Identitätsdiebstahl im Kontext zum Bundesgesetz über elektronische Identifizierungsdienste (BGEID)

In diesem Aufsatz soll Folgendes erläutert werden: „Die Umsetzung des BGEID kann das Risiko für Identitätsdiebstahl vergrössern.“ Basis der kommenden Ausführungen bilden die Gesetzesvorlage BGEID (nach der Verabschiedung durch das Parlament), die Botschaft des Bundes zur Gesetzesvorlage, das technische Konzept 2016 des Fedpol und die Spezifikation IDV 2017.

30. Oktober 2019, Version 3.1

Daniel Muster
8003 Zürich
www.it-rm.ch

Inhaltsverzeichnis

I „Einleitung

„Ich bin nicht ich, sondern ein jemand ganz anderer, der mir verblüffend ähnlich ist.“
Der Doppelgänger,
F. M. Dostojewski (1821- 1881)

Der Autor dieser Abhandlung hat an der Vernehmlassung der E-ID-Gesetzesvorlage teilgenommen und dabei viele der hier aufgeführten Sorgen und Bedenken eingebracht. D.h. die für diese Gesetzesvorlage zuständige Behörde wurde vor dem Verfassen dieses Aufsatzes kontaktiert.

I.1 Begriffe

Bevor mit den Ausführungen zum Identitätsdiebstahl begonnen wird, ist es angebracht, zuerst den Begriff Identitätsdiebstahl zu definieren. Unter Identitätsdiebstahl wird hier verstanden, dass sich jemand für eine andere Person ausgibt oder in ihrem Namen agiert; dies ohne deren Einverständnis. Sei dies in der realen oder auch in der virtuellen Welt. Erfolgt das Agieren im Namen einer anderen Person mit deren Einverständnis, so liegt eine Identitätstäuschung vor.

Anmerkung: Bei Identitätsdiebstahl handelt es sich nicht um einen Diebstahl im Sinne des Strafrechts (Art. 139 StGB), weil die Identität einer Person nicht übernommen, transferiert werden oder den Besitzer wechseln kann.

Die Problematik rund um den Identitätsdiebstahl spitzt sich weiter zu. Dies lässt sich aufgrund der technologischen Weiterentwicklung aus der folgenden sehenswerten, allgemein verständlichen ARD-Reportage „Pässe für Kriminelle“ bei Youtube (Sucheingabe: „Pässe für Kriminelle“) entnehmen.

I.2 Grundlage der vorliegenden Abhandlung

Grundlage der hier vorliegenden Abhandlung bilden das BGEID, deren Botschaft, das KONZEPT 2016 des Fedpol zu den elektronischen Identifizierungsdiensten und die Spezifikation IDV 2017. Auf dem Konzept 2016 basierten einige Bestandteile der E-ID-Gesetzesvorlage ans Parlament.

II Klärung der Sachlage – Schlussfolgerung

II.1 Identifizieren - Authentisieren

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 stattfindet, siehe dazu TRECHSEL zu Art. 354 StGB und SCHMID, Rz 1097, Rz 1100, 1106 - 1107.

Was eine E-ID genau ist, wird weder im Konzept 2016 noch in der Gesetzesvorlage genau definiert. Nach meinem Verständnis besteht eine E-ID aus Personenidentifizierungsdaten, einer analog zur AHV-Nr. sinnverwandten, eindeutigen E-ID-Registernummer (kurz E-ID-Nr.), sowie Angaben, wie man sich im Datennetz „ausweisen“ möchte. Die E-ID würde der Unternehmensidentifikation (UID) nach dem Bundesgesetz über die Unternehmens-Identifikationsnummer (UIDG) in etwa entsprechen. Dies, sofern der UID-Nr. auch noch ein Authentifizierungsmittel beigefügt würde, z.B. ein Zertifikat mit darin enthaltener UID-Nr.

Das „Sich Identifizieren“ im Datennetz ist dem „Sich Identifizieren“ in der realen Welt nicht gleichgestellt. Jedenfalls nicht, was sich die Allgemeinheit darunter vorstellt. Die Mittel für das „Sich Identifizieren“ oder „Sich Ausweisen“ in der digitalen Welt sind übertragbar, z.B. für das Anmelden an einem IT-System. Die körpereigenen biometrischen Informationen können aber nicht auf eine andere Person transferiert werden.

In BGEID (Art. 1 Abs. 1 Bst. a Abs. 2 Bst. a, Art. 2 Bst. b, Art. 12 Abs. 2, Art. 16 Abs. 1 Bst. b), in der Botschaft dazu (BBL 3916, 2018 oben in Übersicht), im Konzept 2016, S. 2 oben im Kasten, wird diesem Umstand nicht Rechnung getragen. Es wird folglich dort unsachgemäss von Identifizieren geschrieben, was falsche Assoziationen wecken,

Missverständnisse hervorrufen und gegebenenfalls auch falsche rechtliche Schlussfolgerungen bewirken kann.

Damit Transaktionen (Dispositionen nach der Anmeldung übers IT-Netz) trotzdem mit einem gewissen oder gewünschten Mass an Verlässlichkeit (Sicherheit) durchgeführt werden können, muss die Verantwortlichkeit der einzelnen Prozesse verlässlich zugeordnet werden können. In Analogie zum Strassenverkehr wird die Verantwortlichkeit der Fahrten eines Fahrzeugs auf den ersten Blick dem Fahrzeughalter zugesprochen. Die Zuordnung der Verantwortlichkeit geschieht aufgrund des Nummernschilds am Fahrzeug und der Angaben im Register des Strassenverkehrsamt.

Deswegen wird hier ein weiterer Begriff eingeführt, damit zwischen „Sich Ausweisen in der digitalen Welt“ und dem „Sich Identifizieren in der realen Welt“ konsequent und sachgerechter unterschieden wird.

Definition 2: Das „Sich Ausweisen“ in der digitalen Welt soll als „Authentisieren“ bezeichnet werden. Das „Authentisieren“ ordnet die Verantwortlichkeit für kommende Abläufe in der IT einer Person zu. Z.B. nach dem Anmelden an einem IT-Server oder das Prüfen einer elektronischen Signatur.

In Analogie dazu kann das Authentisieren als die Zuordnung des Fahrzeugs einem Fahrzeughalter verstanden werden, als Identifizieren die Bestimmung des Fahrers.

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 ein Benutzername (engl. UserID) oder ein geheimer kryptographischer Schlüssel. Bei letzterem überzeugt der zu Authentisierende A das Gegenüber B anhand eines kryptographischen Verfahrens davon, dass A das Geheimnis kennt. A gibt aber dabei das Geheimnis B nicht preis. Dies hat den Vorteil, dass B das Geheimnis von A nicht kennt und sich folglich nicht für A an einem anderen System später anmelden kann.

