Was ist und zu welchem Zweck braucht man eine „Sichere Identität“?
– einige grundlegende Aspekte des Identitäts-Managements –

Prof. Dr. Georg Rainer Hofmann
Information Management Institut IMI
Technische Hochschule Aschaffenburg

Zusammenfassung und Motivation

Der Betrug mit (Digitalen) Geschäftsprozessen und anderes ungesetzliche Verhalten kann durch die „Sichere Identität“ der Kunden und Geschäftspartner erschwert werden. Hier spielen eine „Vertrauensvolle Identität“ und eine „Zuverlässige Identität“ eine wichtige Rolle. Diese beiden Begriffe bilden einen Gegensatz, da zwischenmenschliches Vertrauen typischerweise eine mangelnde technische Zuverlässigkeit kompensiert, und umgekehrt Zuverlässigkeit ein mangelndes Vertrauen. Eine „Sicherheit“ bedeutet einmal ein sicheres Erkennen der „wahren“ Identität von Personen oder Sachen, ein andermal deren Verbergen und damit sicheren (Daten-)Schutz und Anonymität. Mit der „Fälschungssicherheit“ von Identitätsdokumenten werden wiederum die gänzlich verschiedenen Aspekte von deren Integrität, Nicht-Duplizierbarkeit, Verifikation, auch der Inhaber-Autorisierung und Legitimation verbunden. Der Beitrag versucht einige dieser Begriffe im Umfeld der „Sicheren Identität“ zu erklären, so auch die der „amtlichen Identität“ versus der „selbst-souveränen Identität“ SSI. Es werden historische und etymologische Aspekte aufgegriffen und Hinweise zum Identitäts-Management und dessen weiterer Verbreitung gegeben.

1 Eine im Sommer des Jahres 2021 immer noch aktuelle Frage: Was ist eine Identität?

Es gibt in eigenartiger Weise Begriffe, von denen man im Alltag zu wissen glaubt, was sie bedeuten – bei genauerer Betrachtung zeigen sich aber massive Definitionsprobleme. So stellte seinerzeit Bert Rürup [Rüru00] zum Begriff der „Arbeit“ in der Volkswirtschaftslehre fest: „*Jeder weiß zwar, was Arbeit ist. Allerdings ist es bislang noch niemandem so recht gelungen, eine allgemein akzeptierte Definition von Arbeit vorzulegen.*“ Dieses Problem mutet zwar „wissenschaftlich abstrakt“ und sophistisch an. Es hat aber sehr konkrete Folgen, wenn es um die praktische Gestaltung von „fairen Arbeitsbedingungen“ oder um das Finden eines „gerechten Lohn“ geht. Ähnliche Unsicherheiten sind zum Begriff „Geld“ zu beobachten – und so verhält es sich auch mit dem Begriff der „Identität“.

Die vom Verband *Sichere Digitale Identität e.V.* [VSDI19] vorgelegte Definition dürfte zunächst eine breite Zustimmung finden: „*Der Begriff Identität definiert eine Person als einmalig und unverwechselbar. Dafür gibt es eine Vielzahl individueller Attribute wie zum Beispiel Name und Geburtsdatum sowie Gesichtsbild und Fingerabdruck. In der digitalen Welt haben Menschen heute mehrere Identitäten mit unterschiedlichen Merkmalen. Wir stehen mit unserem Namen, Adresse und Fotos in Social Media-Plattformen, tätigen Online-Einkäufe, nutzen andere Online-Dienstleistungen mit Benutzername und Passwort. (…) Eine sichere digitale Identität bedeutet, dass diese nicht manipuliert, gefälscht oder missbraucht werden kann. (…) Aber nicht nur Personen und Organisationen, sondern auch Objekte und Dienste besitzen Identitäten. So können sich Produktionsanlagen beispielsweise bei der Fernwartung eindeutig identifizieren oder sich ein Ersatzteil einer Maschine als Originalteil ausweisen.*“

Diese Definition berücksichtigt nicht hinreichend, dass sich die „Attribute“ einer Person – oder auch einer Sache – im Laufe der Zeit zu ändern vermögen. Ein Mensch dürfte im Alter von sechs versus sechzig Lebensjahren im Gesicht schon sehr verschieden aussehen, und könnte auch seinen Familienamen geändert haben. Er dürfte sich in den Jahrzehnten körperlich in seiner Statur und im Auftreten geändert haben. Er könnte gar das Attribut seiner Fingerabdrücke durch einen bedauerlichen Unfall verloren haben. Der Mensch kann sich durch Krankheiten oder Drogen völlig verändern – so dass er sprichwörtlich „nicht mehr derselbe ist“. Gleichwohl bleibt die Identität dieses Menschen erhalten, nicht nur im Sinne seines subjektiven psychologischen „Ich-Bewusstseins“. Auch ein sich wandelnder Mensch wird im Laufe der Jahrzehnte von seiner sozialen Umgebung trotz der diversen Veränderungen sicher (wieder-)erkannt.

- ➔ Die sich im Laufe eines Lebens kontinuierlich ändernden Attribute haben dazu geführt, dass Identitätsdokumente – wie Ausweise – in aller Regel und sinnvollerweise eine begrenzte Gültigkeit haben. Nach einer definierten Zeit werden die Attribute – wie das Lichtbild des Inhabers – aktualisiert.

Ähnliches ist für Sachen zu beobachten. Robert M. Pirsig erläutert in „Zen und die Kunst ein Motorrad zu warten“ [Pirs78], dass (s)ein Motorrad quasi nur eine „Idee“ im Platonischen Sinn ist – es existiert völlig unabhängig von den materiellen Teilen, aus denen es konstruiert ist. Letztere können ja im Laufe einer jahrelangen Wartung systematisch durch neue Teile ersetzt werden. Der Verfasser dieses Textes besitzt ein Fahrrad aus dem Jahr 1992. Obwohl bis auf die Tretkurbeln und die Sattelstütze keine Teile aus der Anfangszeit mehr daran vorhanden sind – selbst der Rahmen musste wegen Bruchs zweimal ersetzt werden – so ist es doch „das Fahrrad“, das von seinem Besitzer als solches sicher identifiziert werden kann. Wenn es aber die materiellen Dinge und Teile nicht sind – was macht dann die Identität dieses Fahrrads aus?

Dass die Identität eines Gegenstandes offenbar von seiner materiellen Basis unabhängig ist, erkannte schon der antike griechische Philosoph Plutarch mit seinem „Schiff des Theseus“: Das Schiff, mit dem Theseus losfuhr und zurückkehrte ist von den Athenern lange Zeit aufbewahrt worden. Allerdings ersetzten sie viele der alten Planken durch neue. Die Frage, ob ein komplexes Objekt wie das Schiff des Theseus seine Identität verliert, wenn viele oder alle seiner Einzelteile ausgetauscht werden, oder ob es nach wie vor dasselbe ist, kann – so Plutarch – prinzipiell nicht entschieden werden. Zumal die Athener einige dieser alten Teile aus dem Schiff des Theseus in wiederum anderen Schiffen verbauten – werden diese dann ebenfalls „Theseus-Schiffe“? Es ist ein philosophisches Paradoxon.

- ➔ Die „Identität“ einer Person oder einer Sache ist ein grundlegendes philosophisches Problem mit größter lebenspraktischer Relevanz. Die Fragen sind zentral, wer eine bestimmte Person ist, und wozu eine bestimmte Person – aus welchem Grund – berechtigt oder verpflichtet ist, was sie zu tun oder zu lassen hat. Bei konkreten individuellen Sachen (wie etwa Fahrzeugen, Elektro- und Motorwerkzeugen, Jagdwaffen, etc.) ist die Frage ebenfalls an Berechtigungen orientiert, nämlich welche Handlungen damit erlaubt, beziehungsweise untersagt sind, oder auch welche Gewährleistungen damit verbunden sind.

In der Informationsgesellschaft haben „Digitale Identitäten“ eine große Bedeutung erlangt. Wir lesen bei [VSDI19] weiter: „*Sichere digitale Identitäten sind somit eine grundlegende Voraussetzung für eine erfolgreiche Digitalisierung auf allen Ebenen – Politik, Gesellschaft und Wirtschaft. Sie legen die Grundlage für eine vertrauenswürdige elektronische Kommunikation und sichere digitale Geschäftsprozesse. Doch werden die Methoden und Mittel für einen Missbrauch digitaler Identitäten immer umfangreicher und ausgefeilter. Wer jedoch die Bedrohungen kennt, kann vorbeugende Maßnahmen treffen und entsprechende identitätsschützende Technologien einsetzen.*“

- ➔ Konsequenterweise sind vor dem Hintergrund des vordem dargestellten Paradoxons die oben verwendeten Begriffe „Identität“, „sichere Identität“, „digitale Identität“, „vertrauenswürdige Identität“, „zuverlässige Identität“, „Identitätsvielfalt“, „Identitätsmissbrauch“, „Identitätsschutz“ – und andere mehr – systematisch zu hinterfragen. Das soll im Folgenden versucht werden.

