Irrtum - Identifizieren versus Authentisieren

Die Begriffe „Identifizieren“ und „Authentisieren“ sollten so präzise differenziert verstanden und verwendet werden, wie Besitz und Eigentum oder Fahrzeughalter und Fahrzeuglenker. Ansonsten können sich daraus Missverständnisse, falsche Vorstellungen über den zugrunde liegenden Sachverhalt oder gar eine nicht sachgerechte juristische Schlussfolgerung ergeben.

Daniel Muster, www.it-rm.ch, 8003 Zürich

Inhaltsverzeichnis

I Einleitung

Selbst in der Fachliteratur wird ein Wirrwarr betreffend die Begriffe „Identifizieren“ und „Authentisieren“ veranstaltet. Dies gilt auch bei Vorträgen zu IT-Sicherheit. Infolge dieses Durcheinanders werden falsche Assoziationen über den zugrunde liegenden Sachverhalt geweckt, was die Wahrscheinlichkeit einer nicht sachgerechten Beurteilung enorm erhöht. In dieser Abhandlung werden diese und weitere Begriffe im Kontext zur IT-Sicherheit zuerst definiert, die Differenzen herausgeschält und Beispiele für nicht sachgerechte Bundesbestimmungen aufgeführt.

Zusätzlich wird im Kapitel VII dargelegt, warum beim eGovernment andere Sicherheitsstufen im Bereich des Authentisierens wenig sinnvoll sind, als diejenigen, welche per ZertES und Art. 59a OR vorgegeben sind. Dies soll auch als kritische Bemerkung zur Vorlage E-ID-Gesetz verstanden sein, welche nun vom Bundesparlament verabschiedet werden soll.

Diese Abhandlung wurde für ein breites Zielpublikum verfasst, u.a. für Juristen, welche für Sicherheitsfragen in der IT aufgeschlossen sind, wie auch für IT-Fachleute, welche sich für die rechtlichen Aspekte der IT interessieren. Wenn ein breites Publikum angesprochen werden soll, ist es aus didaktischen Gründen nur folgerichtig, dass Ungenauigkeiten aus allen Fachbereichen in dieser Abhandlung enthalten sind. Zum „Miteinander“ zwischen IT und Recht dazu treffend aus BUCHLEITNER/RABL:

> Technik und Recht sprechen nicht nur unterschiedliche Sprachen, die jeweiligen Protagonisten haben idR wenig für das Gegenüber über. Juristen halten Techniker für naiv, weil diese meinen, dass ein funktionierendes System einfach „funktioniert“. Techniker halten wiederum Juristen für unnötig und kompliziert, weil diese idR meinen, dass manches, das funktioniert, trotz allem „nicht geht“.

II Begriffswahl und sicherheitstechnische Mittel

Definition 1: „Identifizieren“ soll folgende zwei Bedeutungen haben:

- Der Vorgang zur Feststellung der Identität einer natürlichen Person, wie dies z.B. bei der Einvernahme einer Person durchgeführt wird (z.B. Art. 143 Abs. 1 Bst. a und Abs. 3, Art. 260 Abs. 1, Art. 262 Abs. 1 StPO).
- Feststellen, wer *in der realen Welt* ein Ereignis oder einen Vorfall verursacht hat (z.B. Art. 255 Abs. 1 StPO, DNA-Analyse).

Das Identifizieren wird anhand biometrischer Verfahren vorgenommen. Z.B. Vergleich mit dem Passfoto, DNA, Sprachproben oder mit Fingerabdrücken, kurzum mit der Suche nach Übereinstimmung mit biometrischen Daten, wie dies beim Erkennungsdienst sattfindet, siehe dazu TRECHSEL zu Art. 354 StGB und SCHMID, Rz 1097, Rz 1100, 1106 - 1107.

Definition 2: Als „Authentisieren" soll die Zuordnung der Verantwortlichkeit für kommende Abläufe in der IT verstanden werden. Z.B. nach dem Anmelden an einem IT-Server oder das Prüfen einer elektronischen Signatur. Das Authentisieren in der IT beabsichtigt: *Der zu Authentisierende A überzeugt B, welcher das Authentisieren vornimmt, davon, dass A ein Geheimnis kennt.* Beispiele für ein solches Geheimnis sind ein Passwort und UserID oder ein geheimer kryptographischer Schlüssel. Bei letzterem überzeugt der zu Authentisierende A das Gegenüber B anhand eines kryptographischen Verfahrens davon, dass er das Geheimnis kennt. Er gibt aber dabei das Geheimnis nicht preis. Dies hat den Vorteil, dass B das Geheimnis von A nicht kennt und folglich sich nicht für A an einem anderen System danach anmelden kann.