II.2 Erste Zusammenfassung

Beim Authentisieren sind die Geheimnisse wie ein Passwort einfach und bequem auf jemand anderen übertragbar. Beim Identifizieren ist die physische Identität zum Glück noch nicht übertragbar. Wie erwähnt, bedeutet Authentisieren letztlich das Zuordnen der Verant-

wortlichkeit, weil am anderen Ende der Datenkommunikation nicht wirklich festgestellt werden kann, wer das Geheimnis besitzt und sich damit anmeldet oder „digital ausgewiesen“ hat. In Analogie dazu kann aufgrund der Bestimmung des Fahrzeughalters nicht darauf geschlossen werden, wer mit dem Fahrzeug gefahren ist.

II.3 Identifikator

Das Wort Identifikator im Kontext zur AHV-Nr. oder zur E-ID-Nr. erweckt die Vorstellung, dass eine Person damit identifiziert werden kann, siehe z.B. Art. 8 Abs. 1 und Art 21 BGEID. Eine AHV-Nr., wie auch eine E-ID-Nr., identifizieren eine natürliche Person bekanntlich nicht. Die AHV-Nr. und die E-ID-Nr. sind 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 einzigen 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.

II.4 Schlussfolgerung

Aufgrund dessen, dass die Begriffe „Identifizieren“ und „Authentisieren“ nicht sachgerecht verwendet werden, werden falsche Erwartungen geweckt und der online-Anmeldung fälschlicherweise zu viel Bedeutung und folglich zu hohe Sicherheit beigemessen. Diese falsche Erwartungshaltung erhöht das Risiko für Missbrauch (engl. Fraud). Z.B.:

- Wird beim Empfang einer E-Mail nicht in Zweifel gezogen, dass jemand anderer als der Eigentümer der E-Mail Adresse die E-Mail versandt hat. Aufgrund der Angaben in der E-Mail trifft nun der Empfänger zum Schaden des Eigentümers der E-Mail-Adresse etwelche Dispositionen.
- Die geplante Änderung des ZertES. Mit der Einführung der Gesetzesvorlage soll das persönliche Erscheinen (Identifizieren) bei der Ausstellung eines geregelten Zertifikats dem Authentisieren mittels E-ID gleichgestellt werden (neu Art. 9 Abs. 1^{bis} ZertES).

In Analogie zum Autofahren lässt sich aufgrund des Nummernschilds nicht der Fahrer ermitteln, sondern lediglich der Fahrzeughalter und somit die Verantwortlichkeit für das Fahrzeug zuordnen. Dies sofern, dass

- das Nummernschild nicht an ein anderes Fahrzeug befestigt wurde
- und die Registrierung beim Strassenverkehrsamt zuverlässig (verlässlich) erfolgt ist.

Anmerkung: In verschiedenen technischen Konzepten und juristischen Abhandlungen (des Bundes zur E-ID) wird diese Differenzierung nicht vorgenommen und das Anmelden mit der E-ID als sicher und unproblematisch (für die Identifizierung) eingestuft. Z.B. wird auch in Art. 2 Bst. b Ziff. 2 ZertES festgehalten, dass eine Signatur die Identifikation einer Person ermöglicht. Dies ist nicht der Fall, weil die Mittel zum Leisten einer elektronischen Signatur übertragbar sind.

III Allgemeine Bedenken zur Sicherheit im Umfeld der E-ID

Wie soeben ausgeführt, kommt der Sicherheit bei der Zuordnung der Verantwortlichkeit eine zentrale Bedeutung zu. Im Folgenden werden nun die Sicherheitsbedenken aufgeführt, welche die verlässliche Zuordnung in Frage stellen. Kann die Verantwortlichkeit nicht ausreichend verlässlich zugeordnet werden, so kann dies dazu führen,

> *dass jemand für etwas einzustehen hat, wofür er nicht verantwortlich ist, weil z.B. jemand anderer in seinem Namen agiert hat.*

III.1 Ausgabe der E-ID

Es mag bezweifelt werden, ob die Herausgabe der E-ID in privater Hand die gleiche Sicherheit und vor allem die gleiche Unabhängigkeit bietet. Gesellschaftlich wichtige und sicherheitsrelevante Aufgaben der Registerführung mit Personen- oder Unternehmensdaten werden in bewährter Weise hoheitlich wahrgenommen, wie das Führen des Grundbuchamts, des Handelsregisters, des Personen- und Stimmregisters, wie auch die Vergabe der AHV-Nr., der UID-Nr. und die Herausgabe der Nummernschilder beim Fahrzeug.

Werden Aufgaben jedoch durch Private wahrgenommen, leidet die Sicherheit erfahrungsgemäss meistens unter der Kosten-/Nutzenrechnung.

Kontinuität ist ein wesentlicher Faktor der Verlässlichkeit, was wiederum ein Sicherheitsfaktor oder -merkmal darstellt. Ein privates Unternehmen kann Konkurs anmelden, eine staatliche Organisation nicht. Wenn alle Stricke reissen, d.h. kein privates Unternehmen die Ausstellung einer E-ID übernehmen will, muss der Bund diese Aufgabe übernehmen. Die Konsequenzen für die Kommunikation mit einer E-ID bei Konkurs des entsprechenden E-ID-Herausgebers werden in Kapitel IV.2.3 „Verfügbarkeit“ dargelegt.

III.2 Verschiedene Sicherheitsniveaus

III.2.1 Begriffe

Als „E-ID-Herausgeber“ wird hier die Anbieterin von „elektronischen Identitätsdienstleistungen“ gemäss Art. 1 Abs. 1 Bst. b BGEID bezeichnet.

Das „E-ID-System“ ist der Informatikdienst des E-ID-Herausgebers (Art. 2 Abs. a BGEID). Es dient dem Authentisieren des E-ID-Eigentümers, welcher eine E-ID bei diesem Herausgeber bezogen hat.

Ein „E-ID-Dienst“ ist die Kurzform für „E-ID-verwendeter-Dienst“ nach Art. 2 Abs. b BGEID. Er nutzt die weiteren Dienstleistungen des E-ID-Herausgebers, einen E-ID-Eigentümer authentisieren zu lassen. Ein solcher-E-ID-Dienst kann eine Behörde oder ein privates Unternehmen sein. Bsp. für ein privates Unternehmen ist ein Detailhändler oder ein Finanzinstitut.

III.2.2 Problematik 1 Sicherheitsniveau als Solches

Verschiedene Sicherheitsniveaus sind bei der Anwendung der E-ID angedacht. Dies führt oft zu langen Diskussionen über die Wahl, welches Sicherheitsniveau eingesetzt werden soll. Dabei wird meist aus Kostengründen ein niedrigeres Niveau bei den Anwendern gewählt. Zudem stellen sich folgende Fragen:

- Kennt der Gutglaubensschutz des Bürgers gegenüber dem Staat verschiedene Sicherheitsstufen, u.a. verschiedene Kategorien der Verlässlichkeit, und wie lässt sich dies unterteilen und abgrenzen?
- Ist es sinnvoll und praktikabel, verschiedene Sicherheitsstufen bei gleicher Haftung zu handhaben, und welche Sorgfaltspflicht wird bei den einzelnen Stufen gefordert?