Keinesfalls haltbar ist eine Synonymität der Begriffe „vertrauenswürdig“ und „zuverlässig“. Die Gegenläufigkeit dürfte etwa aus dem Szenario des Gebrauchtwagenhandels allgemein bekannt sein, wo die Vertrauenswürdigkeit der Verkäufer die technische Zuverlässigkeit der Autos kompensieren kann – und umgekehrt. Die Zuverlässigkeit technischer Systeme ist eine analytisch oder statistisch erfassbare Größe, die Systemfehlfunktionen adressiert. Vertrauenswürdigkeit ist hingegen ein psychosoziales Phänomen [Hart11] [Toma10]. Die oben aus [VSDI19] zitierte *„vertrauenswürdige elektronische Kommunikation“* ist – als in sich widersprüchlich – zu hinterfragen.

Archetypus: Wer bist Du? Ich kenne Dich doch! – Was ist das? Das kommt mir bekannt vor!

Die Fähigkeit, Personen oder Sachen sicher zu erkennen, ist eine Grundkomponente der sozialen Kompetenz des Menschen [Lisch13]. Ist jemand von der Störung der Prosopagnosie betroffen, dem „Nichterkennen von Gesichtern“, so führt das zu massiven Störungen im sozialen Umgang [Jime11]. Freilich wissen sich die Betroffenen zu orientieren, weil sie ihre Mitmenschen am Klang der Stimme, oder der Art wie sie sich bewegen, ebenfalls sicher erkennen können.

Selbst ein Hund kann sowohl „seine Leute“ (Herrchen, Frauchen, etc.), als auch „seine Sachen“ (Fressnapf, Spielzeug, Leine, etc.) sicher erkennen [Zime92]. Das archetypische Erkennen von Personen oder Sachen ist also kein Spezifikum des Menschen. So schrieb vor etwa 2700 Jahren der Prophet Jesaja „*ein Rind erkennt seinen Eigner, ein Esel die Krippe seines Meisters*“ – wie Buber und Rosenzweig diesen Halbsatz in Kapitel 1, Vers 3 übersetzen.

Auf der Metaebene ist wiederum der Auftritt von Ochse und Esel ein wichtiges Attribut von Darstellungen der Weihnachtsgeschichte. Daran wird das Abstraktum „Weihnachtsgeschichte“ ziemlich sicher identifiziert, obwohl in der Weihnachtsgeschichte bei Lukas die Tiere gar nicht vorkommen. Die Weihnachtsgeschichte wird paradoxerweise an Attributen erkannt, die diese überhaupt nicht besitzt.

➔ Das sichere Identifizieren von Personen und Sachen ist ein Archetypus, der nicht nur bei Menschen, sondern auch bei anderen höheren Säugetieren existiert. Diese quasi „ursprüngliche“ Art der *vertrauensvollen Identifikation* funktioniert ohne Ausweise oder anderweitige technische Ausstattungen. Diese Identifikation basieren auf dem psycho-sozialen Phänomen des Vertrauens.

Wird die archetypische vertrauensvolle Identifikation durch eine Identifikation durch Ausweise oder anderweitige Technik abgelöst, so ist das irritierend und kostet entsprechenden sozialen Kredit. So dürfte es einem altbekannten Kunden kaum gefallen, wenn er sich künftig beim Betreten eines Geschäftslokals formal ausweisen müsste. Grob boshaft wäre es, die zum Kaffee eingeladene engere Familie vor dem Betreten der Wohnung einer Ausweiskontrolle zu unterziehen – im Sinne von „wir müssen doch wissen, mit wem wir es zu tun haben“. Wobei das letztgenannte Problem mit einer Ausweiskontrolle auch nicht zu lösen wäre.

Symbole der Identität: Der Besitz und die Akzeptanz von Insignien

Seit jeher haben Menschen das Bedürfnis, ihre Identität durch entsprechende materielle Attribute zu belegen. Dabei geht es typischerweise nicht so sehr darum, erkennen zu geben, *wer man ist*, sondern vielmehr zu signalisieren, welchen Status, welche Funktion, und insbesondere welche Macht und damit verbundene *Befugnisse und Kompetenzen man hat*. Bei [Alth13] wird ausgeführt: „*Im Mittelalter prägten rituelle Kommunikationsformen den öffentlichen Umgang der Mächtigen miteinander. (…) Durch öffentliche Rituale erhielt eine rangbewusste Gesellschaft alle Informationen, die für eine geregelte Herrschaftsausübung nötig waren. Rituale informierten über Rechte und Pflichten, signalisierten den Zustand von Beziehungen und spiegelten die bestehende Ordnung wider.*“

Auch in aktueller Zeit spielen Rituale und damit verbundene – sichtbare – Insignien eine zentrale Rolle. Durch ein Insigne wird das Individuum erkennbar identifiziert als ein Inhaber von Macht und Befugnis, auch politischer Herrschaft. Insignien können Kleidungsstücke sein, wie Uniformen mit Rangabzeichen, Kopfbedeckungen, wie Kronen, Helme, Federhauben, Amtsketten, Sheriffsterne. Insignien können aber auch Gegenstände sein, so etwa ein Zepter, Marschallstab, Kriminaldienstmarke, etc. die vom Inhaber besessen und sichtbar herumgetragen oder vorgezeigt werden können. Ein spezielles Insignie ist das Siegel, welches als Petschaft oder Siegelring gestaltet sein kann. Der Abdruck des Siegels bestätigt, dass eine Handlung – typischerweise die Ausfertigung einer Urkunde – tatsächlich von der befugten Stelle oder Person ausgeführt worden ist. Ebenfalls spezieller Natur sind Tür- oder Schrankschlüssel. Die Schlüssel sind Instrumente eines befugten Zugangs – sie werden aber nicht von Menschen, sondern von Sachen – den passenden Schlössern – quasi „anerkannt“.

Die Insignien der Neuzeit sind Pässe und Bescheinigungen, die in materieller (Papier-)Form oder als immaterielle digitale Dokumente gestaltet sind. Der Begriff „Pass“ kommt von lateinisch „*passare*“ – hindurchgehen – der Begriff „Passport“ von „*passare portas*“ – durch Tore hindurchgehen (dürfen). Eine „Bescheinigung“ ist die Dokumentation einer dahingehend glaubhaften Versicherung, dass etwas „durch Augenschein“ gültig und verlässlich ist. Die ersten Pässe bekamen beispielsweise durch Siegel eine Gültigkeit, nannten aber nicht unbedingt den Namen des Inhabers. Sie waren damit so übertragbar wie ein moderner ÖPNV-Fahrschein, der nur bescheinigt, dass man das Entgelt für die S-Bahn oder den Bus bezahlt hat – aber die Anonymität des Fahrgastes wahrt. Passdokumente räumten etwa ab dem Mittelalter einen speziellen Schutz für reisende Personen ein. Das war auch bei dem Pass der Fall, den König Ludwig XI. in Frankreich im Jahr 1462 einführte: Entlassene Soldaten mussten einen solchen Pass mitführen, um belegen zu können, dass sie keine Deserteure sind. Später mussten auch Kaufleute durch eine Bescheinigung ihrer Heimatstadt ihre Rechtschaffenheit belegen können, um an einem fremden Markt handeln zu dürfen [Groe04].

➔ Eine Identität kann über ein Insignie belegt werden. Der Gebrauch von Insignien hat eine lange Tradition, sie sind auch in der Moderne akzeptiert und relevant. Bei einem Insignie ist der Besitz entscheidend – das Insignie darf nicht in die „falschen Hände“ gelangen. Komplementär muss das Insignie in Bezug auf seine Bedeutung quasi „anerkannt“ werden. Das ist ein generelles Merkmal von Identitätszeichen und Identitätsdokumenten, dass sie anerkannt werden müssen – sonst läuft ihre Bedeutung ins Leere. Die

Anerkennung kann sowohl durch Menschen als auch durch entsprechend konstruierte Maschinen und Apparate erfolgen.

Anonymität: Sag bloß nicht, wer ich bin!