Unterschiede: Beim Authentisieren sind die Geheimnisse wie ein Passwort einfach und bequem auf jemand anderen übertragbar. Beim Identifizieren ist zum Glück die physische Identität noch nicht übertragbar. Wie erwähnt, bedeutet Authentisieren letztlich das Zuordnen der Verantwortlichkeit, weil am anderen Ende der Datenkommunikation nicht wirklich festgestellt werden kann, wer das Geheimnis besitzt und sich damit anmeldet oder „digital ausgewiesen" hat.

III Beispiele für die irreführende Begriffswahl in Bundesbestimmungen

III.1 ZertES

Gemäss Art. 2 Bst. b Ziff. 2 des Bundesgesetzes über die elektronische Signatur (ZertES) ermöglicht eine fortgeschrittene elektronische Signatur die Identifizierung des Inhabers des privaten kryptographischen Schlüssels. Die elektronische Signatur ermöglicht jedoch eine Identifizierung nicht. Die Mittel für das Leisten einer elektronischen Signatur sind nämlich leicht übertragbar. D.h. der geheime kryptographische Schlüssel für die Signaturerstellung und die PIN für dessen Freischaltung können einem Dritten ohne nennenswerten Aufwand übertragen oder von einem Dritten gestohlen werden. Dieser Aufwand ist deutlich geringer als die Nachahmung einer Handunterschrift. Ein kurzer Exkurs zu den Begriffen Identifizieren und Authentisieren im Kontext zur elektronischen Signatur und zur Haftung befindet sich in „Anhang I elektronische Signatur - Identifizieren und Authentisieren".

III.2 BÜPF, VÜPF

In verschiedenen Bereichen werden aus Geräten Daten gelesen und ausgewertet. Nicht zuletzt, um sich ein genaueres Bild über das Kundenverhalten zu verschaffen. Auch aufgrund des Inkrafttretens des Nachrichtendienstgesetzes des Bundes (NDG) und infolge der Kompetenzerweiterung bei der Überwachung des Post- und Fernmeldeverkehrs, legitimiert durch das BÜPF, werden mehr Daten gesammelt werden. Folglich besteht dabei die Gefahr, dass man die aus den Geräten gesammelten Daten irrtümlich einer anderen Person, z.B. dessen Eigentümer, zuordnet. Beispiele für die falsche Zuordnung der erhobenen Daten:

- Eine registrierte Gesprächsverbindung (Einzelverbindungsnachweis) wird dem Eigentümer des Endgeräts zugesprochen. D.h. es wird intuitiv und meist ohne Zweifel angenommen, dass der Eigentümer des Handys das registrierte Gespräch geführt hat. Das wäre, als ob man von der Nummer des Kontrollschildes eines zu einem bestimmten Zeitpunkt beobachteten Fahrzeugs darauf schliessen würde, dass der Eigentümer oder Halter des Fahrzeugs zu diesem Zeitpunkt gefahren ist.
- In Zukunft kann man (un)dank IoT (Internet der Dinge) z.B. feststellen, wie oft und wann genau eine Kühlschranktür geöffnet wurde. Dabei wird festgestellt, dass in einem Single-Haushalt die Kühlschranktür 10mal über die Nacht verteilt geöffnet wurde. Folglich wird vermutlich davon intuitiv abgeleitet, dass sich der Besitzer der Wohnung morgens übermüdet ans Steuer seines Fahrzeugs gesetzt hat. Dabei wird kaum erwogen, dass der Besitzer des Kühlschranks die Nacht nicht alleine verbracht und jemand anderes den Kühlschrank geöffnet haben könnte.

Das Risiko, zweifelsfrei Personendaten vermeintlich korrekt zuzuordnen, wächst. U.a. auch, weil in Bundesvorschriften nicht sachgerechte Begriffe verwendet werden. Hierzu folgende Beispiele:

- Art. 21 (u.a. Abs. 1 Bst. a und e) und 22 Abs. 1 und 1^{bis} BÜPF. Die Überwachung eines Fernmeldeanschlusses oder eines Handys ohne zusätzliche Erfassung biometrischer Inhalte erlaubt keine Teilnehmeridentifikation. Z.B. kann die E-Mail von einem Hacker versandt werden, das Gespräch am Privatanschluss von einem Einbrecher geführt worden sein. Oder das Gespräch kann mit dem Handy von je-

mandem geführt werden, der nicht Eigentümer des Geräts ist. Analoges trifft auf Art. 19 Abs. 1 Bst. a und b BÜPF für die Überwachung des Postverkehrs zu.