- Ist es dann für den Rechtsunkundigen noch benutzerfreundlich?
- Gibt es eine allgemein verbindliche Richtlinie, welches Sicherheitsniveau für einen entsprechenden E-ID-Dienst notwendig ist, damit nicht vorgeworfen werden kann, dass die erforderliche Sorgfaltspflicht nicht eingehalten worden ist?

III.2.3 Problematik 2 Authentisieren, Zertifikat

Mit den Daten, welche in Art. 5 BGEID aufgeführt sind, lässt sich kein Authentisieren bewerkstelligen. Es bedarf noch eines Mittels für das Authentisieren; z.B. eines Passwortes oder eines elektronischen Zertifikats. Welche Technologien für die einzelnen Sicherheitsniveaus beim Authentisieren verwendet werden dürfen, ist nicht klar. Dies wird durch die Verordnung geregelt werden (Art. 4 Abs. 4 BGEID). Weil in der Gesetzesvorlage keine Differenzierung zwischen Authentisieren und Identifizieren gemacht wird, ist der Kompetenzumfang des Bundes aus Art. 4 Abs. 4 unbekannt.

Zudem wird Technologieneutralität (Art. 1 Abs. 3 BGEID) verlangt. Doch die Technologie bestimmt die Sicherheit und somit auch das Sicherheitsniveau. Das Unterstützen verschiedenster Technologien verursacht zudem nicht zu unterschätzende Kosten.

Verlässlich werden Transaktionen nur dann abgewickelt, wenn die Authentisierung aller involvierten Parteien entsprechend verlässlich erfolgt. Z.B. muss unterbunden werden, dass sich jemand im Namen einer anderen Person bei einem IT-System anmelden und in deren Namen Transaktionen vornehmen kann. Beim Anmelden bei einem E-ID-Dienst lediglich mit User Name und Passwort ist dies ohne weiteres möglich. Zudem ist kaum feststellbar, dass sich jemand anderer als der legitimierte Benutzer mit Username und Passwort angemeldet hat. Z.B. könnte sich auch ein Mitarbeiter eines E-ID-Herausgebers im Namen einer bei ihm registrierten Person bei einem IT-System anmelden.

Solches kann unterbunden werden, wenn die E-ID zusammen mit einem Zertifikat ausgegeben und verwendet wird, d.h. die entsprechende E-ID-Registernummer, kurz E-ID-Nr., wie eine UID-Nr. ins (geregelte) Zertifikat aufgenommen wird, siehe dazu Art. 7 ZertES. Bei einer auf Zertifikat basierten Anmeldung ist die Anmeldung im Namen eines Anderen bei sachgemässer Anwendung nach Stand der Technik nur mit enormem Aufwand und mit entsprechender Zeit möglich. Sachgemäss bedeutet hier, dass u.a. die in VZertES geforderten Sicherheitsmassnahmen eingehalten werden.

In Analogie dazu, bedarf es einer verlässlichen Bindung zwischen Fahrzeugnummer, Autotyp und Fahrzeughalter. Diese Bindung übernimmt der Fahrzeugausweis. In der digitalen Welt leistet eine solche Bindung das elektronische Zertifikat.

Im Moment ist jedoch noch unklar, ob es ZertES konform ist, eine E-ID-Nr. wie die UID-Nr. ins geregelte Zertifikat aufzunehmen. Das, was ins geregelte Zertifikat aufgenommen werden muss und kann, ist m.E. in Art. 7 Abs. 2 und 3 ZertES abschliessend aufgezählt. Eine E-ID-Nr. wird dabei nicht erwähnt. Eine Änderung dieses Artikels ist mit der E-ID-Gesetzesvorlage aber nicht angedacht.

Anmerkung: Was die blosse Verwendung der Sozialversichertennummer und einem Passwort bei der Authentisierung an Sicherheitsproblemen verursachen kann, lässt sich aus der Anzahl Vorkommnissen an Identitätsdiebstahl in den USA entnehmen.

Eine Übersicht der Zertifikatsausstellung wird im Anhang 1, MUSTER II dargelegt.

III.3 Daten

III.3.1 Art der Personendaten

Werden viele Einwohner der Schweiz eine E-ID beziehen, dann erhalten gemäss dem BGEID private Unternehmen Personendaten für die Identifikation im grossen Stil. Dabei ist nicht oder noch nicht geregelt, ob Betrieb und Datenhaltung vollständig in der Schweiz erfolgen muss. Ansonsten könnten dann die Daten für die Identifikation einer Person im Ausland gespeichert und folglich dort zugänglich sein.

Gemäss Art. 5 Abs. 3 BGEID werden bei der Sicherheitsstufe „hoch“ folgende Personendaten beim E-ID-Herausgeber gehalten: E-ID-Nr., amtlicher Name und Vorname, Geburtsdatum, Geschlecht, Geburtsort (vermutlich Heimatort), Staatsangehörigkeit und Gesichtsbild. Gemäss Art. 8 Abs. 2 BGEID kann die E-ID auch noch die AHV-Nr. enthalten. Gemäss Art. 5 Abs. 4 E-BGEID kann das Fedpol die Personenidentifizierungsdaten an den E-ID-Herausgeber mit zusätzlichen Informationen versehen, soweit dies für die Erfüllung der Aufgaben des E-ID-Herausgebers erforderlich ist. Welche Informationen dies genau sind, ist zum jetzigen Zeitpunkt unklar. Weiter ist auch unklar, welche Daten die entsprechenden Sicherheitsniveaus für das Authentisieren benötigen.

Zusammenfassend lässt sich feststellen, dass viele Daten beim E-ID-Herausgeber vorhanden sein können, die ein Identitätsdieb begehrt.

Folgende Frage stellt sich nun: Wie steht es um die Verantwortlichkeit des E-ID Herausgebers und um die möglichen Konsequenzen für die Einzelnen, wenn ein unberechtigter Dritter Zugang zum Server (E-ID-System) erhält und die Personendaten kopiert? Z.B. wurden die Personendaten von ca. 1 Mia. Einwohnern in Indien für die Identifizierung kopiert, siehe PÄSSE FÜR KRIMINELLE.

III.3.2 Verwendung biometrischer Informationen

Gemäss KONZEPT 2016 und Botschaft S. 3928, S. 3941, S. 3952 sind im Rahmen der E-ID noch biometrische Informationen vorgesehen. Wie diese Informationen im Rahmen der Authentisierung eingesetzt werden sollen, wird dabei nicht dargelegt. Folglich wird auch nicht ersichtlich, welchen Beitrag diese Informationen zur Sicherheit leisten. Zum Authentisieren, das „Sich ausweisen in der digitalen Welt“ jedenfalls nicht. Sie würden lediglich dann Mehrwert an Sicherheit erbringen, wenn sie zur sicheren Speicherung und der Freischaltung der Mittel zur Authentisierung dienten. Z.B. ein Fingerabdruck zum Freischalten einer Applikation für die Authentisierung.

Mit biometrischen Informationen sollte jedoch äusserst behutsam und sorgfältig umgegangen werden, wie die erwähnte ARD-Reportage aufzeigt. Diese Informationen sollten äusserst sicher verwaltet und aufbewahrt werden.