Thomas Claes fragt in „Passkontrolle! – Eine kritische Geschichte des sich Ausweisens und Erkanntwerdens“ [Clae10]: „*Wieso müssen sich Menschen ausweisen? Und wieso versuchen die Staaten ihre und fremde Bürgerinnen und Bürger zu identifizieren? Die Geschichte des sich Ausweisens und Erkanntwerdens ist die Geschichte wachsender Gouvernementalität und Disziplinierung der Bevölkerung in der Moderne. Früher wies man sich aus, indem man schriftliche Empfehlungen angesehener Bürger, Geistlicher oder des Landesherrn mit sich trug. Fürsprache oder Leumund waren die Pässe der Vormoderne, was sich seit dem 19. Jahrhundert gründlich änderte. Fragen der Biometrie, Chiptechnologie und der Kryptografie werfen heute ganz neue Diskussionen auf.*“

Anonymität bedeutet das Verbergen der Identität, ein *Pseudonym* ist hingegen ein selbstbestimmt und frei gewählter nicht-amtlicher Name – etwa ein Künstlername – und der Gebrauch eines dahingehend „falschen“ Identitätsmerkmals. Die Wahrung der Anonymität erscheint als ein Grundrecht jeder Person, denn Anonymität kann persönlichen Schutz bedeuten, der Verlust der Anonymität kann schwere Nachteile mit sich bringen. Das im christlichen Abendland notorisch prototypische Verbrechen, der „Verrat des Judas“ nach Markus Kapitel 14 ist im Kern quasi „nur“ die Offenlegung einer Identität, ein „Identitätsmissbrauch“ für einen „Judaslohns“. In deutscher Übersetzung lesen sich die Kernsätze etwa so: „*Und Judas, einer der Zwölf, ging zu den Hohepriestern. Denn er wollte ihnen [Jesus] übergeben. Als die das hörten freuten sich und versprachen, ihm Silber zu geben. (…) [Es] hatte aber der ihn übergebende [Judas] ein Zeichen vereinbart: Wen [auch] immer ich küssen werde, der ist [es]; haltet ihn und führt ihn zuverlässig ab*“.

Wenn in moderner Zeit der Wahrung von Anonymität und den Anliegen des Datenschutzes mit einem reaktionären „wir haben doch nichts zu verbergen“ entgegnet wird, so muss man sehen, dass der Verrat des Judas kein klassisches Verbrechen war – es war nur ein (antikes) *Persönlichkeitsschutz-Vergehen*. Judas gibt – gegen Geld – einen Hinweis für die Gehilfen des Tempel-Establishments. Judas verstößt *nicht* gegen ein damals geltendes Gesetz oder Gebot, er hat nicht einmal gelogen. Das Vorgehen des Judas ist perfider Weise juristisch völlig korrekt.

➔ Ein Gegensatz von „zuverlässigem“ und „vertrauensvollem“ Identitätsmanagement wird erneut evident: Die Aufhebung der Anonymität und Identifikation des Jesus durch Judas war *zuverlässig* – aber eine *vertrauensvolle* Tat war das sicher nicht. Judas hat seinen ehemaligen sozialen Kontext durch seinen Vertrauen-vernichtenden Hinweis für die Tempelpolizei nachhaltig zerstört.

Identitätsdokumente und Idiosynkrasie

Das Ende der historisch gewachsenen allgemeinen Anonymität im Alltag und einen Fortschritt für das Passwesen brachte die Französische Revolution mit sich. Im Juni 1791 versuchte König Ludwig XVI. in einer Verkleidung s einer Verurteilung zu entkommen. Es wird erzählt, dass Ludwig aber anhand einer Münze erkannt wurde, auf der er abgebildet war. Die französische Revolutionsregierung verlangte in der Konsequenz generell für das Passieren der Grenzen ins Ausland nun einen *Pass*, der den Namen und eine Personenbeschreibung enthielt. Ein Nebeneffekt der Französischen Revolution war die Entstehung des modernen „Staatsbürgers“ und die Abgrenzung der „Ausländer“, diese beiden Identitätsformen wurden durch das Passwesen quasi erst „kreiert“ – und damit besser überwachbar [Clae10].

➔ Mit der Erfindung des allgemeinen Passwesens wurde die Identität des Menschen quasi „verdoppelt“: Nun existierte er einmal als physische (vertrauenswürdige) Person, aber auch als abstraktes (zuverlässiges) Dokument „Pass“. Ohne seinen „Pass“ war der Mensch nun ein „Nichts“ – der vorherige Normalfall der Anonymität im Alltag war damit stark relativiert worden. Der Gebrauch von *zuverlässigen* Identitätsdokumenten ersetzte zunehmend das *vertrauensvolle* archetypische Erkennen.

Konsequenterweise führten einige Staaten eine *Ausweispflicht* ein. Sie existiert auch in der Bundesrepublik Deutschland nach § 1 Personalausweisgesetzes (PAuswG) für Bürger ab dem vollendeten 16. Lebensjahr. Es ist ordnungswidrig, weder einen Personalausweis noch einen Reisepass zu besitzen; das kann nach § 32 PAuswG

mit einem Bußgeld bestraft werden. Eine generelle – staatlich-gesetzliche – Mitführpflicht gibt es nur für Sonderfälle, wie etwa für Arbeitnehmer während der Arbeitszeit zur Verhinderung illegaler Beschäftigung.

In Analogie zu den gesetzlichen amtlichen Pässen haben private und halb-öffentliche Einrichtungen ebenfalls „Pässe" eingeführt. Man kennt etwa Mitgliedsausweise für Vereine oder andere Gruppen, auch Studenten-, Mitarbeiter- und Werksausweise sind weit verbreitet. Diese Spezialausweise machen oft nur Sinn, wenn sie mit einer *Mitführpflicht* kombiniert werden. Es gibt etwa Gebäude von Firmen oder Instituten, die nur mit den entsprechenden Mitarbeiter- oder Besucherausweisen betreten werden dürfen. In vielen Fällen müssen solche Ausweise *als Insignie sichtbar* getragen werden.

Juristisch und ökonomisch relevante Identitätsdokumente können materiell oder digital realisiert werden. Sie heißen, merkwürdigerweise teilweise synonym:

- Pass – als Reisepass, Impfpass, Gerätepass
- Ausweis – als Personalausweis, Fahrausweis, Mitgliedsausweis
- Schein – als Führerschein, Fahrschein, Seminarschein, Kraftfahrzeugschein
- Karte – als Fahrkarte, Visitenkarte, Kundenkarte, Geldkarte, Eintrittskarte
- Ticket – als Flugticket, Bahnticket
- Brief – als Kraftfahrzeugbrief, Gesellenbrief, Meisterbrief
- Zertifikate – als Herkunfts- oder Echtheitszertifikate, Digitales Zertifikat, Qualitätszertifikat
- Marken – als Briefmarken, Gebührenmarken oder Dienstmarken
- Siegel – als Prüfsiegel und Klebesiegel
- Zeugnis – als Schulzeugnis, Arbeitszeugnis, Führungszeugnis.

Die Gesamtheit von Eigenschaften einer Person oder einer Sache heißt *Idiosynkrasie*. Der Begriff der „Idiosynkrasie" bedeutet „eigentümliche Beschaffenheit und Eigenheiten einer Person". Damit ist die Idiosynkrasie ein grundlegender Begriff zur Identität. Eine Person oder eine Sache kann mithilfe von Eigenschaften (wie körperliche Eigentümlichkeiten, Attribut, Name, Anschrift, Kennzeichen, etc.) identifiziert werden. Wenn *alle relevanten* Eigenschaften einer Person oder einer Sache übereinstimmen, dann ist eine dahingehende eineindeutige Identität gegeben.

Die Idiosynkrasie einer Identität beinhaltet in der Regel einen mehrdimensionalen, aus Komponenten zusammengesetzten Satz von Attributen oder Daten. Diese oben gelisteten Identitätsdokumente haben meistens einen Formularcharakter und eine dahingehend modellhafte formale Struktur. In Personalausweisen – beispielsweise – stehen als Komponenten der Name, das Geburtsdatum, die ladefähige Anschrift, etc. In einem Bahnfahrschein finden wir die Fahrstrecke, das Datum, die Klasse, den Preis, etc. In einem Fahrzeugbrief stehen die Fahrzeugnummer, eine Reihe technischer Merkmale, die diversen Besitzer des Fahrzeugs, etc. pp.

➔ Identitäten beruhen auf einer modellhaften *Idiosynkrasie*. Teile der Idiosynkrasie – Untermengen der beschreibenden Attribute – können in Identitätsdokumenten (formal) aufgezeichnet werden. Sie bezeichnen nicht notwendigerweise eine bestimmte Person oder Sache, aber mindestens eine Legitimation, Berechtigung oder eine Funktion – sonst sind sie sinnlos.