- Zu weiteren, falschen Erwartungen betreffend Teilnehmeridentifikation bei der Überwachung des Fernmeldeverkehrs, S. 11 Abs. 5, S. 16 drittletzter Abs. in ERLÄUTERUNG VÜPF, wie auch Anhang VÜPF, Ziff. 13 und 33. Weiteres Beispiel siehe Art. 19 Abs. 1 und 2 VÜPF.

III.3 Gesetzesvorlage E-ID

Bei der Gesetzesvorlage E-ID werden die Begriffe „Identifizieren"/"Identifizierung" (z.B. Art. 2 Abs. b) ebenfalls nicht sachgerecht verwendet. Sie stimmen nicht mit dem überein, was die Allgemeinheit darunter versteht. In der Botschaft zur Gesetzesvorlage, S.14:

> Der Einsatz der E-ID mit dem Sicherheitsniveau «hoch» verlangt mindestens eine Zwei-Faktor-Authentifizierung, wobei ein Faktor biometrisch sein muss. Zusätzlich muss das Authentifizierungsmittel einen direkten Nachweis der Authentifizierung der Inhaberin oder des Inhabers liefern können, der vom E-ID verwendenden Dienst überprüft werden kann. Die Handhabung einer solchen E-ID ist vergleichbar mit einem Smartphone mit Fingerabdruck-, Gesichts- oder Stimmenerkennung, integriert in einem abgesicherten Bereich mit persönlichem Zertifikat.

Biometrische Techniken und Informationen sind dann geeignet, wenn das Erfassen der Prüfdaten (z.B. Einlesen eines Fingerabdrucks), das Vergleichen (mit den Fingerabdruckdaten in der Datenbank) und das Gewähren des Zutritts vollständig von „einer Hand" vorgenommen werden. Z.B. beim Einlesen des Fingerabdrucks im Smartphone zwecks Gewährens des Zugangs zu den darauf abgespeicherten Daten ist dies erfüllt, oder bei Zutrittssystemen in einem Hochsicherheitstrakt wie bei einem Gefängnis.

Beim Anmelden übers Internet erfolgt dies normalerweise nicht aus einer Hand, was zu erheblichen Sicherheitslücken führen kann. Dies z.B. weil die eingelesenen Fingerabdruckdaten kopiert, zu einem späteren Zeitpunkt bei einer anderen Authentisierung eingespielt werden können und dabei unberechtigt Zutritt verschafft werden kann. Die gesammelten biometrischen Daten können auch dazu dienen, das Identifizieren zu umgehen. Siehe dazu auch die allgemein verständliche Dokumentation der ARD „Pässe für Kriminelle".
Folglich versprechen biometrische Verfahren im Rahmen des Authentisierens nicht die zu erwartende Sicherheit oder schaffen sogar weitere Schwachstellen.

III.4 Identifikator

Das Wort Identifikator im Kontext zur AHV-Nr. erweckt die Vorstellung, dass eine Person damit identifiziert werden kann. Eine AHV-Nr. identifiziert eine natürliche Person bekanntlich nicht. Die AHV-Nr. ist lediglich ein Schlüsselattribut oder eine Registernummer in einer Datenbank für Personendaten. Ein Schlüsselattribut ist in einer Datenbank mit Personendaten ein Attribut, welches nur Angaben zu einer Person enthält. Analog dazu ist eine ISBN-Nr. ein Schlüsselattribut in einer Datenbank mit darin enthaltenen Informationen zu einem Buch.

Ein Identifikator eignet sich sehr bedingt fürs Authentisieren, weil diese Angabe ohne Aufwand kopiert werden kann und man sich damit als jemand anderen übers Datennetz ausweisen kann. Er dient lediglich der *vermeintlich* sicheren, eindeutigen Zuordnung der Abläufe im Datennetz auf eine natürliche Person.

