Rechtliche und technische Aspekte der E-Akte in der Anwaltschaft

Johannes Lahann

Zusammenfassung. Das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten ("ERV-Gesetz" oder auch "E-Justice") vom 10.10.2013 erlaubt ab 01.01.2022 als Kommunikationsweg zu den Gerichten einzig den elektronischen Rechtsverkehr.
Für Rechtsanwälte bedeutet dies, dass Schriftsätze bei Gericht ausschließlich über elektronischen Weg eingereicht werden dürfen. Ein erster Schritt beinhaltet die Einführung besonderer elektronischer Anwaltspostfächer durch die Bundesrechtsanwaltskammer, welche bereits bis 01.01.2016 genutzt werden sollen.
Der Beitrag befasst sich mit den daraus resultierenden Konsequenzen sowohl im Bereich der Kommunikationswege zwischen Anwälten und Gerichten als auch in der internen Organisation einer Anwaltskanzlei. Insbesondere sollen die rechtlichen Anforderungen und die daraus ableitbaren technischen Herausforderungen diskutiert und ein Lösungsansatz erarbeitet werden.

Schlüsselwörter: ERV-Gesetz, Elektronische Akte, Sicherheit und Datenschutz, Integrität, Anwaltskanzlei, Gerichte

1 Einleitung

Motivation

Der digitale Fortschritt ist in der heutigen Welt nicht mehr wegzudenken. Dies beinhaltet auch die Digitalisierung innerhalb der Justiz. Durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten (ERV-Fördergesetz) vom 10.10.2013 erhält diese Entwicklung einen weiteren deutlichen Schub. In naher Zukunft soll die Kommunikation mit den Gerichten ausschließlich elektronisch ablaufen. Dazu soll bis zum 01.01.2016 ein besonderes elektronisches Anwaltspostfach eingeführt werden und bis zum 01.01.2022 soll die Übermittlung der vorbereitenden Schriftsätze sowie deren Anlagen zwischen Rechtsanwälten und den Gerichten nur noch auf elektronischen Wege stattfinden. Damit das Gesetz erfolgreich umgesetzt werden kann, bedarf es Anpassungen sowohl in den Kommunikationswegen zwischen Anwälten und Gerichten als auch in der internen Organisation in der Anwaltskanzlei. Insbesondere ist eine Wechsel auf eine digitale Datenverwaltung zwar nicht rechtlich gefordert, aber allein aus Effizienzgründen sinnvoll. Dabei ergeben sich technische und rechtliche Bedingungen welche miteinbezogen werden müssen.

Zielstellung

Das Ziel dieser Arbeit ist die Ausarbeitung der technischen und rechtlichen Aspekte der elektronischen Akte innerhalb der Anwaltskanzlei. Insbesondere sollen:

- die sich neu ergebenen rechtlichen Herausforderungen innerhalb der Kommunikation zwischen Anwalt und Client sowie Anwalt und Gericht als auch innerhalb der internen Organisation definiert werden. Dabei soll vor allem das neue elektronische Anwaltspostfach näher beleuchtet werden.
- aus den rechtlichen Aspekten, die technischen Problemstellungen abgeleitet und unter zu Hilfenahme aktueller Literatur verschiedene Lösungsansätze herausgefiltert werden.
- Vorschläge gegeben werden, wie durch Einführung der E-Akte die Arbeitsabläufe in der Anwaltschaft und mit dem Mandanten sowie vor Gericht beschleunigt werden können.

Gliederung

Im ersten Teil der Arbeit (Kapitel 2) wird die aktuelle Gesetzeslage bzgl. des Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vorgestellt. Dabei werden insbesondere die Begriffe Elektronisches Übermittlungswege, Elektronische Dokumente, Elektronische Formulare sowie das Elektronische Schutzschriftenregister näher erörtert. Kapitel 3 beschreibt die Auswirkungen des Gesetzes auf die Anwaltskanzleien und die daraus resultierenden technischen Herausforderungen. In Kapitel 4 wird der technische Hintergrund geschaffen, um die in Kapitel 3 erörterten Anforderungen technisch zu diskutieren. Dabei werden unter anderem aktuelle Verfahren zur Authentifizierung, Autorisierung und zur Erstellen von digitalen Signaturen vorgestellt. Kapitel 5 befasst sich mit der visuellen und technischen Umsetzung des Anwaltspostfachs(folgt eine kurze Erklärung was genau). Abschließend werden in Kapitel 6 die Ergebnisse der vorherigen Kapitel zusammengefasst und Ergänzungen sowie ein Ausblick gegeben.