Grundsätzlich sollten biometrischen Informationen zum Authentisieren nicht verwendet werden (dürfen), da sie keinen Mehrwert an Sicherheit beim Authentisieren beitragen. Sind die biometrischen Angaben einmal unberechtigten Dritten bekannt, so lässt sich dies nicht mehr rückgängig machen. Ungültig erklären (revozieren) lassen sich die biometrischen Informationen nicht. Im Unterschied zu Username und Passwort oder einem elektronischen Zertifikat.

Selbst zur „sicheren“ Speicherung von Geheimnissen sollten keine biometrischen Daten eingesetzt werden, weil die Überprüfung der zu verifizierenden biometrischen Information für den Zugang sensitiver Informationen oft ungenügend sicher ist, sowie auch die Aufbewahrung der biometrischen Informationen.

III.4 Sperren einer E-ID

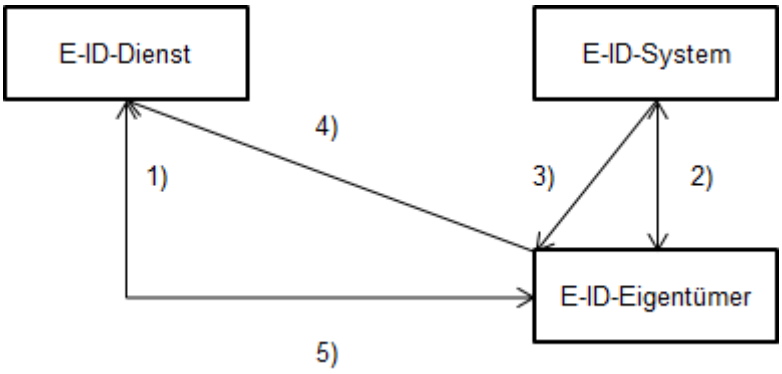
Irreführend bei den Erläuterungen in KONZEPT 2016 und gemäss Art. 11 BGEID ist, dass eine E-ID gesperrt und widerrufen, d.h. ungültig erklärt werden kann. Lediglich die Mittel

für die Authentisierung können gesperrt oder ungültig erklärt werden, wie z.B. ein elektronisches Zertifikat. Nicht gesperrt werden können jedoch Personenidentifizierungsdaten, insbesondere die biometrischen Informationen.

IV Sicherheitsbedenken bei der Umsetzung

IV.1 Sachverhalt

Zwischen dem E-ID-Dienst (Art. 2 Abs. 2 BGEID), dem E-ID-System (Art 2 Abs. 1 BGEID) und dem E-ID-Eigentümer besteht ein Dreiecksverhältnis, siehe folgendes Bild. Das E-ID-System wird vom E-ID-Herausgeber betrieben und dient u.a. der Authentisierung der E-ID-Eigentümer, welche dort die E-ID bezogen haben.



Figur 1 Kommunikationsaufbau mittels E-ID

Will ein E-ID-Eigentümer einen E-ID-Dienst benutzen (1), dann muss er sich vorgängig beim E-ID-System authentisieren (2). Das E-ID-System stellt bei erfolgreichem Authentisieren dem E-ID-Eigentümer eine elektronische Bestätigung aus (3). Der E-ID-Eigentümer übergibt diese Bestätigung dem E-ID-Dienst (4). Wird die Bestätigung vom E-ID-Dienst akzeptiert (5), dann kann der E-ID-Eigentümer den E-ID-Dienst nutzen.

IV.2 Schlussfolgerungen

IV.2.1 Sicherheit beim Anmelden

Der E-ID Dienst, z.B. das Patientendossier, authentisiert den E-ID-Eigentümer, z.B. Arzt oder Patient, nicht. Jedenfalls ist dies so angedacht, siehe KONZEPT 2016 Skizze 1 S. 8, Skizze 8 S. 35. Folglich hat sich der Dienst vollständig auf die Angaben des E-ID-Systems in der elektronischen Bestätigung zu verlassen. Ohne nennenswerten Aufwand könnte sich

der E-ID-Herausgeber im Namen des E-ID-Eigentümers ausgeben. Ob solches erkannt würde, mag bezweifelt werden.

Weil das E-ID-System Dreh- und Angelpunkt für den Verbindungsaufbau ist, kann es zudem erahnen, bei welchem E-ID-Dienst ein bestimmter E-ID-Eigentümer eine Berechtigung für den Zugriff auf Daten besitzt. Es könnte also z.B. feststellen, bei welcher Bank der E-ID-Eigentümer ein Konto besitzt und dort das eBanking abwickelt.

Die Sicherheit der elektronischen Bestätigung ist für die Sicherheit der Authentisierung des E-ID-Eigentümers von grosser Bedeutung. Die Bestätigung sollte vom E-ID-System am besten mit einer nach ZertES geregelten Signatur versehen werden. Darauf sollte im Rahmen der Ausführungsvorschriften zu Art. 20 Abs. b BGEID geachtet werden. Was nützt es aus Sicht des E-ID-Dienstes, wenn die Authentisierung des E-ID-Eigentümers beim E-ID-System mit grosser Verlässlichkeit stattfindet, aber die Bestätigung des E-ID-Systems an den E-Dienst nicht mindestens gleich sicher ist?

Im Sinne der IT-Sicherheit kann es sinnvoll sein, dass sich der E-ID-Eigentümer (Benutzer) bereits beim gesicherten Kommunikationsaufbau beim E-ID-Dienst authentisiert. Ein weiteres Authentisieren über das E-ID System ist dann nicht mehr erforderlich. Damit das Authentisieren mit der „E-ID“ entsprechend funktioniert, muss die E-ID-Nr. im Zertifikat enthalten sein.

Hier zeigt sich, dass zwischen E-ID-Nr., Personendaten für die Ausstellung der E-ID und dem Authentisieren mit der E-ID über das E-ID-System in der Gesetzesvorlage hätte konsequent unterschieden werden sollen. In der Vorlage wird zudem nicht definiert, was eine E-ID ist.

IV.2.2 Weiterleitung der Personendaten und Nutzerprofile

Wie erwähnt, erfolgt jegliches Authentisieren des E-ID-Eigentümers mit seiner E-ID beim E-ID-System des E-ID-Herausgebers. Dabei werden Personenattribute des E-ID-Eigentümers vom E-ID-Herausgeber an den E-ID-verwendeten Dienst transferiert. Gemäss Art. 8 Abs. 2 BGEID kann eines der Personenattribute auch die AHV-Nr. enthalten.

Weil das E-ID-Systems Dreh- und Angelpunkt des Verbindungsaufbaus einer Datenkommunikation ist, hat er Kenntnis darüber, welchen E-ID-Dienst der E-ID-Eigentümer auswählt und für welchen dieser sich authentisieren lässt. Dies bietet dem E-ID-Herausgeber die Möglichkeit, Benutzerprofile des E-ID-Eigentümers anzufertigen. Deswegen lässt sich, wie im NZZ-ARTIKEL dargelegt, vertreten, dass die E-ID mehr einer Kreditkarte gleicht als einem (elektronischen) Pass.