III.5 Anonymität – Vertraulichkeit

Anonymität und Vertraulichkeit sind zwei Paar Schuhe. Mit dem Anonymisieren will man das Gegenteil von Authentisieren erreichen, nämlich die Zuordnung gewisser Daten oder die Zurechenbarkeit gewisser Abläufe verhindern. Mit der Vertraulichkeit wird bezweckt, dass nur von einem bestimmten (Personen)Kreis Daten gelesen und Abläufe verstanden werden können. Das Gewähren der Einsichtnahme für einen bestimmten (Personen)Kreis bedingt aber, dass zuvor mit gewünschter Sicherheit eruiert werden kann, wer Einsicht nehmen will. Also bedarf es einer vorgängigen Authentisierung.

Im allgemeinen Sprachgebrauch vermischen sich jedoch die Begriffe. Ein treffendes Beispiel dafür ist das Stimmgeheimnis. Der Wortteil „Geheimnis“ assoziiert, dass man damit die Vertraulichkeit schützen will. Dies ist hier nicht zutreffend. Bei der Aus- und gegebenenfalls auch bei der Nachzählung sind die Stimm- oder Wahlzettel für jeden daran Beteiligten ersichtlich und somit lesbar. Die Urne dient dazu, dass keine Zwischenergebnisse vor Urnenschluss bekannt gegeben werden und damit das Verhalten der Stimmberechtigten, welche ihre Stimme noch nicht abgegeben haben, noch beeinflusst werden kann

Mit dem Stimmgeheimnis bezweckt man, dass die abgegebene Stimme nicht einer Person eindeutig zugeordnet werden kann. D.h. die Rückverfolgbarkeit der Stimmabgabe soll unterbunden werden. Folglich sollte bei der Beurteilung und Einführung eines e-Voting Systems u.a. darauf geachtet werden, dass die elektronische Stimmabgabe nicht bis zum Wähler oder Abstimmenden zurückverfolgt werden kann.

Da beim Anonymisieren und beim Schutz der Vertraulichkeit unterschiedliche Ziele verfolgt werden, ist zu erwarten, dass die Techniken und Methoden zum Schutz dafür jeweils unterschiedlich ausfallen. Nicht so gemäss Rundschreiben 2008/21 „Operationelle Risiken – Banken Konsequenzen/Empfehlungen“ der FINMA. Dort in Rz 12 und 20 wird das Anonymisieren als eine Methode zum Schutz der Vertraulichkeit empfohlen. Zur Bedenklichkeit, wie wirksam das Anonymisieren zum Schutz der Vertraulichkeit in der Praxis ist, siehe MORGENROTH, S. 59 ff.

IV Exkurs

IV.1 Auswertung von Personendaten

Nicht das Datensammeln
ist problematisch,
sondern das Zuordnen
Inspired by Tom Stoppard:
It's not the voting
that's democracy.
It's the counting!

Algorithmen der Statistik sollen dazu beitragen, noch mehr Informationen aus den gesammelten Daten zu gewinnen. Doch Algorithmen und das Internet scheren sich einen Deut um Wahrheit. Oft wird dabei nicht unterschieden, ob zwischen den Daten eine Kausalität oder nur eine Korrelation vorliegt. Ein illustratives Beispiel hierzu. „Wenn es sommerlich warm ist, wird mehr Eiscreme konsumiert und die Menschen kühlen sich öfters in einem Bad ab. Letzteres führt dazu, dass mehr Menschen ertrinken oder gerettet werden müssen.“

Zwischen der Temperatur und dem Genuss von Eiscreme liegt eine Kausalität vor. Nicht aber zwischen dem Konsumieren von Eiscreme und den Badeunfällen. Ansonsten könnte man daraus schliessen, dass der Verzehr von Eiscreme Badeunfälle fördert oder umgekehrt. Was sich aus der Zunahme an konsumierten Eiscreme aber schliessen lässt, ist, dass sich die Badeunfälle vermutlich nun häufen werden.

IV.2 Falsch formulierte Haftungsbestimmung

Wie in der Einleitung erwähnt, besteht manchmal ein Missverständnis über den zugrunde liegenden Sachverhalt. Dies kann so weit gehen, dass eine falsche Haftungsbestimmung erlassen wird. Die Haftungsbestimmung in Art. 59a OR wurde mit der Revision des ZertES auf den 1. Januar 2017 angepasst. Doch die Bestimmung war vor und ist nach der Revision nicht korrekt formuliert.