2 Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten

Das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten ändert die Prozessordnungen und Verfahrensgesetze für die Gerichte grundlegend. Bisher konnten die Länder selbst über die Einführung der elektronischen Verordnungswege entscheiden. Dies wird durch eine bundesweit eintretende Regelung am 01.01.2022 ersetzt, die ausschließlich elektronischen Kommunikationswege für Anwälte und Behörden zu den Gerichten erlaubt. Gleichzeitig wurden an mehreren Stellen Vorschriften zur Barrierefreiheit in die Gesetze eingefügt. In diesem Kapitel werden die wesentlichen gesetzlichen Änderungen vorgestellt. Dazu werden als Quellen im wesentlichen Bacher (2014a)[1] und Carstens (2015)[2] herangezogen.

Elektronisches Anwaltspostfach

Nach § 31a der Bundesrechtsanwaltordnung (BRAO) müssen Rechtsanwälte ab dem 1. Januar 2016 für die Gerichte über ein besonderes elektronisches Anwaltpostfach erreichbar sein. Die besonderen elektronischen Anwaltspostfächer werden von der Bundesrechtsanwaltskammer für die Rechtsanwälte eingerichtet. Eine detaillierte Beschreibung des elektronischen Anwaltspostfach folgt in Kapitel 5.

Elektronische Übermittlungswege

Die Vorschrift des § 130a der Zivilprozessordnung (ZPO) sieht vor, dass vorbereitende Schriftsätze und deren Anlagen, schriftlich einzureichende Anträge und Erklärungen der Parteien sowie schriftlich einzureichende Auskünfte, Aussagen, Gutachten, Übersetzungen und Erklärungen Dritter ab dem 01.01.2018 flächendeckend als elektronisches Dokument bei Gericht eingereicht werden können. Während elektronische Dokumente an das Gericht bisher mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen sein müssen, wird es zukünftig möglich sein, elektronische Dokumente auch ohne qualifizierte elektronische Signatur zu übermitteln, wenn hierfür einer der nachfolgenden, vom Gesetzgeber im Hinblick auf die die Authentizität und die Integrität des übermittelten elektronischen Dokuments als sicher bezeichneten Übermittlungswege genutzt werden. Als sichere Übermittlungswege benennt das Gesetz in § 130a Abs. 4 ZPO erstens den Postfach und Versanddienst eines De-Mail Kontos, zweitens die Nutzung des elektronischen Anwaltspostfach und der elektronischen Poststelle

[1] Klaus Bacher (2014a). "Das Gesetz zur Förderung des elektronischen Rechtsverkehr". In: 998-1003.

[2] Andreas Carstens (2015). "Grundlagen für eine barrierefreie IT in der Justiz". In: *Barrierefreie Informationssysteme: Zugänglichkeit für Menschen mit Behinderung in Theorie und Praxis* 6, S. 177.

des Gerichts, drittens den Übermittlungsweg zwischen einem hierfür eingerichteten elektronischen Postfach einer Behörde und der elektronischen Poststelle des Gerichts und viertens sonstige bundeseinheitliche Übermittlungswege, die durch Rechtsverordnung festgelegt werden.

Elektronische Dokumente

Mit der flächendeckenden Einführung des elektronisches Rechtsverkehrs wird es möglich werden, sowohl die Schriftsätze der Verfahrensbeteiligten und Erklärungen Dritter als auch gerichtliche Dokumente(Urteile, Beschlüsse, Protokolle,etc..) als elektronisches Dokument zu übermitteln. Nach § 174 Abs. 3 Satz 4 ZPO werden Rechtsanwälte und andere Prozessbevollmächtigte zudem verpflichtet, ab dem 01.01.2018 einen sicheren Zugang im Sinne des § 130a ABS.4 ZPO für Zustellungen elektronischer Dokumente durch das Gericht zu eröffnen. Daher werden elektronische Dokumente des Gerichts die bisherigen Papierdokumente zunehmend ersetzen. § 191a ABs. 3 Satz 1 GVG sieht vor, dass die Texte barrierefrei zugänglich und nutzbar sein müssen. Daneben können auch Fotos und Skizzen beigefügt werden. Für elektronische Dokumente, die an das Gericht übermittelt werden, sieht § 130a Abs.2 Satz 1 ZPO vor, dass sie für die Bearbeitung durch das Gericht geeignet sein müssen. Die technischen Rahmenbedingungen werden durch die Rechtsverordnung festgelegt. Insbesondere soll eine Bearbeitungs- und Suchfunktion der elektronischen Dokumente bereitgestellt werden. Daher soll die Übermittlung elektronischer Dokumente als Scans bzw. Bilder auf zu Beweiszwecken eingescannte Urkunden, Nachweise und Belege begrenzt werden.