Das BGEID verlangt in Art. 16 Abs. 2, dass die Nutzerprofile nicht weitergegeben werden dürfen. Doch stellt sich hierbei die Frage, wie ein Verstoss dieser Bestimmung überhaupt festgestellt werden kann. Gesetzt den (hypothetischen) Fall, dies ist möglich, dann stellt sich die nächste Frage, wie solches dann geahndet wird und wie es um die Wiedergutmachung steht.

Anmerkung: Je besser das Verhalten einer Person bekannt ist, desto eher kann deren Identität von Dritten unbemerkt übernommen werden.

Beim Anmelden lediglich auf Basis eines elektronischen Zertifikats könnte der Aussteller des Zertifikats kein Nutzerprofil des Zertifikatseigners betreffend Kommunikation herstellen.

IV.2.3 Verfügbarkeit

Da das E-ID-System Dreh- und Angelpunkt für den Verbindungsaufbau zu einem E-ID-Dienst ist, funktioniert ein Kommunikationsaufbau mit einem E-ID-Dienst nicht, wenn das E-ID-System nicht in Betrieb ist. Das heisst, alle Eigentümer einer E-ID vom entsprechenden Herausgeber können dann keine Kommunikationsverbindung zu irgendeinem E-ID-Dienst aufbauen.

Angenommen, der E-ID-Dienst sei das elektronische Patientendossier und der E-ID Eigentümer sei ein Arzt, dann kann der Arzt weder Daten aktualisieren noch abrufen, solange das E-ID-System nicht funktioniert. Wie schnell der Kommunikationsaufbau bei Konkurs des E-ID-Herausgebers für dessen E-ID-Eigentümer wieder zu funktionieren und wie verfügbar ein E-ID-System zu sein hat, ist meines Wissens zurzeit noch unklar. Mangelnde Verfügbarkeit ist im Kontext eines Patientendossiers bedenklich.

IV.2.4 Nachvollziehbarkeit

Zur Nachvollziehbarkeit der Kommunikationsabläufe äussert sich die Vorlage nicht. Ohne Nachvollziehbarkeit kann jedoch der Urheber eines Vorfalls oder eines Schadens nicht ausreichend bestimmt werden.

IV.3 Vergleich

Um die Sicherheit des Verbindungsaufbaus mit höchster Stufe zu „würdigen“, ist ein Vergleich mit dem Verbindungsaufbau alleine auf Basis von elektronischen Zertifikaten angebracht. Bei einem gesicherten Verbindungsaufbau alleine auf Basis von Zertifikaten ist im Unterschied zu einem gesicherten Verbindungsaufbau mittels E-ID auf höchster Sicherheitsstufe keine Drittpartei (E-ID-System) involviert. Dies hat folgende Vorteile:

- Der Herausgeber des Zertifikats kann nicht erahnen, bei welchen Diensten der Zertifikatsbezüger Rechte besitzt.
- Der Kommunikationsaufbau ist sicherer. Grund: Die Einbindung einer Drittpartei beim Kommunikationsaufbau schmälert prinzipiell die Sicherheit des Kommunikationsaufbaus und somit der darauf folgenden gesicherten Kommunikation.
- Höhere Verfügbarkeit
- Die Nachvollziehbarkeit ist bei 2 involvierten Parteien einfacher als bei 3 zu bewerkstelligen.
- Der Herausgeber des Zertifikats kann nicht einfach und bequem ein Kommunikationsprofil des Zertifikatsbezügers erstellen.

IV.4 Unklares

IV.4.1 Einleitung

In seiner Stellungnahme zur E-ID-Gesetzesvorlage hat der Kanton Zürich u.a. auf Folgendes hingewiesen:

> Neben diesen grundsätzlichen Bemerkungen bleibt allgemein anzufügen, dass im vorgelegten Vorentwurf in vielen (keineswegs nur untergeordneten) Fragen auf die noch zu erarbeitende Verordnung verwiesen wird, welche die erforderlichen Präzisierungen bringen soll. Unter diesen Umständen regen wir an, auch die noch auszuarbeitende Verordnung in die Vernehmlassung zu geben, damit dort die Bedürfnisse der Kantone und gegebenenfalls der Gemeinden eingebracht werden können.

Dass Skepsis bei den kommenden technischen Vorschriften nicht unbegründet ist, lässt sich anhand der elektronischen Eingabe von Rechtsschriften an die Verwaltung oder ans Gericht entnehmen. Die elektronische Eingabe von Rechtsschriften erfolgt über eine Zustellplattform, welche die Rechtsschriften zwischenlagert und dabei den Empfänger informiert, dass eine Rechtsschrift abzuholen ist. Die Post und ein anderes privaten Unternehmen betreiben je eine solche Zustellplattform.

Die Eingabe der Schriften ist nun so ausgestaltet, dass diese Unternehmen - von aussen nicht feststellbar und ohne jeglichen Aufwand - eine Kopie der Rechtsschrift anfertigen und Einsicht darin nehmen können. Gemäss Kapitel 4.3.1 Abs. 2 Bst. c der technische Ausführungsvorschrift ZUSTELLPLATTFORM ist es nicht vorgesehen, dass elektronische Rechtsschriften vor dem Versand nur so verschlüsselt werden dürfen, dass einzig der Empfänger der Rechtsschrift diese entschlüsseln kann.

Wenn Rechtsschriften elektronisch so versandt werden, dass sie einem unbeteiligten Dritten zugänglich gemacht oder offenbart werden, ist der objektive Tatbestand der Berufs- oder der Amtsgeheimnisverletzung erfüllt. Siehe dazu auch PLÄDOYER. Das Bundesparlament war sich bei der Revision des BGG oder VwVG gewiss nicht bewusst, dass eine solche technische Realisierung für die elektronische Zustellung der Rechtsschriften angedacht war.

Die Versichertenkarte ist ein weiteres Beispiel dafür, wie bedenklich die Umsetzung von Art. 42a KVG sein kann. Z.B. haben Logopäden, Ernährungsberater, Physiotherapeuten das uneingeschränkte Recht, den Hinweis auf eine Patientenverfügung und die Kontaktadressen

zu überarbeiten, d.h. lesen, schreiben und löschen, siehe Anhang in VVK. Der Versicherte hat nicht die Möglichkeit, autonom, d.h. ohne einen Leistungserbringer, seine Personendaten auf seiner Versichertenkarte einzusehen und diese zu kontrollieren. Für die Sicherheit ist m.E. wichtig, dass der Versicherte seine Daten auf der Karte problemlos kontrollieren kann. Weitere Problempunkte, siehe SOZIALVERSICHERTENKARTE.

IV.4.2 Unklar in der Realisierung

Wer einen E-ID-verwendenden Dienst betreiben will, braucht eine Vereinbarung mit einem IdP (Art. 20 BGEID). Warum dies vermutlich nicht ausreicht, soll anhand des folgenden Beispiels illustriert werden:

> E-ID-Eigentümer Peter Muster hat eine E-ID beim Herausgeber A bezogen und will sich beim E-ID-Dienst „Sorglos“ anmelden. Doch dieser Dienst hat lediglich eine Vereinbarung mit dem E-ID-Herausgeber B abgeschlossen.