Anstatt:

> Der Inhaber eines kryptografischen Schlüssels, der zur Erzeugung elektronischer Signaturen oder Siegel eingesetzt wird, haftet Drittpersonen für Schäden, die diese erleiden, weil sie sich *auf ein gültiges geregeltes Zertifikat* einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 18. März 2016 über die elektronische Signatur verlassen haben.

sollte es heissen:

> Der Inhaber eines kryptografischen Schlüssels, der zur Erzeugung elektronischer Signaturen oder Siegel eingesetzt wird, haftet Drittpersonen für Schäden, die diese erleiden, weil sie sich *auf eine elektronische Signatur* verlassen haben, welche mit einem geregelten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 18. März 2016 über die elektronische Signatur gültig geprüft werden kann.

Die Verwaltung (Ausgabe, Ungültigkeitserklärung, Auskunftserteilung) eines geregelten Zertifikats einer anerkannten Anbieterin von Zertifizierungsdiensten liegt im Normalfall ausserhalb der Verantwortlichkeit des Eigentümers der dazu passenden privaten kryptographischen Schlüssel, ausser er ist zugleich Eigner der anerkannten Anbieterin von Zertifizierungsdiensten. Der Eigentümer des privaten Schlüssels kann normalerweise lediglich ein Zertifikat beantragen und es vor Ablauf der Gültigkeit wieder revozieren, d.h. für ungültig erklären lassen. Er kann prüfen, ob die im Zertifikat enthaltenen Angaben zutreffen. Doch für die Verlässlichkeit des Zertifikats gegenüber Dritten haftet die anerkannte Anbieterin, Art. 17 Abs. 1 ZertES, weil nur sie entsprechende Zertifikate in ihrem Namen ausstellen darf oder sollte.

In der Handlungsmacht des Inhabers des privaten kryptographischen Schlüssels ist das Erstellen der elektronischen Signatur, jedoch in sehr beschränkter Weise die Verwaltung der dazugehörigen elektronischen Zertifikate. Er könnte auch nicht verhindern, dass die anerkannte Anbieterin ohne sein Einverständnis ein Zertifikat mit seinem Namen ausstellen würde und eine Falschbeurkundung mit seinem Namen im Zertifikat vornähme.

Seltsam an der bestehenden Ausgestaltung der Haftung nach Art. 59a OR ist auch, dass sowohl dem Inhaber des privaten kryptographischen Schlüssels als auch dem Herausgeber des Zertifikats (Art. 17 Abs. 1 ZertES) nach Wortlaut die Haftung für dasselbe, nämlich für die Verlässlichkeit der Angaben im Zertifikat, attestiert wird.

Der „Entlastungsbeweis“ zur Haftung nach Art. 59a Abs. 2 OR (das Glaubhaftmachen) bezieht sich auf die Handhabung des kryptographischen Schlüssels, welcher zur Erstellung

der Signatur verwendet wird, nicht aber auf die Handhabung oder Erstellung des Zertifikats.

Der Rechtssatz in Art. 59a Abs.1 OR ist folglich nicht sachgerecht formuliert.

V Fazit, Konsequenzen

Die Begriffe „Authentisieren“ und „Identifizieren“ sollten wegen ihrer (rechtlichen) Konsequenzen strikt auseinandergehalten werden; wie bei Eigentum und Besitz, oder Fahrer und Halter eines Fahrzeugs. Falls kein Unterschied, z.B. in Bezug auf die zivil- oder strafrechtliche Haftung gemacht werden sollte, so sollte dies im vollen Bewusstsein der Sachlage geschehen, wie z.B. bei Art. 6 Abs. 1 OBG (Ordnungsbussengesetz). Meines Erachtens wird es dann besonders kritisch, wenn sich eine Verurteilung in einem Strafprozess einzig auf Ereignisse betreffend die Authentisierung abstützt, welche jedoch *vermeintlich* zur Identifikation einer natürlichen Person dienten.

VI Anhang I elektronische Signatur - Identifizieren und Authentisieren

Der Prozess des Ausstellens eines elektronischen Zertifikats nach ZertES für eine natürliche Person soll als Beispiel dazu dienen, die beiden Begriffe eingehender zu erläutern.

VI.1 Prinzip des elektronischen Zertifikats

Das Prinzip der Ausstellung der elektronischen Zertifikate und ihrer Anwendungen beruhen grundsätzlich auf einem mathematischen Verfahren. Das Verfahren hat die Eigenschaft, dass zwei unterschiedliche Schlüssel erzeugt und verwendet werden. **Doch aus der Kenntnis eines Schlüssels lassen sich „keine“ Rückschlüsse auf den anderen Schlüssel desselben Schlüsselpaars ziehen,** siehe folgende Abbildung, Punkt 1)**.** (Die Aussage im letzten Satz wurde aus didaktischen Gründen vereinfacht.) Dies, obwohl sie mathematisch eindeutig miteinander verbunden sind und zugeordnet werden können. Weil keine Rückschlüsse möglich sind, kann ein Schlüssel des Paars veröffentlicht und der andere privat (geheim) gehalten werden. Sinnigerweise bezeichnet man den veröffentlichten Schlüssel als öffentlichen Schlüssel, den anderen als privaten.