Elektronische Formulare

Nach § 130c ZPO kann das Bundesministerium der Justiz für die elektronische Kommunikation mit den Gerichten ab dem 1. Juli 2014 durch Rechtsverordnung elektronische Formulare einführen. Die Rechtsverordnung kann bestimmen, dass die in den Formularen enthaltenen Angaben ganz oder teilweise in strukturierter maschinenlesbarer Form zu übermitteln sind. Die Formulare sind auf einer in der Rechtsverordnung zu bestimmenden Kommunikationsplattform im Internet zur Nutzung bereitzustellen. Die Rechtsverordnung kann bestimmen, dass eine Identifikation des Formularverwenders abweichend von § 130 a Absatz 3 ZPO auch durch Nutzung des elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes erfolgen kann. Elektronische Formulare sind nach § 191a Abs. 3 Satz 1 bzw. Satz 3 GVG blinden oder sehbehinderten Personen barrierefrei zugänglich und nutzbar zu machen.

Elektronisches Schutzschriftenregister

Die Vorschrift des § 945a Abs. 1 ZPO sieht vor, dass die Länder ein zentrales länderübergreifendes elektronisches Register für Schutzschriften führen.

Schutzschriften sind vorbeugende Verteidigungsschriftsätze gegen erwartete Anträge auf Arrest oder einstweilige Verfügung . Hierzu regelt die Verordnungsermächtigung in § 945 b ZPO, dass das Bundesministerium der Justiz durch Rechtsverordnung die näheren Bestimmungen über die Barrierefreiheit festlegt.

Auch dieses neue Regelung sieht ab 1.1.2017 eine Nutzungspflicht für Anwälte vor. Nach § 49c BRAO ist der Rechtsanwalt verpflichtet Register ausschließlich über das elektronische Schutzschriftenregister einzureichen.

3 Vorgang

Anhand eines typischen Ablaufs in einer Kanzlei wird im folgenden kurz dargestellt, welche Interaktionen mit einer Akte in einem Prozess durchlaufen werden. Normalerweise wird von einem Mitarbeiter die Post empfangen, und die enthaltenen Dokumente in die entsprechenden Akten einsortiert. Dem Anwalt werden die aktuellen Akten in sein Postfach abgelegt. Dabei sind die neusten Informationen noch nicht abgeheftet. Nach Erhalt der Akte kann der Anwalt mit seiner Arbeit beginnen. Oftmals werden die Briefe diktiert und von einem Mitarbeiter geschrieben. Dabei ist ein nicht zu unterschätzender Aufwand die Formatierung der Briefe so wie die Ergänzung der Kennnummern. Die Kommunikation der Anwälte mit den Mandanten erfolgt im Regelfall über Postverkehr. Nach Absprache ist auch die Nutzung von Emails denkbar. Während der Bearbeitung eines Prozesses unterscheidet der Anwalt zwischen Hand und Gerichtsakte. Dabei beinhaltet die Gerichtsakte die Dokumente, welche vom Anwalt an das Gericht gesendet werden und ist von dem Mandanten zu jeder Zeit einsehbar. Die Handakte übergibt der Anwalt dem Mandanten nach Ablauf des Prozesses nach seiner Bezahlung.

4 Was muss geändert werden?

5 Anforderungen

5.1 Besonderes elektronisches Anwaltspostfach § 31a Brao

Ab 01.01.2016 muss von der Bundesrechtsanwaltskammer für jeden Rechtsanwalt ein elektronisches Anwaltspostfach bereitgestellt werden.

Erreichbarkeit Das elektronische Anwaltspostfach muss für jeden Rechtsanwalt erreichbar sein und darf nicht von diesem ignoriert werden. Elektronische Zustellungen werden zwar nur gegen Empfangsbekenntnis erfolgen. Jedoch ist der Anwalt zu dieser nach § 14 BORA verpflichtet. Die Empfangsbekenntnis kann bis 01.01.2018 auch auf altmodischen Wege erfolgen. Danach muss es auf elektronischen Wege in strukturierte maschinenlesbarer Form stattfinden.

Zugangssicherung Um die Zugangssicherung zu gewährleisten, darf der Zugang nur nach Authentifizierung durch zwei von einander unabhängigen Sicherungsverfahren erfolgen. Als geeignete Sicherungsmittel sind z.B. eine Chipkarte sowie die Eingabe eines PIN denkbar.