Einzelne Attribute einer Identität – Teile der Idiosynkrasie – können sich teilweise ändern. Das ist bei Personen ei Teil des Alterungsprozesses, bei Sachen können einzelne Teile ausgetauscht oder technisch verändert werden. Es ist aktuell – immer noch – ungeklärt, welcher Anteil einer Idiosynkrasie erhalten bleiben muss, damit eine Identität einer Person oder Sache nicht völlig zerstört wird – sondern (wieder-)erkennbar bleibt.

Verknüpfung von Identitätsdokumenten mit realen Personen oder Sachen

Viele Identitätsdokumente sind gegenüber der Person oder der Sache *nicht neutral*: Sie bilden die Identitäten im engeren Sinn. Ein Personalausweis gehört eineindeutig zu einer ganz bestimmten Person – und zu keiner anderen. Ein Fahrzeugbrief gehört zu genau einem bestimmten Fahrzeug. Einige Identitäten sind hingegen *Personen-neutral*, aber nicht *Personen-unabhängig*. Viele Fahrscheine oder Eintrittskarten sind gegenüber der Person neutral – wer sie vorzeigt, der kann fahren oder teilnehmen. Bei einem Türschlüssel ist es egal, *wer* damit ein Schloss öffnet, aber *ohne* eine Person kann das Schloss nicht geöffnet werden. Man kann in diesem Sinn auch Banknoten als – Personen-neutrale – Identitätsdokumente auffassen. Sie weisen ihrem Besitzer ein Bargeldvermögen zu und berechtigen ihn damit zum Begleichen von Geldschulden.

Für die Nicht-Neutralität eines Identitätsdokuments in Bezug auf eine Person oder Sache muss im Identitätsdokument mindestens eine Autorisierungs-Komponente vorhanden sein, die einen fälschungssicheren Bezug zur identifizierenden Person oder Sache herstellt. Personalausweise weisen etwa ein Lichtbild, einen Fingerabdruck, etc. auf. Sie verbinden das Dokument eineindeutig mit einer einzigen konkreten Person. Die Fahrgestellnummer – am Fahrzeug eingeprägt und im Fahrzeugbrief aufgeführt – bindet die Idiosynkrasie im Fahrzeugbrief damit an ein bestimmtes konkretes Fahrzeug. Ein Datenträger mit der Idiosynkrasie-Komponente kann als Chip etwa einem Haustier implantiert werden (vulgo ein „gechipter Hund") und schafft so eine eineindeutige Verbindung zwischen dem konkreten Tier und (s)einem Heimtierausweis.

➔ Eine Verknüpfung von Identitätsdokumenten mit realen Personen oder Sachen basiert auf Autorisierungsmerkmalen. Diese können *passiv* sein, wie Lichtbilder, Fingerabdrücke, Körpermerkmale und daher auch bei Identitätsfeststellungen gegen den Willen der Betroffenen eingesetzt werden. Oder *aktiv* verwendet werden, wie Passwörter, Parolen, PINs, wenn sie für eine Legitimation eingesetzt werden sollen.

Die Autorisierungsmerkmale haben in der Regel eine begrenzte zeitliche Gültigkeit und müssen daher regelmäßig erneuert werden. Einige Merkmale wie TANs sind nur einmal pro Einsatz verwendbar.

Emission und Akzeptanz der Identitätsdokumente, Selbst-Souveräne Identität SSI, Protokolle

Identitätsdokumente – Pässe, Ausweise, Digitale Identitäten – werden

- von *Emissions-Stellen (Emittenten)* ausgestellt oder ausgegeben, dies erfolgt
- im Rahmen eines spezifischen *Registrierungs-Protokolls.*

Sie werden

- einem *Besitzer* oder Benutzer zugeordnet – und werden von diesem *geeignet aufbewahrt*

und

- von *Akzeptanz-Stellen (Akzeptoren)*
- im Rahmen eines weiteren spezifischen *Übermittlungs-Protokolls*

anerkannt – oder zurück gewiesen.

Dabei bilden Emittent und Akzeptor ein symmetrisches Verhältnis: Der Emittent wird das Identitätsdokument so zu gestalten versuchen dass es – gemäß eines entsprechenden Standards –von einem Akzeptor über das Übermittlungs-Protokoll anerkannt werden kann. Emittent und Akzeptor bilden ein Doppeltes Netz – was auch als „Henne-Ei-Problem" bekannt ist. Die Emission ist ohne eine Akzeptanz – und umgekehrt – jeweils sinnlos. Für selbstsouveräne Identitäten SSIs ist der Aufbau des erforderlichen Doppelten Netzes eine nicht geringe organisatorische und ökonomische Herausforderung.

Für eine „Sichere Identität" sind drei der oben genannten Faktoren von besonderem Interesse:

- Das *Registrierungs-Protokoll* regelt, wie der Inhaber ein Identitätsdokument erhält. Das erfolgt auf aktiven Antrag, etwa im Fall eines Reisepasses oder eines Führerscheins. Oder als passive Zuteilung, wie bei Werks- oder Studierendenausweisen, der sich die Betroffenen kaum entziehen können.
  Eine Vielzahl von Digitalen Nutzungsidentitäten – etwa im E-Commerce – werden den Kunden mit Nachdruck offeriert. Nur mit einer Registrierung, oft mit der Verwendung einer Email-Adresse als Identifier und einem Passwort als Autorisierung, ist ein Zugang zu den Systemen möglich.
  Es existiert ein Zielkonflikt zwischen der Sicherheit der Registrierung und dem dafür seitens des Nutzers zu erbringenden Aufwand, welcher wiederum in Relation zum Nutzwert des Identitätsdokuments gesehen werden muss. Der Aufwand kann als Prüfung und vorherige Schulung wie bei Führerscheinen, oder aber als Kompliziertheit des zu durchlaufenden Registrierungs-Protokolls gestaltet sein. Ist der Aufwand zu hoch, leidet die Verbreitung der Identitätsdokumente.
- Die *Aufbewahrung* ist – im einfachen Fall physischer Ausweise – eine verlustsichere Aufbewahrung in der Zuständigkeit der Inhaber. Im immateriellen Fall der Passwörter und PINs muss sich der Inhaber diese nicht nur irgendwie „merken" sondern auch unter Verschluss halten – was in der Tat sehr aufwändig sein kann, da es für viele Personen um etliche – dutzende –Passwörter geht. Eine Lösung können Zertifikate im Web-Browser, E-Mail-Client, etc. sein, die eine „sichere" Verbindung zu einem Serverrechner aufbauen, die Identität des Rechners überprüfen und die Daten verschlüsselt übertragen.

Vermehrt kommen *Passwort-Manager* oder *Wallets* zum Einsatz, die Benutzernamen und Passwörter verwalten, der Zugang erfolgt über ein „Masterpasswort", das anstelle von vielen verschiedenen Passwörtern gemerkt werden muss. Beim Verlust oder – ungewollter – Offenlegung des Masterpassworts sind unter Umständen alle Passwörter verloren. Bei Cloud-basierten Passwort-Manager-Diensten werden sensible Daten einem – vertrauenswürdigen? – Unternehmen anvertraut.
Ein – sinnvolles – Identitätsmanagement berücksichtigt auch den Fall, dass die Aufbewahrung scheitert. So werden Ausweise bei Verlust durch die Emittenten ersetzt – nach Maßgabe entsprechender Regelungen. Software-Systeme haben eine „Passwort vergessen"-Funktion.

- Das *Übermittlungs-Protokoll* – siehe hierzu die Ausführungen weiter unten.

Im wichtigsten Spezialfall ist eine *amtliche Stelle* der Emittent eines Identitätsdokuments. Dies ist bei Personalausweisen, Führerscheinen, Kraftfahrzeugbriefen, Banknoten, etc. der Fall. Dabei werden Identitäten von Personen oder Sachen *zentral* verwaltet. Die Akzeptanz ist weitgehend gesetzlich geregelt. Kann ein amtlicher Personalausweis vorgelegt werden, so *muss* er anerkannt werden – und damit ist die Ausweispflicht der entsprechenden Person erfüllt. Mit Euro-Banknoten der Europäischen Zentralbank kann eine Zahlschuld in Deutschland beglichen werden; der Gläubiger *muss* die Banknoten – unbegrenzt – annehmen. Im Gesetz über die Deutsche Bundesbank (BbankG) heißt es in § 14 *„Auf Euro lautende Banknoten sind das einzige unbeschränkte gesetzliche Zahlungsmittel.*"

➔ Amtliche Identitätsdokumente – Personalausweis, Reisepass – sind unentbehrlich, wenn es um gerichtsnotorische Vorgänge und eine beweiserhebliche Feststellung von Identitäten geht. Die Fälschungssicherheit von amtlichen Identitätsdokumenten spielt eine zentrale Rolle und spiegelt wider sich in deren Nicht-Duplizierbarkeit, der Integrität der Dokumente und der Autorisierung der Benutzer.