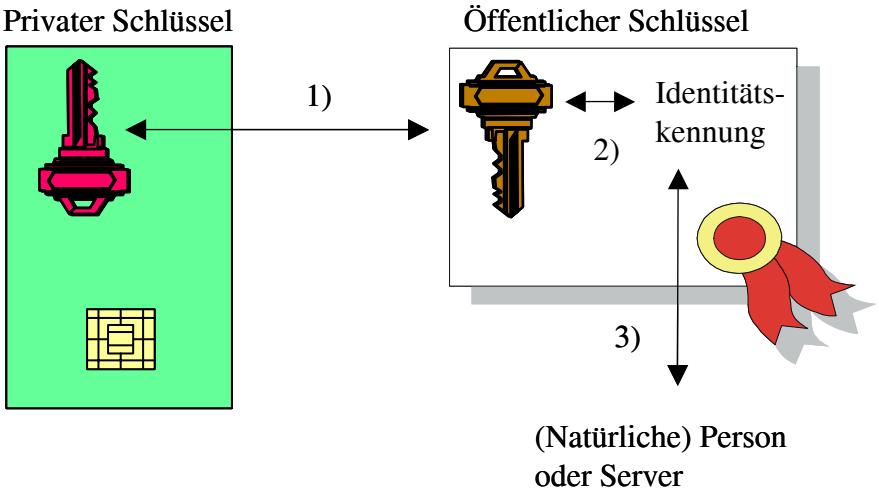

Abb. 1 Skizze zur Funktionsweise rund um die elektronischen Zertifikate

Die Anmeldung übers Netz funktioniert prinzipiell nun so, dass man die andere Partei übers Datennetz davon überzeugt, dass man den anderen, dazu passenden privaten Schlüssel kennt, ohne dabei diesen zu enthüllen. Eine natürliche Person A generiert nun ein Schlüsselpaar nach diesem Verfahren. Publiziert A den öffentlichen Schlüssel nun in ihrem Namen, so kann sich eine andere Person B über das Datennetz davon „vergewissern“, dass Person A die entsprechenden Daten gesandt hat. Person A kann nämlich mittels eines mathematischen Prozesses Person B davon überzeugen, dass sie Kenntnis vom dazu gehörigen privaten Schlüssel hat. Den Vorgang des Überzeugens wollen wir als „Authentisieren“ bezeichnen.

Nun kann jeder behaupten, er sei z.B. der Verwaltungsratspräsident des Unternehmens XY mit dem entsprechenden öffentlichen Schlüssel. Deswegen sind digitale Zertifikate unerlässlich, welche die Zugehörigkeit von öffentlichem Schlüssel und gewissen Personenattributen wie Name, Adresse usw. beglaubigen und verknüpfen 2). Anhand dieser Attribute im Zertifikat kann ein Rückschluss auf die natürliche Person oder auf den Server gemacht werden 3). Dies nach einer erfolgreichen Authentisierung.

Bevor der Aussteller des elektronischen Zertifikats die Personenattribute akzeptiert, sollte er sich davon vergewissern, dass die Person wirklich diejenige ist, welche sie vorgibt zu sein. Der Aussteller muss die Person also zuerst identifizieren 3). Erst dann sollte er dessen Attribute (Identitätskennung) erfassen und Teile davon ins Zertifikat aufnehmen 2).

Wenn der private Schlüssel bekannt wird, so kann sich ein andere Person C als A übers Datennetz bei Person B für A ausgeben. Deswegen werden die privaten Schlüssel am bes-

ten in sicheren Einheiten wie einer Crypto Card (eine mögliche Ausprägung der sicheren Signaturerstellungseinheit) aufbewahrt.