Zugangsberechtigung Gemäß § 31a Abs. 2 BRAO können unterschiedliche Zugangsberechtigungen für Rechtsanwälte und für andere Personen eingerichtet werden. So kann in Kanzleien mit mehreren Anwälten der Posteingang bei einem/r Sekretär/in erfolgen und der oft etablierte Arbeitsablauf kann somit

beibehalten werden. Je nach Signatur des Dokuments(siehe Abschnitt Signatur) kann auch die Versendung an das Gericht von dem/r Sekretär/in übernommen werden.

Barrierefreiheit Nach § 31a Abs. 1 Satz 1 BRAO soll das besondere elektronische Anwaltspostfach barrierefrei ausgestaltet werden. Das Bundesministerium der Justiz wird durch § 31b BRAO ermächtigt, die Einzelheiten zur Barrierefreiheit durch Rechtsverordnung zu regeln.

5.2 Elektronische Dokumente

Erzeugung Jede Kanzlei muss bis zum Inkrafttreten der Nutzungspflicht am 1. Januar 2022 Schriftsätze Anlagen und sonstige Dokumente in elektronischer Form zu erstellen. Aus Sicherheitsgründen (siehe Anforderungen Revisionssicherheit, Authentizität & Integrität) ist es empfehlenswert die Dokumente im pdf-Format einzureichen. Papierdokumente von Mandanten können eingescannt und in PDF-Form gespeichert werden

Signatur Signatur durch besonderes elektronisches Anwaltspostfach Dateisignatur am Dokument selbst angebracht Container-Signatur

Versand Der Versand elektronischer Dokumente an das Gericht ist normalerweise an bestimmte Fristen gebunden. Die Führung der Akten in der Kanzlei kann sowohl elektronisch als auch in Papierform erfolgen und ist dem Anwalt freigestellt. Die elektronische Authentifizierung eines einzureichendem Dokumentes muss zwingend durch den Anwalt passieren. (vgl. Zugangsberechtigung). Nach der Authentifizierung kann der Versand von einen anderen Kanzleimitarbeiter übernommen werden. Die Übermittlung des Dokuments muss, wie in Abschnitt elektronische Übermittlungswege beschrieben, auf einen sicheren Übermittlungsweg erfolgen. Dies ist z.B. durch die Nutzung des elektronischen Anwaltspostfach gegeben.

Barrierefreiheit

Vertraulichkeit Nur Menschen mit den notwendigen Berechtigungen dürfen Zugriff auf die Information erhalten. Dies beinhaltet sowohl die Einsicht einzelner Dokumente als auch die Übersicht über die vorhandenen Informationen. Berechtigungen müssen sich je nach Aktenbestand unterscheiden und können sich über einen Zeitraum ändern. Außerdem muss gegebenenfalls zwischen Lese und Bearbeitungsrechten unterschieden werden.

Authentizität und Integrität Der Autor eines Dokumentes muss klar erkennbar sein. Dabei darf es nicht möglich sein sich als andere Person auszugeben. Ein Dokument darf nur verändert werden, wenn die notwendigen Berechtigungen vorliegen.

Revisionssicherheit Falls ein Dokument über einen Zeitraum verändert wurde, muss die Historie der Veränderungen einsehbar sein. Dabei sollte für jede Änderung Zeitpunkt und Autor der Änderung vorliegen. Des weiteren sollten vergangene Änderungen gegebenenfalls rückgängig gemacht werden können.

Verbindlichkeit Wie im vorigen Abstritt beschrieben muss der Autor eines Dokumentes zu jedem Zeitpunkt eindeutig identifiziert werden können. Daraus folgt, dass es nicht möglich ist die Autorenschaft eines Dokumentes abzustreiten.

Verfügbarkeit So wie die notwendigen Berechtigungen vorliegen, sollte ein Dokument zu jedem Zeitpunkt einsehbar sein.

Schutz personenbezogener Daten Trotz der gegebenen Informationen soll die elektronische Akte nicht genutzt werden können um die Arbeitszeiten zu überwachen. So sollen z.B. die Änderungszeitpunkte der Dokumente durch die Richter verborgen bleiben. Diese Anforderung steht im direkten Konflikt mit der Revisionssicherheit.

Langzeitarchivierung Die obengenannten Anforderungen müssen von der erstmaligen Anlage an erfüllt werden. Dabei ist es nicht ausreichend, dass diese bis zum Abschluss des Verfahrens gegeben werden.

6 technische Aspekte

Authentifizierung

Es existieren viele verschiedene Authentifizierungsverfahren, welche sich in ihrer Komplexität unterscheiden. Die einfachsten Verfahren erwarten die Eingabe von Benutzername und Passwort. Allerdings gehören diese auch zu den unsichersten Verfahren. Damit eine Authentifizierung möglich ist, müssen eindeutige die Person identifizierende Eingaben vorliegen. Diese lassen sich in drei Kategorien unterscheiden.