Nicht-zentral und nicht-amtlich verwaltete Identitätsdokumente dienen der selbst definierten Identität von Personen und Sachen. Hierfür hat sich der Begriff der „Selbst-souveränen Identität" (*Self-Sovereign Identity – SSI*) eingebürgert. Die SSI sind als solche nichts Neues, sondern seit langer Zeit und sehr häufig im Alltag anzutreffen. Es gibt viele Beispiele für SSI-Identitätsdokumente:

- Gedruckte Visitenkarten mit Namen und Berufs- und Büro-Kontaktdaten.
- Firmenausweise, die den Zugang zu Werksgelände regeln, eventuell mit RFID-Chips zum Öffnen von Schranken und Türschlössern.
- Kundenkarten, die der Identifikation von Kunden und der Verwaltung von Rabatten („*Loyalty*") dienen.
- User-Identifier, die den Zugang zu einem IT- oder Software-System regeln, kombiniert mit entsprechenden Passwörtern zur Legitimation des Benutzers.
- Gerätekarten zur eindeutigen Identifikation von Sachen, wie Geräten und Apparaten im Falle eines Gewährleistungsanspruchs.
- Eintrittskarten aller Art zu Veranstaltungen, Fahrscheine für den ÖPNV .
- Währungssurrogate und „Eigenes Geld" in Form von Gutscheinen, Rabattmarken, Bitcoins, etc.
- und viele andere mehr.

➔ Auch die SSI-Dokumente haben Berechtigungen und Befugnisse zur Folge. Bei der Fälschungssicherheit von SSI-Identitätsdokumenten spielen daher die Nicht-Duplizierbarkeit, Integrität der Dokumente und Autorisierung der Benutzer ebenfalls eine spezifische Rolle. Entscheidend sind die jeweiligen Sicherheitsanforderungen der Anwendungsszenarien, die mit den SSI-Identitätsdokumenten verknüpft sind.

Eine Mischform stellen SSI-Identitätsdokumente dar, die einem *zentralen multilateralen Standard* genügen. Diese sind zwar nicht-amtlich, aber standardisiert. Dies ist etwa bei Geld- und Kreditkarten der Fall, die nach Maßgabe ihrer standardisierten Gestaltung von einer Vielzahl von Akzeptanzstellen anerkannt werden. Andere Beispiele sind das „eduroam"-Zugangsprotokoll für WLANs in akademischen Einrichtungen, oder international gültige Flug- und Bahnfahrscheine. Die Etablierung solcher Standards ist ebenfalls mit dem Aufbau des Doppelten Netzes der Emittenten und Akzeptoren verbunden – und kann sehr aufwändig und teuer sein. Eine noch einmal ganz andere Frage ist, inwieweit Identitätsdokumente auch international anerkannt werden. Dies gestaltet sich bei den SSIs zum Teil weit einfacher als bei nationalen amtlichen Dokumenten. Die universelle Akzeptanz von amtlichen Identitätsdokumenten ist ein (noch) unerreichtes Ideal.

Mit den Identitätsdokumenten sind *Übermittlungs-Protokolle* verbunden, mit denen sie vom Besitzer oder Benutzer an den Akzeptor übergeben werden, um eine Legitimation – Berechtigung oder Befugnis – zu erreichen. Zu nennen sind, mit Beispielen:

- *Vorzeigen* des Identitätsdokuments, mit einer Inaugenscheinnahme durch den Akzeptor: Vorzeigen eines Personalausweises zur Alterskontrolle, oder eines Führerscheins bei der Verkehrskontrolle.
- *Übergeben* an den Akzeptor als den dann neuen Besitzer: Gutscheine, Vouchers, Banknoten.
- „*Entwerten*“ (versus englisch „*Validation*“) der Identitätsdokumente, wodurch eine Blanko-Berechtigung „entwertet“ und zu einer konkreten Berechtigung „validiert“ wird: Stempeln von ÖPNV-Fahrscheinen mit dem Tagesstempel, Abreißen eines Entwertungsteils bei Eintrittskarten, Lochen von Fahrkarten.
- *Modifizieren*: Anbringen von Visa in Reisepässen, Anbringen von Stempelzeichen in Kunden-Treue-Rabattkarten im Einzelhandel.
- *Elektronisches Lesen* von Digitalen Identitätsnachweisen: Die Idiosynkrasien sind als Daten auf Magnetstreifen, RFIDs, Chips mit Kontakten, Optischen Mustern, etc. gespeichert und können entsprechend maschinell – elektro-optisch – erfasst werden.
- *Kombiniertes Elektronisches Lesen mit Autorisierungen*: Das elektronische Lesen von Digitalen Identitätsnachweisen wird kombiniert mit der Autorisierung des Besitzers: Zum Datensatz muss ein Passwort, eine PIN, oder extra auf separatem Weg übermittelte TAN eingegeben werden, um den Datensatz als für den Besitzer authentisch zu validieren. Diese Übermittlungs-Protokolle müssen dafür mit einem vorherigen Registrierungs-Protokoll kombiniert werden. In den Registrierungs-Protokollen werden neben den Datensätzen der Identifier und den Datenträgern auch die zusätzlichen Mechanismen (Passwörter, PINs, TANs, etc.) festgelegt.

Die Übermittlungs-Protokolle haben für die Anwender einen verschieden hohen Aufwand, der sich natürlich in der Verbreitung der Gesamtszenarien niederschlägt. Einige Anwendungen der Elektronischen Identität haben eine zum Teil recht geringe Verbreitung, weil die Übermittlungs-Protokolle, inklusive der vorher nötigen Registrierungs-Protokolle, mit einem (zu) hohen Aufwand verbunden sind, oder weil der Aufbau des notwendigen Doppelten Netzes (noch) nicht gelungen ist.

Ontogenese und Fälschungssicherheit der Identitätsdokumente

Identitätsdokumente von Personen und Sachen sind *Artefakte* – sie entstehen nach Maßgabe eines definierten Prozesses; sie werden durch die Emittenten produziert. Bei *Personen* ist eine Anmeldung bei ihrer Geburt, am Standesamt des Geburtsortes nach dem Personenstandsgesetz die Regel. Das ist quasi die „Schöpfung“ der *wahren – quasi axiomatischen – Personenidentität*. Die darauf basierende Geburtsurkunde mit Namen und Geburtsdatum und Geburtsort ist *die Referenz* für das Ausstellen aller weiteren Identitätsdokumente, speziell des amtlichen Personalausweises und Reisepasses. Bei Findelkindern wird das Geburtsdatum geschätzt, bei Immigranten ohne jegliche Papiere versucht man diese Basisparameter der Identität in einer Identitätsfeststellung durch eine Befragung zu erfahren. Dem Verfasser dieses Textes ist ein Fall persönlich bekannt, wo einem männlichen Kind versehentlich beim Personenstandsregister eine – *axiomatisch wahre* – weibliche Identität zugewiesen wurde. Das hatte in der Bundesrepublik der 1980er-Jahre durchaus seine Vorteile, angesichts der damals noch bestehenden Wehrpflicht.

Bei *Sachen* werden von den Herstellern typischerweise Seriennummern (*Manufacturer Serial Number* MSN) als eineindeutige Bezeichnung eines Produkts vergeben. Nach Norm ISO 8000-2 ist die Definition der MSN „*Nummer, die zur Identifizierung eines einzelnen Vorkommens eines Erzeugnisses verwendet wird*“. Bei Software müssen MSN in der Regel über das Netz angegeben werden, um das System nach einer Produktaktivierung benutzen zu können. Die MSNs der Software können eventuell mit den MSNs der Hardware verbunden werden. Ziel ist jedenfalls das Vermeiden der illegalen Nutzung von Software. Bei Fahrzeugen wird eine *Vehicle Identification Number* VIN von den Hersteller nach ISO-Norm 3779 vergeben. Die VIN dienen zu Garantiezwecken und zum Qualitätsmanagement, oder aber zur Identifikation gestohlener Fahrzeuge.

Ein wichtiger Qualitätsaspekt von Identitätsdokumenten ist deren *Fälschungssicherheit*. Identitätsdokumente müssen fälschungssicher – oder *authentisch* – sein. Das lateinische „*authenticus*“ bedeutet etwa „verbürgt, zuverlässig, echt“. Bei der Fälschungssicherheit von amtlichen Identitätsdokumenten und SSIs geht es um

- ihre Nicht-Duplizierbarkeit,
- die Integrität der Dokumente,
- die Verifikation der enthaltenen Daten, und
- die Autorisierung ihrer Benutzer.

