformitaetsbewertungsstelle/. letzter Zugriff: 2019-04-10.

Bundesamt für Sicherheit in der Informationstechnik. *Elektronische Signaturen, Siegel und Zeitstempel*. 19. Feb. 2019. URL: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/Elektronische_Signaturen_Siegel_und_Zeitstempel/Elektronische_Signaturen_Siegel_und_Zeitstempel_node.html. letzter Zugriff: 2019-02-19.

Bundeskanzleramt. *Allgemein bürgerliches Gesetzbuch*. 1812. URL: https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001622. letzter Zugriff: 2019-04-03.

– *E-Government-Gesetz*. 1. März 2004. URL: https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230. letzter Zugriff: 2019-04-17.

– *Signatur- und Vertrauensdienstegesetz*. 8. Juli 2016. URL: https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009585. letzter Zugriff: 2019-01-12.

– *Signatur- und Vertrauensdiensteverordnung*. 8. Juli 2016. URL: https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009619. letzter Zugriff: 2019-01-18.

– *Signaturgesetz*. 19. Aug. 1999. URL: https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10003685&FassungVom=2016-06-30. letzter Zugriff: 2018-12-10.

– *Telekommunikationsgesetz*. 19. Aug. 2003. URL: https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849. letzter Zugriff: 2019-03-31.

Eckert, Claudia. *IT-Sicherheit : Konzept - Verfahren - Protokolle*. München : Wien : Oldenbourg, 2003. ISBN: 3486272055.

ETSI. *Draft ETSI EN 319 411-2*. Techn. Ber. Juni 2015. URL: https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.00.06_20/en_31941102v020006a.pdf. letzter Zugriff: 2019-04-24.

Europäische Kommission. *Durchführungsbeschluss (EU) 2015/1505*. 9. Sep. 2015. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1554036444949&uri=CELEX:32015D1505. letzter Zugriff: 2019-03-31.

– *Durchführungsbeschluss (EU) 2015/1506*. 9. Sep. 2015. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32015D1506. letzter Zugriff: 2019-04-10.

– *Durchführungsbeschluss (EU) 2016/650*. 25. Apr. 2016. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016D0650. letzter Zugriff: 2019-04-10.

– *Durchführungsverordnung (EU) 2015/1502*. 9. Sep. 2015. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32015R1502. letzter Zugriff: 2019-04-17.

– *Durchführungsverordnung (EU) 2015/806*. 22. Mai 2015. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32015R0806. letzter Zugriff: 2019-04-10.

– *EG-Richtlinie 1999/93/EG*. 13. Dez. 1999. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A31999L0093. letzter Zugriff: 2019-01-13.

– *Verordnung (EU) 2016/679 - DSGVO*. 27. Apr. 2016. URL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016R0679. letzter Zugriff: 2019-02-17.

– *Verordnung (EU) Nr. 910/2014 - eIDAS*. 23. Juni 2014. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910. letzter Zugriff: 2019-03-31.

Europäische Union. *Durchführungsrechtsakte und delegierte Rechtsakte*. 14. Feb. 2017. URL: https://ec.europa.eu/info/law/law-making-process/adopting-eu-law/implementing-and-delegated-acts_de. letzter Zugriff: 2019-04-03.

– *Verordnungen, Richtlinien und sonstige Rechtsakte*. 24. Mai 2018. URL: https://europa.eu/european-union/eu-law/legal-acts_de. letzter Zugriff: 2019-01-12.

ISO/TC 68/SC 2. *ISO 21188:2018 - Public key infrastructure for financial services*. Techn. Ber. Apr. 2018. URL: https://www.iso.org/standard/63134.html. letzter Zugriff: 2019-01-18.

Kustor, Mag. Peter. *Bewahrungsdienst laut eIDAS*. E-Mail Korrespondenz. 12. Apr. 2019. URL: https://lithilion.at/download/Bewahrungsdienst_laut_eIDAS.eml.

Richtervereinigung. *Stufenbau der Rechtsordnung*. 2019. URL: https://richtervereinigung.at/justiz/rechtssystem/stufenbau-der-rechtsordnung/. letzter Zugriff: 2019-01-18.

RTR. *Telekom-Control-Kommission – die weisungsfreie Kollegialbehörde*. URL: https://www.rtr.at/de/tk/TKK. letzter Zugriff: 2019-04-07.

Servida, Andrea. *Beginn der Tätigkeit als qualifizierter VDA*. Auskunft des Head of eSign der EU. 30. Apr. 2019. URL: https://lithilion.at/download/Reply_to_Mr_Paul_Lackner_Ares_2019_2482298.pdf.

Vogt, Theresa. „Auswirkungen der eIDAS-Verordnung auf das Records Management der öffentlichen Verwaltung in Deutschland“. Magisterarb. Fachhochschule Potsdam, 3. Aug. 2015. URL: https://opus4.kobv.de/opus4-fhpotsdam/files/1008/Masterarbeit_Vogt%2CTheresa-ohne+adr.pdf.