- Wissen: Eingabe einer geheimen Information, beispielsweise ein PIN.
- Gegenstand: Auslesen eines Gegenstandes,z.B. eine Karte oder ein USB-Token
- Attribut: Ein Indentifikationsmerkmal der Person, beispielsweise das Augenmuster oder der Fingerabdruck eines Menschen.

Multi-factor authentication Je nach Authentifizierungsverfahren reicht die Eingabe einer Information (Single Factor Authentication) oder es müssen mehrere Faktoren eingegeben werden (Multi Factor Authentication). Dabei kann jeder Faktor die Person eindeutig identifizieren. Damit eine Authentifizierung

erfolgreich ist müssen jedoch alle Eingaben korrekt sein. Bei der Multi Factor Authentication werden aus Sicherheitsgründen Faktoren aus unterschiedlichen Kategorien gewählt. Ein typisches Beispiel ist die Authentifizierung an einem Bankautomat. Dazu ist die Eingabe eines PINS, sowie einer Bankkarte notwendig. Nur wenn beide Faktoren vorliegen und zueinander passen ist die Authentifizierung erfolgreich.

Mutual authentication erlaubt dem Benutzer zu verifizieren, dass die Authentifizierung an dem gewünschten System erfolgreich war, sodass er nur nach einer erfolgreichen Authentifizierung seine sicherheitskritischen Daten ein gibt. *Phishing Attacks* zielen darauf ab, Benutzern eine Authentifizierung vorzutäuschen, sodass sie danach z.B. ihr Passwort eingeben, obwohl sie nicht mit dem gewünschten System verbunden sind.

Shared Secrets (Passwords) *Shared Secrets* wie Passwörter oder PINS sind die meist genutzten Schlüssel um Sicherheit zu gewährleisten und Zugriff auf Online Portale erlauben. Ein Problem dabei ist jedoch, dass die Erfahrung gezeigt hat, dass Menschen dazu neigen schlechte Passwörter zu wählen, sie leicht offen legen, oder ihre Passwörter vergessen. Dies macht es einfach für einen Spezialisten das Passwort zu stehlen.

One time passwords (otp) Ein *One time password* ist ein Passwort, welches sich für jede Verwendung ändert. Es werden zwei grundlegende Möglichkeiten unterschieden, wie ein *One time password* funktioniert:

- Es wird eine Liste von Tans generiert, die zwischen dem Benutzer und System geteilt wird. Bei jeder Verwendung wird der Benutzer nach einer der Tans gefragt.
- Bei jeder Passworteingabe wird das Passwort vom Benutzer neu generiert und vom System verifiziert. Dabei kann das Passwort z.B. eine Funktion von der aktuellen Zeit sein, welches der Benutzer und das System teilen.

SSL/TLS Protokoll SSL/TLS sind Protokolle, die für den sicheren Austausch von Informationen zwischen Client und Server genutzt werden. Im folgenden wird kurz der Vorgang eines *SSL Handshake* unter Nutzung des *RSA exchange* Algorithmus beschrieben:

1. *Client Hello:* Der Client sendet für die SSL Kommunikation notwendige Informationen wie z.B. die SSL Version.
2. *Server Hello:* Der Server antwortet mit für den Client relevanten Informationen, u.a. mit dem SSl Zertifikat des Servers (Public Key).
3. Der Client überprüft das Zertifikat auf Korrektheit. Ist dies gegeben, erzeugt der Client den Schlüssel für die spätere Kommunikation und verschlüsselt ihn mit dem *Public Key* des Servers.
4. Der Server entschlüsselt den Schlüssel mit dem Private Key.
5. Für die Session wird der Session Schlüssel zur Verschlüsselung der Kommunikation genutzt.

Autorisierung/Zugriffskontrolle

Der Sinn und Zweck von Zugriffskontrolle ist die erlaubten Operationen auf einen Datensatz einzuschränken. In der Informatik beschränken Zugangsberechtigungen sowohl die erlaubten Operationen eines Nutzers als auch die eines Programms. In diesem Sinne soll Zugriffskontrolle alle Operationen, welche die Sicherheit einschränken, verhindern. Im folgenden werden verschiedene Grundsätze der Zugriffskontrolle beschrieben.

Voraussetzung Damit Zugriffskontrolle möglich ist, muss das System den Benutzer erkennen. Dies bedeutet, dass sich der Benutzer in einem ersten Schritt in dem System anmelden muss(vgl. Authentifizierung). Vor jeder Anfrage muss erneut überprüft werden, ob der Benutzer die nötigen Berechtigungen besitzt.