Das Anstreben von Fälschungssicherheit hat erstens *ökonomische Gründe*. Identitätsdokumente in der Form von Fahrscheinen, Eintrittskarten, Banknoten, Briefmarken, Fahrzeugbriefen, etc. haben einen mit ihrem Nutzwert verbundenen Marktwert und Preis. Sie können – beziehungsweise sie müssen – käuflich erworben werden. Die Fälschungssicherheit bedeutet, dass die Dokumente nicht durch eine Fälschung ihre Knappheit verlieren und wertlos werden.

Das Anstreben von Fälschungssicherheit hat zweitens *juristische Gründe*. Bei den nicht Personen-neutralen Identitätsdokumenten ist man an einer Fälschungssicherheit der Dokumente interessiert. Man möchte nicht, dass Personen Rechte erlangen, die ihnen nicht zustehen – etwa über einen gefälschten Führerschein, oder durch die Verwendung von falschen Ausweisen. Man hat kein Interesse daran, für eine Straftat oder Handlung zu haften, die jemand anders mit einer „gestohlenen Identität" – etwa einem gefälschten Personalausweis – begangen hat.

➔ Bei der Fälschungssicherheit sind die vier Aspekte der Nicht-Duplizierbarkeit, der Integrität der Dokumente, der Verifikation der enthaltenen Daten, und der Autorisierung der Benutzer *unabhängig voneinander und separat* zu betrachten.

Das Problem der *Nicht-Duplizierbarkeit* der Identitätsdokumente wurde historisch durch physisch-mechanische Kompliziertheit gelöst – wie kompliziert geformte Türschlüssel und Siegel. Später hat man durch drucktechnische Komplikationen, wie Wasserzeichen, Hologramme, etc. die Ausweisdokumente, Eintrittskarten, Banknoten, etc. einigermaßen fälschungssicher gestaltet. Es besteht seit jeher ein gewisser Wettbewerb zwischen der verfügbaren Technik auf Seiten der Emittenten versus der verfügbaren Technik auf der Seite der Fälscher. Digitale Identitätsdokumente sind als solche leicht zu kopieren und zu duplizieren. Man sichert sie daher zusätzlich ab, durch Merkmale der Autorisierung, oder durch die Verwendung technisch schwierig kopierbarer Datenträger.

Das Problem der *Integrität* der Dokumente wird durch Komplikationen im verwendeten Medium realisiert – oft durch Spezialpapiere. Eine entsprechende Technik garantiert Nicht-Radierbarkeit und Lichtechtheit. Dadurch sind Änderung von Teilen einer Idiosynkrasie erkennbar: Die Änderung des Geburtsdatums einer Person, unter Beibehaltung der anderen Daten, dürfte in einem Personalausweis kaum möglich sein. Ähnlich leicht erkennbar wäre die Änderung des Nennwerts einer Banknote. Digitale Identitätsdokumente erreichen eine Integrität durch die Verwendung von digitalen Prüfwerten, die erkennen lassen, ob ein Dokument verändert worden ist. So werden solche Prüfwerte etwa mit dem *Secure Hash Algorithm* SHA berechnet. Der SHA findet auch Verwendung im Metier der Integrität der „Block"-Dokumente und ihrer seriellen Verkettung in Form einer „Blockchain". Die Integrität von Identitätsdokumenten auf der Basis einer Blockchain mit Verwendung des SHA-3 ist praktisch absolut.

Die klassische *Autorisierung* der Identität ist die Unterschrift der agierenden Inhaber-Personen. Digitale Identitätsdokumente haben als Instrument der Autorisierung ihrer Benutzung oft den Einsatz zusätzlicher Passwörter oder Kennzahlen, die den gerade benutzten Datensatz legitimieren. Klassisch ist das Password in Verbindung mit einen User-Namen (Benutzername-Kennwort-Systemzugang) – oder auch die PIN bei der Benutzung einer girocard oder Kreditkarte. Das Password oder der PIN ist – vergleichbar einem Türschlüssel – sorgfältig gegen den Zugriff Unbefugter zu schützen. Die PINs werden bei der girocard oder dem elektronischen Personalausweis über separate und abhörsichere Tastaturen eingegeben – was wiederum einen zusätzlichen Aufwand bedeutet. Wird die PIN einer girocard offenbart, so wird sie neutral gegenüber der eigentlich berechtigten Person. Dieser letztere Aspekt wird durch die Verwendung von Einmalkennwörtern, wie den Transaktionsnummern TANs vermieden. SSI-Identitätsdokumente benutzen in der Regel selbst gewählte Passwort-Autorisierungen. Letztere werden von den Emittenten in eigener Verantwortung im Rahmen einer Benutzerregistrierung angelegt.

Elektronische Identität (eID)

Mit der Entwicklung der Informationsgesellschaft ist die Verwendung von *Digitalen „Elektronischen" Identitäten eID* zum Alltag geworden. In Analogie zu den oben dargestellten Aspekten gibt es *amtliche und SSI-eID*. Die amtliche eID ist der (neue) Elektronische Personalausweis.

Die einfachsten SSI-eID sind Datensätze, die einen Teil der Idiosynkrasie einfach als (ungeschützte) Zeichenketten darstellen – sie sind sehr einfach zu fälschen. Sehr gebräuchlich sind SSI-eID für das Log-in in irgendwelche Systeme mit einer Benutzerbezeichnung und einem Passwort. Ähnlich einer Insignie darf ein solches Passwort nicht in die „falschen Hände" gelangen. Diverse eID werden pro Person dutzendfach verwendet, um auf alle möglichen Systeme im Bereich der Verwaltung und des Handels zuzugreifen. Eine amtliche eID mit einer Zertifizierung

und einer Autorisierung – etwa durch einen PIN – kann auch als elektronische Unterschrift benutzt werden, um Dokumente digital zu signieren.

Prinzipiell sind die eID von einem Trägermedium unabhängig. Zur Verwendung kommen sogenannte „Apps“ auf Smartphones, elektronische Ausweise in Kartenform, RFID-Chips, etc. Die physische Realisierung als separate Karte ist möglicherweise deshalb attraktiv und sehr verbreitet, weil die der traditionellen Form eines Insignie nahe kommt.

Legitimationsprüfungen – mit eID

Legitimationsprüfungen stellen eine Sonderform der Identitätsfeststellung dar. Es geht um die Feststellung einer Legitimation – also Berechtigung oder Befugnis – nach Maßgabe einer amtlich-öffentlichen oder privaten Verordnungslage. Legitimationsprüfungen basieren in der Regel auf einer oder nur sehr wenigen Komponenten der Idiosynkrasie.

Typische Beispiele für Legitimationsprüfungen sind die Feststellung

- der Volljährigkeit – nicht unbedingt des Lebensalters – etwa beim Erwerb alkoholischer Getränke im Verbrauchermarkt.
- einer (deutschen) Staatszugehörigkeit, oder der Gültigkeit eines Aufenthaltstitels.
- von korrektem Namen und korrekter ladefähiger Anschrift eines Kunden im Handel.
- von korrektem Namen und ladefähiger Anschrift bei der Eröffnung von Konten bei Kreditinstituten.
- der vollständigen Personenstandsdaten bei notariellen Beurkundungen, bei Behörden, etc.

Nach dem Geldwäschegesetz (GWG) müssen sich die Einzahler von Bargeld mit korrektem Namen und korrekter ladefähiger Anschrift legitimieren. Legitimationsprüfungen nach dem GWG müssen mit einem amtlichen (elektronischen) Personalausweis oder einem Reisepass erfolgen. Ersatzweise werden Identitätsdokumente verwendet, die wiederum auf diese amtlichen Identitätsdokumente zurückgeführt werden können. Im Prinzip werden für Legitimationsprüfungen drei Verfahren angewendet:

- Die unmittelbare persönliche Inaugenscheinnahme des vorgezeigten physischen Identitätsdokuments, wie dem Personalausweis, eventuell wird eine Ablichtung zu den Akten genommen.
- Das Video-Ident-Verfahren – ein Evidenz-basiertes Verfahren – zur (Online-)Identifizierung.
- Der elektronische Identitätsnachweis mit der Online-Ausweisfunktion.

Das *Video-Ident-Verfahren* ist eine Online-Identifizierung per Video-Chat. Es wird vor allem von Online-Banken und Direktbanken zur Legitimation ihrer prospektiven Kunden genutzt. Das Video-Ident-Verfahren arbeitet mit einer Internetverbindung, die live-Videos über ein Smartphone, Tablet oder einen PC mit Webcam übertragen kann. Es wird ein gültiger Ausweis oder Reisepass benötigt. Nicht unüblich ist das Szenario, in dem der prospektive Kunde von der Bank per E-Mail eine URL erhält, die auf die WWW-Page eines unabhängigen Identifizierungs-Dienstleisters verweist, der nach dem Vertrauensdienstegesetz zertifiziert ist, und die Online-Identifizierung per Video-Chat durchführt.