Um dieses Problem zu lösen, gibt es u.a. folgende 2 Möglichkeiten:

1. Ein E-ID-Dienst trifft mit jedem E-ID-Herausgeber eine Vereinbarung.
2. Ein Intermediär zwischen den verschiedenen E-ID-Herausgeber wird eingeschalten. Die technische Realisierung dafür wurde in IDV 2017 spezifiziert. (In der Gesetzesvorlage ist diese Partei jedoch nicht aufgeführt.)

Das Einschalten eines weiteren Systems (Intermediär) reduziert erfahrungsgemäss die Verfügbarkeit. Zudem besteht die Möglichkeit, dass der Intermediär Einsicht in Daten für die Authentisierung nehmen und ein Benutzerprofil erstellen kann. Die Rechte und Pflichten eines Intermediär dürfen jedoch nicht über die Verordnung geregelt werden, weil sie in einem Gesetz enthalten sein müssen (Art. 164 Abs. 1 BV).

IV.4.3 Sicherheitsrelevant, aber unklar

Hier eine Liste dessen, was im Kontext zum Identitätsdiebstahl/E-ID auch noch unklar ist.

- Welche Attribute des E-ID-Eigentümers vom E-ID-Herausgeber an den E-ID-Dienst gesendet werden dürfen.
- Wie sicher sich das E-ID-System gegenüber dem E-ID-Eigentümer und dem E-ID-Dienst authentisieren muss.

- Wie sicher sich der E-ID-Dienst gegenüber dem E-ID-Eigentümer authentisieren muss.
- Welche Sicherheit bei der Authentisierung die 3 Sicherheitsniveaus je enthalten und welche weiteren Daten des E-ID-Eigentümers dazu erforderlich sind, siehe. Art. 5 Abs. 4 BGEID.
- Wie sicher die Personenidentifizierungsdaten beim E-ID-Herausgeber gespeichert werden.
- Wie konform mit bestehenden Bestimmungen der Prozess des Authentisierens erfolgt, wenn die Kommunikation mittels E-ID zwischen den Behörden oder zwischen Berufsgeheimnisträger(n und Behörde) erfolgt und das E-ID-System und die E-ID-Herausgabe in privater Hand liegt. Werden dann die Informationen der Behörde einem privaten Unternehmen offenbart (zugänglich gemacht)? Zu „offenbaren“, siehe STRATENWERTH/WOHLERS, TRECHSEL Kommentar zu Art. 320 und 321 StGB.

V Haftung

No Reliability without Liability!
Sicherheit (Verlässlichkeit) ohne Haftung bei Nichteinhalten der Vorschriften zu erwarten, ist illusorisch.

V.1 Zu den Haftungsbestimmungen als Solchen

Die Haftungsbestimmungen im E-ID-Gesetz greifen nicht, weil sie sich nach dem OR richten. Bei einem Schaden fällt bei grobem Drittverschulden die Schadensersatzforderung weg oder wird erheblich reduziert. Warum eine Haftung für grobes Drittverschulden jedoch notwendig ist, siehe MUSTER I. Bei der elektronischen Signatur auf Basis von geregelten Zertifikaten (Art. 59a OR) und bei deren Ausstellung (Art. 17 ZertES) besteht m.E. eine Haftung für grobes Drittverschulden. Folglich macht es wenig Sinn, eine E-ID ohne dazugehöriges geregeltes elektronisches Zertifikat zu verwenden.

Anmerkung: Bei Strolchenfahrten gibt es eine Haftung des Fahrzeughalters für grobes Drittverschulden (Art. 75 Abs. 3 SVG).

V.2 Ermittlung des Verursachers

Damit der Verursacher eines Schadens eruiert werden kann, müssen die Prozesse (in der IT) nachvollziehbar sein. Diese Anforderung wurde meines Wissens nicht aufgestellt. In den entsprechenden eCH-Standards wurde meines Wissens dieses Thema nicht abgehandelt.

Erschwerend kommen u.a. folgende Faktoren hinzu:

- Bei der Anmeldung mit einer E-ID können 3 oder sogar 4 Parteien involviert sein, z.B. wenn mehrere E-ID-Herausgeber involviert sind oder ein Intermediär zwischen den Herausgebern eingebaut wird, siehe IDV 2017.
- Selbst wenn der Prozess nachvollziehbar ausgestaltet wird, so liegen die Informationen zur Feststellung des Verursachers nicht beim E-ID-Eigentümer, was die Ermittlung des Verursachers eines Schadens für ihn enorm erschweren kann.

V.3 Koordination

Die Haftung ist im Gegensatz zur EU nicht abgestimmt. Zurzeit besteht in der Schweiz je eine andere Haftung bei der Herausgabe von Zertifikaten, einer UID-Nr. und bei einer E-ID. Zudem besteht keine oder eine andere Anerkennungs- und Überwachungsstelle. Abstim-

mungsprobleme sind zu erwarten, was wiederum der (Rechts)Sicherheit abträglich sein kann.

V.4 Quantifizierung des Schadens bei Verlust der Personendaten

Z.B. der Schaden zum Zeitpunkt der illegalen Kopie der Personenidentifizierungsdaten lässt sich meist nicht oder nur schwerlich quantifizieren. Welchen weiteren Schaden die Kopie dieser Daten infolge des technologischen Wandels in Zukunft noch verursachen kann, ist noch schwerer zu beziffern. Ohne quantitative Angaben des Schadens ist eine Haftungsklage bedeutungslos, siehe z.B. KELLER, LUTERBACHER.

Ein möglicher Lösungsansatz zur Minderung des Schadens wäre die Einführung eine dem Vertragsrecht ähnliche kumulative Konventionalstrafe bei der ausservertraglichen Haftung.

V.5 Rechtsweg - Kontrolle

Missstände werden vermutlich eher zur Kenntnis genommen und behoben, wenn sich die vom Missstand Betroffenen wirksam zur Wehr setzen können. Daran sollten sich möglichst alle beteiligen dürfen. U.a. kann dies vereinfachter erfolgen, wenn der Rechtsweg für die Betroffenen erschwinglich ist, d.h. z.B. über ein öffentlich-rechtliches Verfahren. Die Ausstellung der E-ID sollte folglich als öffentliche Aufgabe taxiert werden, damit eine natürliche Person mit beschränkten finanziellen Mitteln eine Haftungsklage einreichen und bei Abweisung der Klage die Kosten tragen kann.

V.6 Abstimmung der Haftung

In Kapitel IV.1 “Sachverhalt” wurde das Dreiecksverhältnis E-ID-System, E-ID-Dienst und E-ID-Eigentümer beim Aufbau der Kommunikation dargelegt. Grundsätzlich sollen alle nach dem Obligationenrecht haften (Art. 32 Abs. 1 BGEID) haften. Unklar dabei ist,

- wie der Bund haftet, wenn er eine dieser Rollen einnimmt (Art. 32 Abs. 2 BGEID). Haftungen aus anderen Gesetzen gehen der Haftung des Bundes aus dem VG vor, siehe auch Kommentar zu Art. 3 VG, N 54 LUTERBACHER.
- wie ein E-ID-Dienst haftet, wenn er kantonale hoheitliche Aufgaben abwickelt. Anzunehmen ist nach den Bestimmungen des BGEID.
- wie der E-ID-Herausgeber haftet, wenn ein nach ZertES geregeltes Zertifikat Bestandteil der E-ID und deren Anwendung ist.