Zugriffssteuerungsmatrix Die Zugriffssteuerungsmatrix ist ein abstraktes Sicherheitskonzept, welches jedem Benutzer zu jedem Objekt gewisse Rechte zuweist. Das bedeutet insbesondere, dass für jedes Objekt unterschiedliche Berechtigungen gelten können. Es wurde 1971 von Butler W. Lampson eingeführt(Quelle).

Rollenbasierte Zugriffskontrolle Role Based Access Control (RBAC; deutsch: Rollenbasierte Zugriffskontrolle) ist in Mehrbenutzersystemen oder Rechnernetzen ein Verfahren zur Zugriffssteuerung und -kontrolle auf Dateien oder Dienste. Das RBAC-Modell wurde 1992 von D.F. Ferraiolo und D.R. Kuhn beschrieben[1] und 2004 als ANSI-Norm 359-2004 verabschiedet.

Die alternative Methode, einem realen Benutzer (User) direkt Rechte und Zugriffe auf verschiedene Systeme zu geben, stellte sich durch die steigende Zahl von Benutzern als unübersichtlich und daher fehlerträchtig dar. Das auf Benutzerrollen basierende Konzept soll nun die Rechte anhand von Arbeitsprozessen abstrahieren.

Bei der rollenbasierten Zugriffskontrolle werden den Benutzern des Computers oder Netzwerks Rollen zugeordnet. Benutzer können dabei mehrere Benutzerrollen besitzen. An eine Rolle sind beispielsweise 1 bis n Gruppenzugehörigkeiten gebunden. Je nach Rollenzuordnung des Benutzers (und den damit verbundenen Gruppenzugehörigkeiten) erteilt oder sperrt das System dann das Zugriffsrecht auf Betriebsmittel. Häufig werden vor allem Lesen, Schreiben und Ausführen von Dateien mittels RBAC kontrolliert; das Verfahren ist jedoch nicht darauf beschränkt.

Militär Sicherheitsbestimmung Das Prinzip der Militär Sicherheitsbestimmung ist es Informationen basierend auf ihrer Sicherheitsstufe zu klassifizieren. Es wird unterschieden zwischen

- unclassified

- restricted
- confidential
- secret
- topsecret

Jeder Information ist ein Tupel aus Rang und Kompartiment zugeordnet. Dabei bestimmt das Kompartment zu welchen Projekten die Information gehört. Eine Person kann auf Informationen bis zu einer gewissen Sicherheitsstufe zugreifen. Die Zugangsberechtigung einer Person wird ebenfalls als Tupel aus Rang und Kompartiment dargestellt.

Bell-LaPdula Modell Das *Bell-LaPdula Modell* ähnelt dem *Military security policy*. Zusätzlich werden unterschiedliche Schreib- und Leserechte definiert. Insbesondere kann kein Datensatz höherer Sicherheitsstufe gelesen und kein Datensatz mit niedriger Sicherheitsstufe geschrieben/bearbeitet werden.

Conditional Policies *Conditional Policies* bedeutet, dass Sicherheitskriterien zusätzlich zu den bereits genannten Punkten auch abhängig von dem aktuellen Kontext des Benutzers sein können. Beispielsweise kann der Zugang zu speziellen Daten, nur von einem bestimmten Ort und auch nur für einen gewissen Zeitraum freigeschaltet werden.

Biba Modell Das *Biba Model* dient der Wahrung der Integrität. Es beinhaltet das Daten einer niedrigeren Sicherheitsstufe wie der Benutzer nicht gelesen und Daten einer höheren Sicherheitsstufe nicht geschrieben werden dürfen. Es ist damit eine Umkehrung des *Bell-LaPdula Modells*.

Separation of duty Das Prinzip *Separation of duty* besagt, dass für eine wichtige Aufgabe immer mehr als eine Person verantwortlich sind. Dies beinhaltet das wichtige Entscheidungen nur unter Zustimmung aller Verantwortlichen getroffen werden dürfen. Dadurch sollen sowohl Fehler als auch Machtmissbrauch verhindert werden

Chinese Wall Policy Nach dem *Chinese Wall Policy* darf ein Benutzer nur auf Daten zugreifen, die nicht im Konflikt mit anderen Daten stehen, welche dem Benutzer zur Verfügung stehen. Dadurch soll ein Interessenkonflikt des Benutzers vermieden werden.

Principle of Least Privilege Das *Principle of Least Privilege* besagt, dass Personen nur auf diejenigen Daten zugreifen dürfen, die für ihre Arbeit zwingend erforderlich sind.