Für das Video-Ident-Verfahren muss der zu identifizierende prospektive Kunde selbst vor der Kamera zu sehen sein. Er muss sowohl die Vorder- als auch die Rückseite seines Personalausweises – lesbar – in die Kamera halten. Manche Identifizierungs-Dienstleister versenden zusätzlich eine TAN per SMS, die mit eingegeben werden muss. Danach gilt die Identifikation als erfolgt, aufgrund dieser Legitimation könnten mit der Bank Geldgeschäfte abgewickelt werden. Das Video-Ident-Verfahren kann der Kunde – im Gegensatz zum Post-Ident-Verfahren – komplett online abwickeln. Für das Post-Ident-Verfahren hingegen muss der Kunde persönlich in einer Deutsche-Post-Filiale vorsprechen, um sich seine Identität dort bestätigen zu lassen.

➔ Sowohl das Post-Ident-Verfahren, als auch das Video-Ident-Verfahren sind nach dem Geldwäsche-Gesetz die zulässige Basis für Legitimationen. Nichtsdestoweniger kann nicht verkannt werden, dass ein gut gefälschter Ausweis über das Video mit seiner limitierten Bildqualität möglicherweise nicht als ein solcher erkannt werden kann. Da diese Evidenz-basierten Verfahren einen gewissen Personal- und Zeit-Aufwand mit sich bringen, sind die nicht beliebig skalierbar.

Auf der Grundlage des Gesetzes über eine Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums mit Funktion zum *elektronischen Identitätsnachweis* („eID-Karte-Gesetz“ – eIDKG) können Legitimationen

elektronisch erfolgen. Der entsprechende Dienst lässt sich für den Endanwender relativ komfortabel realisieren, was die Abbruchquote beim Abschluss rechtssicherer Geschäfte und Verträge – „*onboarding*“ – zu verringern vermag.

Eine zentrale Rolle spielt beim *elektronischen Identitätsnachweis* die Anwendungssoftware der „AusweisApp2“, die für PCs, Smartphones, Tablets, etc. gratis verfügbar ist. Mit ihr ist eine elektronische Legitimation über das Internet mit dem neuen deutschen Personalausweis oder dem elektronischen Aufenthaltstitel möglich. Die AusweisApp2 baut eine verschlüsselte Verbindung zwischen dem Ausweis auf dem Kartenleser und einem eID-Server des sogenannten „Dienstanbieters“ her. Ein Dienstanbieter ist etwa eine Behörde, ein Betreiber eines E-Shops, oder auch eine Arztpraxis. Für diesen Vorgang wird ein Smartphone als NFC-Kartenleser benutzt, die PIN wird über das Smartphone abhörsicher eingegeben. Der vordem erforderliche Gebrauch eines separaten Lesegerätes mit separater Tastatur – ein erhebliches Akzeptanzhindernis – entfällt damit. Der Prozess läuft auf der Seite des Dienstanbieters vollautomatisch. Da es keinen großen Personalaufwand gibt, ist der *elektronische Identitätsnachweis* leichter skalierbar für Massenanwendungen.

Der Dienstanbieter stellt – in Vorbereitung der Legitimation – einen begründeten Antrag bei der Vergabestelle für Berechtigungszertifikate (VfB) mit Angabe der Datenfelder, die er auslesen möchte. Das eigentliche Berechtigungszertifikat wird von einem privaten Berechtigungszertifikate-Anbieter (BerCA) erworben. Das Zertifikat des eID-Servers wird vom Ausweis des Nutzers überprüft, ebenso wie der vorgelegte elektronische Ausweis seitens des eID-Servers selbst. Nach erfolgreichem Test kann der Nutzer die vom Dienstanbieter verlangten Daten mit einer – persönlichen, geheimen – PIN freizugeben und so übermitteln. Interessant für den Aufbau des Doppelten Netzes ist der Umstand, dass für alle neuen Personalausweise seit dem Mai 2017 die eID-Funktion standardmäßig aktiviert ist und nicht mehr ausgeschaltet werden kann. Im Notfall kann der Ausweisinhaber über ein Sperrkennwort die eID-Funktion zentral sperren lassen.

- ➔ Mit der dynamischen Weiterverbreitung der standardmäßigen amtlichen eID-Funktion besteht die berechtigte Hoffnung, dass mit dem *elektronischen Identitätsnachweis* eine gute Basis für einen allgemeinen Identitätsnachweis für Legitimationen im Rahmen der Betrugsprävention („*Fraud Protection*“) im Handel gegeben ist.

Der Dienstanbieter betreibt – oder lässt betreiben – einen eID-Server, der die Kommunikation mit dem Personalausweis herstellt. Gemäß der EU-Verordnung Nr. 910/2014 (eIDAS-Verordnung) akzeptieren alle Organisationen, die öffentliche digitale Dienste in einem EU-Mitgliedstaat bereitstellen, ab dem 29. September 2018 die elektronische Identifizierung, ausgestellt in einem der EU-Mitgliedstaaten.

Identitäts-Management in der unternehmerischen Praxis – Betrugsprävention

Im Zuge der fortschreitenden Digitalisierung ist es in der entwickelten Informationsgesellschaft – selbstredend – nicht mehr möglich, ein archaisch-ursprüngliches Identitätsmanagement auf der Basis des unmittelbaren psychosozialen Vertrauens zu realisieren [Brun21]. Die zu adressierenden sozialen und ökonomischen Kontexte sind zu umfangreich geworden – man kann in der täglichen Lebenspraxis nicht mehr alle Personen persönlich kennen.

Ein Identitäts-Management ist kein Selbstzweck. Es sind durchaus die allgemeinen Prinzipien des Informationssystem-Managements anwendbar, es gibt eine Hierarchie in der Planung:

i. Welches (Unternehmens-)Ziel soll mit
ii. welchen Szenarien und Nutzwerten,
iii. welchen Prozessen und mit
iv. welcher Technologie erreicht werden?
v. Mit welchen Projekten lassen sich diese Ziele erreichen?
vi. Wie lassen sich die Systeme betreiben?

Es kann zu bedauerlichen Fehlinvestitionen führen, wenn eine – quasi „aktuelle“ – Technologie der Ausgangspunkt der Überlegungen ist – im Sinne von „wir investieren innovativ in SSIs oder Blockchain“ – dieser Ansatz kann zu einer bedauerlichen Kombination von hohem finanziellen Aufwand mit unbrauchbaren Ergebnissen führen.

In der Folge stellen sich einige Gestaltungsfragen zu Digitalen Identitätsdokumenten in der Praxis:

- Welche Attribute und Elemente der Idiosynkrasie soll das Identitätsdokument abbilden, beziehungsweise speichern?
- Welche sinnvollen Datenschutz-freundlichen minimalen Teilmengen („*Application Profiles*“) gibt es? Warum ist der Zugriff auf Daten der amtlichen Identitätsdokumente berechtigt und begründet?
- Welche Benutzer benutzen welche Verfahren – Video-Ident, Post-Ident, eID – um SSI-Identitätsdokumente mit amtlichen Identitätsdokumenten zu verknüpfen?
- Welche Formen der Fälschungssicherheit der Identitätsdokumente sind angebracht? Welcher Aufwand für Nicht-Duplizierbarkeit, Integrität und Autorisierung ihrer Benutzer ist sinnvoll?
- Wie gestaltet sich die konkrete Akzeptanz und Nutzung der (SSI-)Identitätsdokumente, auf der Basis welcher Nutzwerte?

Ein zentraler Nutzwert für ein Identitätsmanagement ist die Vermeidung von Betrug. In der gewerblichen Wirtschaft läuft eine Forderung ins Leere, wenn die Identität des Geschäftspartners gefälscht ist, und Daten wie die Rechnungsanschrift oder die Lieferanschrift nicht korrekt sind. Eine Forderung ist nicht werthaltig, wenn sie auf einem dahingehend nichtigen Kaufvertrag basiert, da eine unbefugte Person eine Bestellung vorgenommen hat. Eine Forderung ist auch dann nicht werthaltig und wird zurückgewiesen, weil der ordnungsgemäße Eingang oder Erhalt einer Ware bestritten wird. Ein entsprechendes Identitäts-Management kann die Frage beantworten, ob ein Geschäft mit einem bestimmten Geschäftspartner sinnvoll ist und die Geschäftsvorgänge absichern. Im B2B ist für Mahnverfahren die Gerichtsverwertbarkeit einer Identität erforderlich. Generell ist für das gerichtliche Mahnverfahren die Gerichtsverwertbarkeit einer Identität unabdingbar, sowohl im B2B- als auch im B2C-Geschäft. Die aus dem B2C-E-Commerce bekannten Absicherungen greifen im B2B aufgrund der weit höheren Umsatzvolumina nicht.