Für den Betrieb eines E-ID-Dienstes bedarf es einer Vereinbarung mit einem Betreiber eines E-ID-Systems (Art. 20 BGEID). Ob ein Kontrahierungszwang für den E-ID-Herausgeber besteht und inwieweit seine Haftung für die verschiedenen Pflichten ausbedungen werden kann, ist im BGEID nicht ersichtlich. Da die Sicherheit der Kommunikation zentral vom E-ID-System abhängt, wird der E-ID-Herausgeber möglichst die Haftung in der Vereinbarung wegbedingen. Ob in diesem Bereich der EDÖB die Befugnis hat, bei der Prüfung der Vereinbarungsmuster dort korrigierend einzuwirken (Art. 15 Abs. 1 Bst. l BGEID), ist unklar. Zudem hat die EIDCOM, die Bewilligung erteilende Behörde, den EDÖB lediglich anzuhören.

Angenommen, ein Dienst will seine Benutzer (E-ID-Eigentümer) gemäss Sicherheitsstufe hoch (Art. 4 Abs. 1 Bst. BGEID) vom E-ID-System authentisieren lassen, z.B. auf Basis eines nach ZertES geregelten Zertifikats. Nun stellt sich folgende Frage, wenn der E-ID-Dienst aufgrund eines Benutzers (E-ID-Eigentümers) einen Schaden erleidet: Ist es für den E-ID-Dienst haftpflichtrechtlich vorteilhafter, wenn er die Benutzer selber direkt auf Basis eines geregelten Zertifikat authentisiert? D.h., auf die Authentisierung durch das E-ID-System verzichtet. Für den Aussteller besteht nach ZertES für die Richtigkeit der Angaben im geregelten Zertifikat eine milde Kausalhaftung (Art. 17 ZertES).

Mit Verabschiedung des BGEID durchs Parlament ist weiter angedacht, dass das ZertES betreffend Ausstellung der geregelten Zertifikate um Art. 9 Abs. 1^{bis} ergänzt wird. Ein persönliches Erscheinen ist nicht mehr notwendig, wenn der angehende Bezüger eines geregelten Zertifikats mit dem Sicherheitsniveau substantiell vom E-ID-System authentisiert wird. Der Betreiber des E-ID-Systems soll für die korrekte Authentisierung nach OR haften. Der Herausgeber des geregelten Zertifikats haftet gegen aussen mit einer milden Kausalhaftung (Art. 17 ZertES) inklusive grobem Drittverschulden.

V.7 Haftung des E-ID-Eigentümers

V.7.1 Vorspann

Wie erwähnt, wird nirgendwo im Gesetz definiert oder gar umschrieben, was eine E-ID ist. Sie wird bei der Sicherheitsstufe niedrig mit grosser Wahrscheinlichkeit eine immaterielle Ausprägung besitzen, wie z.B. ein Passwort mit Angaben für die Identifizierung. Das heisst, eine E-ID kann in einem solchen Fall nicht verloren gehen, höchstens die Rechte daran. Mit

der Aussage, dass der Verlust einer E-ID gemeldet werden muss, wird (bei mir) normalerweise assoziiert, dass die E-ID eine materielle Ausprägung (Sache) besitzt und mit den uns angeborenen Sinnen überwacht werden kann. Ein Passwort kann jedoch nicht verloren gehen. Lediglich eine weitere Person kann davon Kenntnis erlangen.

V.7.2 Haftung

In Art 12 Abs. 1 BGEID: *„Die Inhaberin oder der Inhaber einer E-ID hat die nach den Umständen notwendigen und zumutbaren Massnahmen zu treffen, damit seine E-ID nicht missbräuchlich verwendet werden kann.“*

Da - wie erwähnt - eine E-ID im BGEID nicht umschrieben, schon gar nicht definiert ist, ist der Umfang der vom E-ID-Inhaber zu treffenden Massnahmen gegen Missbrauch einer E-ID sehr vage. Die Ursache, dass eine E-ID missbräuchlich verwendet wird, kann auch beim E-ID-Herausgeber, gegebenenfalls auch beim E-ID-Dienst liegen. Letzteres, wenn es jemandem aufgrund unzureichender Sicherheitsmassnahmen beim E-ID-Dienst gelingt, sich für einen E-ID-Inhaber auszuweisen. Folglich liegen etliche Massnahmen, welche gegen den Missbrauch seiner E-ID getroffen werden können, ausserhalb des Möglichen des E-ID-Inhabers.

Da wie gesagt, die Nachvollziehbarkeit des Anmeldeprozesses an ein E-ID-Dienst mit einer E-ID im BGEID nicht gefordert wird, liegt es nahe, dass bei Missbrauch einer E-ID der Verdacht einer Sorgfaltspflichtverletzung zuerst auf einen E-ID-Inhaber fällt.

Es wäre wünschenswert, wenn der Bund legitimiert würde, Vorschriften betreffend Sorgfaltspflicht im Umgang mit einer E-ID erlassen zu dürfen. Der Umfang der Sorgfaltspflicht sollte von der Sicherheitsstufe abhängig sein.

V.8 Zusammenfassung des Kapitels

Es besteht die Möglichkeit, dass sich der Haftungsumfang mit der Einführung einer E-ID bei vielen Anwendungen reduziert. Z.B., wenn ein E-ID-Dienst eine kantonal staatliche Aufgabe digital abwickelt.

Betreffend Haftung zwischen E-ID-Herausgeber und E-ID-Dienst stellen sich u.a. folgende Fragen:

- Besteht auch eine Haftung aus Vertrag oder lediglich eine ausservertragliche Haftung nach OR? Es ist anzunehmen, dass sich die Haftung des E-ID-Herausgebers nach einem konzessionierten Gewerbe richtet, und folglich die Haftung aus Vertrag nur beschränkt wegbedungen werden kann (Art. 100 Abs. 2 und Art. 101 Abs. 3 OR).
- Wie steht es um die Sorgfaltspflichten der jeweiligen Parteien? Pflichten und Rechte einer Partei wären jedoch im Gesetz zu umschreiben (Art. 164 Abs. 1 BV). Art. 20 BGEID ist folglich ungenügend ausgestaltet. Für die Sicherheit eines E-ID-Dienstes ist es zentral, wie verlässlich die Informationen des E-ID-Herausgebers sind.

Der Umfang der Sorgfaltspflichten eines E-ID Eigentümers bleibt vage. Einerseits, vieles, was mit einer E-ID missbräuchlich passieren kann, liegt ausserhalb seines Einflussbereichs. Andererseits, was den Umständen zumutbar und notwendig ist, lässt sich aus dem Gesetzestext nicht entnehmen und wird nicht durch eine Verordnung näher erläutert werden, da die Legitimation aus Gesetz fehlt.