Digitale Signaturen

Eine digitale Signatur, auch digitales Signaturverfahren, ist ein asymmetrisches Kryptosystem, bei dem ein Sender mit Hilfe eines geheimen Signaturschlüssels (dem Private Key) zu einer digitalen Nachricht (d. h. zu beliebigen Daten) einen Wert berechnet, der ebenfalls digitale Signatur genannt wird. Dieser Wert ermöglicht es jedem, mit Hilfe des öffentlichen Verifikationsschlüssels (dem Public Key) die nichtabstreitbare Urheberschaft und Integrität der Nachricht zu prüfen. Um eine mit einem Signaturschlüssel erstellte Signatur einer Person zuordnen zu können, muss der zugehörige Verifikationsschlüssel dieser Person zweifelsfrei zugeordnet sein.

Mit digitalen Signaturen lassen sich sichere elektronische Signaturen (fortgeschrittene elektronische Signaturen gem. § 2 Nr. 2 SigG bzw. qualifizierte elektronische Signaturen gem. § 2 Nr. 3 SigG) erzeugen. Die Begriffe digitale Signatur und elektronische Signatur sind jedoch nicht inhaltsgleich: Erstens müssen (zumindest fortgeschrittene) elektronische Signaturen nicht zwangsläufig auf digitalen Signaturen basieren; zweitens ist digitale Signatur ein mathematischer bzw. technischer Begriff, während elektronische Signatur ein juristischer Begriff ist.

Gesetzliche Normen Die Bundesnetzagentur veröffentlicht jedes Jahr eine Liste mit Mindestanforderungen für kryptographische Algorithmen für die Erzeugung qualifizierter elektronischer Signaturen.[2] In der „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung“ vom 18. Januar 2012 werden als geeignete digitale Signaturverfahren RSA , DSA und DSA-Varianten die auf elliptischen Kurven basierend (z. B. EC-DSA, EC-KDSA, EC-GDSA) empfohlen. Zu jedem dieser Verfahren werden die Mindestlängen für die Schlüssel sowie weitere Anforderungen an die Parameter und die Hashfunktion angegeben. [3]

RSA In der modernen Kryptologie hat sich die RSA – Verschlüsslung als eine der sichersten Methoden durchgesetzt. Sie wird heute in wichtigen Bereichen wie im Bankenwesen (z.B. bei der Verschlüsslung von Geheimzahlen) eingesetzt.

Leonard Euler entdeckte eine mathematische Regel, die für die RSA – Verschlüsselung grundlegend ist. Wählt man zwei positive Primzahlen p und q mit $p \neq q$, dann gilt:

$$m^{s(p-1)(q-1)} \mod n = m \tag{1}$$

$m, n \in \mathbb{N}$ mit $n <= n$
Das heißt also, wenn man die Potenz $m^{s(p-1)(q-1)}$ durch n teilt, so erhält man als Rest dieser Division wieder die Basis m. Diese Gültigkeit ist grundlegend für die Verschlüsselung mit dem RSA – Verfahren (siehe Abschnitt 3).

Wollen zwei Teilnehmer sich gegenseitig eine Nachricht senden, welche für die Öffentlichkeit geheim bleiben soll, die also nur von den beiden entschlüsselt werden können soll, so müssen diese zuerst einige Schlüssel festlegen. Zunächst erhält jeder Teilnehmer zwei große, voneinander verschiedene Primzahlen p und q. Je größer p und q sind, desto schwieriger ist die verschlüsselte Nachricht zu knacken. Das Produkt n der beiden Primzahlen ($n = pq$) kann als öffentlicher Schlüssel verwendet werden. Das heißt, dieser kann unverschlüsselt und in aller Öffentlichkeit ausgetauscht werden, ohne dass eine Entschlüsselung einfacher wird. Die Teilnehmer suchen nun nach einer Zahl $e \in \mathbb{N}$ die teilerfremend von der Zahl $(p-1) * (q-1)$ ist, das heißt (p-1)*(q-1) und e haben außer 1 keine gemeinsamen Teiler. Dies ist durch einfaches Probieren schnell herauszufinden. Auch die Zahl e kann im Endeffekt als öffentlicher Schlüssel verwendet werden. Ebenfalls einfach ist es , eine Zahl $d \in \mathbb{N}$ zu finden, für die gilt:

$$e * d = s(p-1)(q-1) + 1 \tag{2}$$

$s \in \mathbb{N}$
Dabei kann die Zahl s so gewählt werden, wie es für d am besten passt, s ist also eine beliebige natürliche Zahl. Nun kann d als geheimer Schlüssel verwendet werden. Entscheidend an dieser Formel ist, dass es einfach für einen Spion ist d zu bestimmen, wenn er e, p und q kennt. Es ist aber, vor allem bei großen p und q, nahezu unmöglich nur durch Kenntnis der öffentlichen Schlüssel n und e den geheimen Schlüssel d herauszufinden.