VI.2 Zweifel und Verlässlichkeit (Haftung)

Person B muss sich, um etwelche Dispositionen nach dem Authentisieren vornehmen zu können, auf Folgendes verlassen (vertrauen) können:

1. Die Angaben im Zertifikat stimmen. D.h. der Aussteller des Zertifikats hat die Identifizierung und das Erfassen der Personenattribute sorgfältig vorgenommen. (Zur Sorgfaltspflicht siehe Art. 5, 6, 7 VZertES).
2. Person A ist sorgsam mit ihrer Signaturerstellungseinheit umgegangen, d.h. sie hat ihren privaten Schlüssel nicht einem Dritten zugänglich gemacht oder ihm übertragen. Zur Sorgfaltspflicht siehe auch Art. 13 VZertES.
3. Sicherheit, dass dem öffentlichen Schlüssel im Zertifikat der zugehörigen private (Authentisierungsverfahren) nur mit grossem Aufwand zugeordnet werden kann. Zur Vereinfachung bei der Einleitung dieses Anhangs wurde geschrieben, dass keine Zuordnung möglich ist, was jedoch nicht zutrifft.

„Wenn wir alle Engel wären, bedürfte es keiner Gesetze“. Also sind gute Gründe, noch besser etwelche Absicherungen notwendig, bevor man sich auf das Verhalten anderer verlässt. Z.B. dass B den Schaden ersetzt bekommt, welcher aufgrund einer nach einer Authentisierung vorgenommenen Disposition verursacht wurde. Damit Schadenersatz geltend gemacht werden kann, sind entsprechende Haftungsbestimmungen erforderlich.

Für die Fälle 1 und 2, d.h. zur Risikominimierung bei durch Person B getroffenen Dispositionen nach dem Authentisieren, sind entsprechende Haftungsbestimmungen in Art. 17 ZertES (Herstellung eines elektronischen Zertifikats) und in Art. 59a OR (Leisten einer elektronischen Signatur) aufgenommen worden.

VII Anhang II Sicherheitsstufen im Kontext Herstellung von elektronischen Zertifikaten

VII.1 Einleitende Bemerkungen

In diesem Kapitel soll kurz erläutert werden, ob es (rechtlich und sicherheitstechnisch) sinnvoll ist, im eGovernment Umfeld das Authentisieren und das Ausstellen der elektronischen Zertifikate unterschiedlich sicher auszugestalten. Für die kommende Erläuterung notwendig ist, sich vorab noch einmal Folgendes vor Augen zu führen: Worauf muss sich B im Kapitel VI.2 "Zweifel und Verlässlichkeit (Haftung)“ verlassen können, damit er

nach dem Authentisieren *ausreichend sicher* etwelche Dispositionen vornehmen kann? Er muss sich sowohl auf die Korrektheit des Zertifikats wie auch auf die Authentizität der Signatur verlassen können.

Ausreichend sicher bedeutet hier, dass er den infolge der vorgenommenen Disposition erlittenen Schaden bei jemandem einfordern kann. Sei dies bei A oder dem Zertifikatsaussteller. Ohne Haftpflichtbestimmung, aber kein Schadenersatz! Je umfassender jemand verantwortlich, sprich haftbar, ist, desto grösser sind die Chancen, dass er für den von ihm verursachten Schaden einzustehen hat. Für unseren Anwendungsfall bedeutet dies: Je umfangreicher A oder der Zertifikatsaussteller haftet, desto risikoärmer kann B etwelche Disposition nach dem Authentisieren vornehmen.

VII.2 Haftung nach ZertES und OR 59a

Zuerst wird nun dargelegt, wie die Haftung zu den geregelten Zertifikaten eines nach ZertES anerkannten Anbieters von Zertifikaten im ZertES ausgestaltet ist.

Haftung gemäss Art 17 ZertES:

> Die anerkannte Anbieterin von Zertifizierungsdiensten haftet u.a. Drittpersonen (hier B), die sich auf ein solches Zertifikat verlassen haben, für den erlittenen Schaden, weil die Anbieterin den Pflichten aus diesem Gesetz und den dazu erlassenen Vorschriften nicht nachgekommen ist.

U.a. gehört es zu den Pflichten, den Nachweis der Identität des Antragstellers für ein Zertifikat sorgfältig zu prüfen (Art. 9 Abs. 1 Bst. a ZertES, Art. 5, 6, 7 VZertES). Wenn z.B. nun ein Dritter C eine Falschbeurkundung, d.h. ein Zertifikat mit den Personenangaben von A, erschleichen kann und dadurch B einen Schaden erleidet, dann haftet der Aussteller des Zertifikats für den Schaden an B. Sofern er nicht beweist, dass er diesbezüglich keine Sorgfaltspflicht verletzt hat. Er hat folglich u.a. für einen vorsätzlich begangenen Schaden, d.h. für grobes Drittverschulden von C, prinzipiell einzustehen.