Ohne die Anforderung der Nachvollziehbarkeit bleibt in vielen Fällen unklar, wer den Schaden verursacht hat und folglich wer das Risiko eines Schadens zu tragen hat.

VI Fazit, Konsequenzen

Identitätsdiebstahl im grossen Stil kann die Polizei und die Strafverfolgung mit Arbeit so überhäufen, dass sie der mit dem Identitätsdiebstahl verbundenen Verbrechen nicht mehr Herr werden können. Dann kann von geregelten gesellschaftlichen Prozessen nicht mehr die Rede sein, insbesondere dann, wenn mithilfe des Identitätsdiebstahls Terroranschläge vereinfacht durchgeführt werden. Dass das Risiko des Identitätsdiebstahls ohne das Ergreifen entsprechender Massnahmen zunehmen wird, zeigt die ARD-Reportage auf.

Aufgrund der hier aufgeführten Sicherheitsbedenken besteht mit der Einführung der E-ID ein Risiko für den Identitätsdiebstahl und eines für die Verfügbarkeit der E-ID-Dienste. Das gesamte Risiko dafür lässt sich noch nicht abschätzen, weil der Inhalt der Verordnung und der technischen administrativen Vorschriften noch unklar ist. Es stellt sich die Frage, ob man sich wie bei der UID auf die Herausgabe einer E-ID-Nr. (Identifikator) beschränkt und auf die Authentisierung mit dem E-ID-System verzichtet. Beim Vollzug von Bundesrecht

besteht diese Wahl jedoch (noch) nicht (Art. 22 Abs. b BGEID). Die E-ID ist zu akzeptieren, wenn sie das geforderte Sicherheitsniveau erfüllt.

Bevor nun die Gesetzesvorlage akzeptiert worden ist, hätte das gesamte Paket dem Bundesparlament offengelegt werden müssen. Ansonsten könnte sich Ähnliches wie bei der elektronischen Eingabe der Rechtsschriften an die Behörde und wie bei der Sozialversichertenkarte ereignen. Das Parlament stimmte der Revision des VwVG und des BGG zu, ohne zu wissen, dass bei der technischen Realisierung der objektive Tatbestand der Amts-, resp. Berufsgeheimnisverletzung erfüllt werden wird.

Es mag u.a. auch bezweifelt werden, dass die angestrebte technische Realisierung benutzerfreundlicher ist als das direkte Anmelden beim Dienst mit einem elektronischen Zertifikat. Erwähnenswert ist: Der Herausgeber des Zertifikats weiss nicht, wer sich bei wem damit authentisiert. Dies im Unterschied zum E-ID-Herausgeber. Deswegen lässt sich daraus schliessen, dass eine E-ID eher eine Kreditkarte darstellt (s. NZZ-ARTIKEL).

Noch folgende persönliche Anmerkung zum Schluss: „Wünschenswert wäre es, wenn KONZEPT 2016 und Botschaft der Vorlage nüchterner abgefasst und weniger mit Marketing ausgestattet wären. D.h. Ausdrücke wie „Einfach und benutzerfreundlich“, „sicher und bequem“ sind zu vermeiden, insbesondere wenn sie nicht zutreffen. Nachteile der technischen Realisierung, wie die damit verbundenen Risiken, sollten ebenfalls dargelegt werden.

VII Angaben

VII.1 Quellenangabe

BOTSCHAFT	Botschaft zum Bundesgesetz über elektronische Identifizierungsdienste, BBl 3915 bis 3988, 2018
IDV 2017	State Secretariat for Economic Affairs SECO, Interface Specification, WP-Number 2400, 7.6.2017
KELLER	Alfred Keller, Haftpflicht im Privatrecht, Band I, Stämpfli Verlag AG, Bern 1993
KONZEPT 2016	„Staatliche anerkannte elektronische Identifizierungsmittel (E-ID)“, Konzept 2016, Bundesamt für Polizei (Fedpol)
LUTERBACHER	Thierry Luterbacher, Fischer Willi (Hrsg.), Haftpflichtkommentar, Dike Verlag, 2016
MUSTER I	Daniel Muster, Haftung für grobes Drittverschulden, http://www.it-rm.ch/dokumente.html
MUSTER II	Daniel Muster, „Irrtum - Identifizieren versus Authentisieren“, Definition von Sicherheitsdiensten, http://www.it-rm.ch/dokumente.html
NZZ-ARTIKEL	Lukas Mäder, Warum die E-ID eher einer Kreditkarte gleicht als einem Pass, NZZ, 23. März 2019
PÄSSE FÜR KRIMINELLE	ARD Reportage zum Identitätsdiebstahl, Pässe für Kriminelle, auf Youtube
PLÄDOYER	Corinne Hauri, Eingaben per E-Mail zu wenig geschützt, Plädoyer 3/13
SCHMID	Niklaus Schmid, Handbuch des Schweizerischen Strafprozessrechts, DIKE Verlag, 2009
SOZIALVERSICHERTENKARTE	Daniel Muster, Sozialversichertenkarte, http://www.it-rm.ch/dokumente.html
STRATENWERTH/WOHLERS	Günter Stratenwerth, Wolfgang Wohlers, Schweizerisches Strafgesetzbuch Handkommentar, Stämpfli Verlag, 2007
TRECHSEL	Stefan Trechsel, Schweizerisches Strafgesetzbuch - Praxiskommentar -, Dike Verlag, 2013

VII.2 Abkürzungsliste, Gesetzestexte, Normen

Abs.	Absatz
Art.	Artikel
BGEID	Bundesgesetzüber über elektronische Identifizierungsdienste

BGG	Bundesgesetz über das Bundesgericht vom 17. Juni 2005, SR 173.110
Bst.	Buchstabe
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101
E-ID-Nr.	E-ID-Registrierungsnummer gemäss Art. 5 Abs. 1 Bst. a E-ID-Gv
Fedpol	Bundesamt für Polizei
idR	in der Regel
KVG	Bundesgesetz über die Krankenversicherung vom 18. März 1994, SR 832.10
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
SVG	Strassenverkehrsgesetz vom 19. Dezember 1958, SR 741.01
u.a.	unter anderem
UIDG	Bundesgesetz über die Unternehmens-Identifikationsnummer vom 18. Juni 2010, SR 431.03
UID-Nr.	Unternehmensidentifikations-Nr. gemäss Art. 3 Abs. 1 Bst. a UIDG
VG	Bundesgesetz über die Verantwortlichkeit des Bundes sowie seiner Behördemitglieder und Beamten vom 14. März 1958, SR 170.32
VVK	Verordnung über die Versichertenkarte für die obligatorische Krankenpflegeversicherung vom 14. Februar 2007 (Stand am 1. Januar 2009), SR 832.105
VwVG	Bundesgesetz über das Verwaltungsverfahren, vom 20. Dezember 1968, SR 172.021
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
Zustellplattform	Anforderungen an Plattformen für die sichere Zustellung im Rahmen von rechtlichen Verfahren (Kriterienkatalog Zustellplattformen) vom 16. September 2014 (Version 2.0), SR 272.11