DSA : wurde von NIST entwickelt und eignet sich speziell für Signaturen. Es ist eine Modifizierte Form des ELGamal Kryptographiesystems und basiert auf dem Problem der Diskreten Logarithmen. *Schlüsselerzeugung:*

1. Erzeuge eine Primzahl p der Länge $512 - 1024$ Bit, sodass das Diskrete Logarithmen Problem in Z_p schwer ist
2. Erzeuge eine Primzahl q mit der Länge 160 Bit und q — (p-1)
3. Wähle ein $a \in Z_p$ das eine q te Wurzel von 1 $\mod p$ ist, d.h. es gelte $a^q = 1(\mod p)$.
4. Schlüsselmenge K des DSA ist:

$$K = (p, q, a, b) : b = a^q \mod p, 0 <= a <= q - 1 \tag{3}$$

Wobei die Werte p, q und b den öffentlichen Schlüssel bilden und a der private Schlüssel ist

Signieren:

Für $x \in \{0,1\}^*, K = (p, q, a, b)$ und eine (geheime) Zufallszahl $k : 1 <= k <= q - 1$ definieren wir die Signatur:

$$\begin{aligned} sig_K(x,k) &= (y,d) - mit \\ y &= (a^k \mod p) \mod q \\ d &= (SHA-1(x) + a*y)k^{-1} \mod q \end{aligned} \tag{4}$$

Wenn $y = 0$ oder $d = 0$, wähle ein neues k

Verifizieren:

Für $x \in 0,1^*$ und $(y,d) \in Z_p * Z_p$, muss die Verifikation folgende Berechnungen durchführen:

$$\begin{aligned} e1 &= SHA-1(x)d^{-1} \mod q \\ e2 &= y*d^{-1} \mod q \\ ver_K(x,(y,d)) = true <=> (a^{e1} * b^{e2} \mod p) &\mod q = y \end{aligned} \tag{5}$$

Sicherer Datenspeicher in der Cloud

Sicherer Datenspeicher auf dem Smartphone

Literatur

Ahn, Gail-Joon und Ravi Sandhu (2000). "Role-based Authorization Constraints Specification". In: *ACM Trans. Inf. Syst. Secur.* 3.4, S. 207–226. ISSN: 1094-9224. DOI: 10.1145/382912.382913.

Bacher, Klaus (2014a). "Das Gesetz zur Förderung des elektronischen Rechtsverkehr". In: 998-1003.

— (2014b). "Elektronischer Rechtsverkehr in der Anwaltskanzlei". In: 1053-1055.

Bao, Feng, Cheng-Chi Lee und Min-Shiang Hwang (2006). "Cryptanalysis and improvement on batch verifying multiple {RSA} digital signatures". In: *Applied Mathematics and Computation* 172.2. Special issue for The Beijing-HK Scientific Computing Meetings, S. 1195–1200. ISSN: 0096-3003. DOI: http://dx.doi.org/10.1016/j.amc.2005.03.016.

Bertino, Elisa, Elena Ferrari und Vijay Atluri (1999). "The Specification and Enforcement of Authorization Constraints in Workflow Management Systems". In: *ACM Trans. Inf. Syst. Secur.* 2.1, S. 65–104. ISSN: 1094-9224. DOI: 10.1145/300830.300837.

Carstens, Andreas (2015). "Grundlagen für eine barrierefreie IT in der Justiz". In: *Barrierefreie Informationssysteme: Zugänglichkeit für Menschen mit Behinderung in Theorie und Praxis* 6, S. 177.

"Elektronische Akten: Anforderungen und technische Lösungsmöglichkeiten". In:

"Elektronischer Rechtsverkehr in Verfahren ohne Anwaltszwang – der Justizgewährungsanspruch des Bürgers als praktischer und theoretischer Störfaktor?" In:

"Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten" (2013). In: Teil 1.NR. 62.

Rivest, R. L., A. Shamir und L. Adleman (1983). "A Method for Obtaining Digital Signatures and Public-key Cryptosystems". In: *Commun. ACM* 26.1, S. 96–99. ISSN: 0001-0782. DOI: 10.1145/357980.358017.

Robling Denning, Dorothy Elizabeth (1982). *Cryptography and Data Security*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc. ISBN: 0-201-10150-5.

Smid, Miles E (1998). "Digital Signature Standard". In:

Smith, Richard E. (2002). *Authentication: From Passwords to Public Keys*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc. ISBN: 0-201-61599-1.