Haftung für das Leisten der elektronischen Signatur nach Art. 59a OR:

> Person A hat für die mit ihrem privaten Schlüssel erstellten Signaturen einzustehen, welche mit ihrem geregelten Zertifikat eines nach ZertES anerkannten Zertifikatsanbieters verifiziert werden können. Dies sofern sie nicht glaubhaft darlegen kann, dass sie die Signatur nicht erstellt hat und sorgsam mit dem privaten Schlüssel umgegangen ist.

Angenommen, einem Dritten C gelingt es, in den Besitz des privaten Schlüssels von A zu gelangen und elektronische Signaturen im Namen von A herzustellen und dabei B zu schädigen. Dies, weil A unsorgfältig mit seinem Schlüssel umgegangen ist. Dann haftet A

grundsätzlich für den daraus an B erlittenen Schaden. Also haftet auch A für grobes Drittverschulden von C.

VII.3 Andere Konstellation

Basiert das Authentisieren nicht auf einem geregelten Zertifikat von einem nach ZertES anerkannten Anbieters, dann richtet sich die Haftung dafür im Grundsatz nach dem Obligationenrecht (OR), gegebenenfalls nach der Staatshaftung. Die Haftung für grobes Drittverschulden widerspricht jedoch unserer Rechtslehre und unserer Rechtspraxis prinzipiell. Folglich besteht meines Wissens anderswo als im ZertES und OR 59a keine Haftung für grobes Drittverschulden. Eine Haftung aus Vertrag ist nur eingeschränkt vorhanden, u.a. weil zwischen B und dem Zertifikatsanbieter im Allgemeinen kein Vertrag besteht. Im eGovernment existiert bei der Mehrzahl der Beziehungen zwischen A und B ebenfalls kein Vertrag. Folglich machen andere Konstellationen und folglich unterschiedliche Sicherheitsvorkehrung beim Authentisieren im eGovernment Umfeld meist wenig Sinn, falls B möglichst risikoarm etwelche Dispositionen nach dem Authentisieren treffen will. Weiter gilt es zu bedenken, dass eine Fülle an falsch vorgenommenen Dispositionen sich negativ auf den Ablauf einer Verwaltung auswirkt.

Viele Inhalte dieses Aufsatzes basieren auf der CAS ARBEIT.

VIII Angaben

VIII.1 Quellenangabe

CAS ARBEIT	Daniel Muster, Bedarf an Regulierung und Interdisziplinarität betreffend Haftung bei Internet der Dinge, September 2017
BUCHLEITNER/RABL	Blockchain und Smart Contracts, ecolex - Fachzeitschrift für Wirtschaft und Recht -, Januar 2017
ERLÄUTERUNG VÜPF	ISC-EJPD ÜPF, 26. Oktober 2011, Erläuterungen zur Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, SR 780.11) sowie Änderung der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (SR 780.115.1)
MORGENROTH	Markus Morgenroth, Sie kennen dich! Sie haben dich! Sie steuern dich!, Knaur Verlag, 2016
SCHMID	Niklaus Schmid, Handbuch des Schweizerischen Strafprozessrechts, DIKE Verlag, 2009
TRECHSEL	Stefan Trechsel, Schweizerisches Strafgesetzbuch - Praxiskommentar -, Dike Verlag, 2013

VIII.2 Abkürzungsliste, Gesetzestexte, Normen

Abs.	Absatz
Art.	Artikel
Bst.	Buchstabe
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 6. Oktober 2000, SR 780.1
E-ID	Bundesgesetz über anerkannte elektronische Identifizierungseinheiten, Gesetzesvorlage 2018
idR	in der Regel
IoT	Internet of Things, Internet der Dinge
NDG	Bundesgesetz über den Nachrichtendienst (Nachrichtendienstgesetz, NDG) vom 25. September 2015, SR 121
OBG	Ordnungsbussengesetz vom 24. Juni 1970, SR 741.03
OR	Schweizerisches Obligationenrecht vom 30. März 1911, SR 220
Rz	Randziffer
StGB	Schweizerisches Strafgesetzbuch, in Kraft seit 1. Januar 1942, SR 311.0
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007, SR 312.0
u.a.	unter anderem
VÜPF	Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 31. Oktober 2001, SR 780.11
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23. November 2016, SR 943.032
z.B.	zum Beispiel
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 18. März 2016, SR 943.03