Sowohl im B2B als auch im B2C haftet in Betrugsfälle der Händler immer für das sogenannte „Veritätsrisiko“. Als Verität bezeichnet man die (Rechts-) Beständigkeit von Forderungen. Der Kunde verpflichtet sich für den Bestand der Forderungen dem Grund und der Höhe nach, einschließlich der vollständigen und mangelfreien Erbringung der zugrunde liegenden Leistungen, verschuldensunabhängig einzustehen Das Veritätsrisiko wird nicht von einer (Vertrauensschaden-) Versicherung getragen – ist von daher also besonders kritisch. Die einschlägigen Zahlungsgarantieanbieter haben in ihren Allgemeinen Geschäftsbedingungen AGB oft die Bedingung, dass die Identität der Kunden mittels einer Einwohnermeldeamtsanfrage nachgewiesen werden muss. Sonst liegt ein Betrugsfall vor, für den der Händler und nicht der Zahlungsgarantieanbieter haftet. Die Zahlungsgarantieanbieter sind dahingehend im B2C großzügig aufgrund der geringeren durchschnittlichen Forderungsbeträge, im B2B-Factoring ist eine solche kulante Einstellung in der Regel nicht gegeben.

Universelle Identitäts-Ökosysteme – das „Henne-Ei-Problem“ des Doppelten Netzes

Beim Projekt „ID-Ideal – Schaufensterregion Sachsen“ [Idid21] heißt es: „*Im Alltag weist man sich (…) durch Mitgliedsausweise oder Urkunden aus. Wenn man diese digital nutzen möchte, muss man sie erst umständlich einscannen und hochladen. In der digitalen Welt weist man seine Identität mittels Benutzerkonten nach. Sie enthalten aber nur Teile der persönlichen Daten und können oft nur bei wenigen Onlinediensten eingesetzt werden*.“

Darauf folgt in [Idid21] ein Plädoyer für ein „umfassendes“ Identitätsmanagement mit einem „Wallet für Alles“: „*Um eine möglichst flächendeckende Anwendung zu erreichen, ist die Interoperabilität zwischen den einzelnen technischen Lösungen nötig. Apps auf dem Smartphone, die als digitale Brieftasche (‚Wallet‘) fungieren, erlauben das Speichern von digitalen Identitäten und weiterer digitaler Nachweise wie Zeugnisse, Urkunden, Berechtigungen und Tickets. Sie nehmen gesicherte Angaben entgegen, die verschiedene Behörden und Institutionen als digitale Identitäten ausgeben. Dafür sind einheitliche digitale Formate und Schnittstellen erforderlich. Wenn sich Anwenderinnen und Anwender dann bei Behörden oder Unternehmer mit ihrer digitalen ID ausweisen wollen, müssen auch diese über die erforderlichen Schnittstellen verfügen. Das Zusammenspiel dieser Interaktionspartner findet in ‚ID-Ökosystemen‘ der jeweiligen Branchen statt. Die Standardisierung und damit die Interoperabilität dieser Ökosysteme will ID-Ideal mit dem ‚ID-Ideal Trust Framework‘ als neutrale, gemeinsame Basis vorantreiben.“*

Es ist offen, inwieweit sich solche *universellen Identitäts-Ökosysteme* verbreiten werden. Das Übergeben aller persönlichen Identitätsdokumente an ein einziges Meta-System – Passwort-Manager, Wallet, etc. – bedeutet für die Benutzerpersonen eine nicht unerhebliche Risikokonzentration. Die Frage ist, ob man den Betreibern solcher – *zuverlässiger?* – Systeme im klassischen Sinn – *wirklich? – vertrauen* kann, und wie etwaige Fehlfunktionen oder ein Ausfall der Systeme adäquat zu adressieren sind.

Fazit und Offene Fragen

Die sichere Identifikation von Personen, Dokumenten und Objekten ist nicht nur eine wesentliche Vorrausetzung, sondern auch ein Treiber für die Digitalisierung von Prozessen in Verwaltung, Wirtschaft und Gesellschaft [eco21]. Aber im Sommer 2021 sind viele Identitäten (noch) nicht digitalisiert – und es konnte in diesem Beitrag gezeigt werden, dass insbesondere die *vertrauensvollen Identitäten gar nicht digitalisiert werden können*. Die auf Benutzernamen und Passwort basierenden Mechanismen sind die am häufigsten verwendeten digitalen Lösungen. Andere Techniken konnten sich in der Breite bislang nicht durchsetzen. Im privaten Bereich sind SSIs wie Single-Sign-On-Dienste wie „Shibboleth“ etwas weiter verbreitet: Hier melden sich Benutzer sich nur einmal an, um auf ein Portfolio von Anwendungen verschiedener Anbieter Zugriff zu haben.

Nach [eco21] wecken Selbstbestimmte Identitäten SSIs gewisse Erwartungen. Ohne dass es einer zentralen Partei bedarf, könnten in einem dezentral organisierten Ökosystem digitale Identitäten – SSIs – erzeugt und vom Benutzer eigenständig kontrolliert werden. Unterschiedliche Ausweisdaten und Profile könnten so für den jeweiligen Anwendungsfall zielgerichtet kombiniert werden. Der Nutzer erhielte im Idealfall deutlich mehr Kontrolle – wer bekommt Einsicht, wer erhält Zugriff? – über die Daten seiner digitalen Identität [eco21].

Es konnte in diesem Beitrag gezeigt werden, dass solche *dezentralen* Systeme SSIs logischerweise keinen Bezug auf die amtlichen staatlichen – *zentral emittierten* – Identitäten haben *können* – die für eine Betrugsprävention und Gerichtsverwertbarkeit allerdings unabdingbar sind. Die Bezugnahme der SSIs auf die Distributed-Ledger-Technologien wie Blockchain ist *lediglich* für die Integrität der Identitätsdokumente hilfreich.

Für die weitere Verbreitung digitaler Identitätsdokumente sind jeweils die Aufwände von ganz entscheidender Bedeutung, die einerseits von den *Emissions-Stellen* dem Besitzer oder Benutzer im Rahmen der *Registrierungs-Protokolle* zugemutet werden, andererseits die Aufwände für eine *geeignete Aufbewahrung* der digitalen Identitätsdokumente durch deren Besitzer, und drittens die Aufwände die die spezifischen *Übermittlungs-Protokolls* der *Akzeptanz-Stellen* mit sich bringen. Hier erscheint als eine Offene Frage die geeignete Balance dieser Aufwände gegen die für die jeweiligen Szenarien erforderliche Sicherheit der Identitätsdokumente.

Wenn Personen durch eine sogenannte „Digitale Identität“ ersetzt werden ist es nicht mehr interessant, ob einem eine bestimmte Person gegenwärtig ist, sondern ob diese Person den richtigen, sie beschreibenden Datensatz vorzeigen kann. Eine gewisse Problemlage ergibt sich, wenn – marktbeherrschende – Unternehmen ihren Kunden eine umfassende Preisgabe ihrer persönlichen Daten und Identität abverlangen. Die Digitale Identität der Kunden wird damit eine funktionale Komponente der Geschäftsprozesse. Zum Teil wird ein Zugriff auf den persönlichen Bereich – wie etwa die Preisgabe einer Email-Adresse – schon aus fast nichtigen Gründen verlangt. Die persönlichen materiellen und geistigen Folgen für ein Individuum, das als Kunde ausgegrenzt und nicht – oder nicht mehr – bedient wird, sind sicher nicht ganz unerheblich. Es ist nicht unkritisch, wenn alle möglichen menschlichen und maschinellen Tätigkeiten und Handlungen von der IT vernetzt „registriert“ werden. Wer diese vollumfassenden Datenmengen der Identität in welcher Form zu welchem Zweck benutzen wird – das ist nicht unwesentlich.

Für Formale Systeme und Prozesse – auch für das Identitätsmanagement – ist zu fordern, dass sie revidierbar sein müssen. Es darf nicht sein, dass ein Formaler Prozess quasi „super-sicher“ ist und nicht mehr durch humane Intervention korrigiert werden kann. Der bewährte anthropozentrische Orientierungspunkt der individuellen Freiheit darf nicht gegen in Aussicht gestellte Nutzwerte Digitaler Systeme eingetauscht werden.

Literaturverzeichnis

[Alth13] Althoff, Gerd: „Die Macht der Rituale. Symbolik und Herrschaft im Mittelalter“, 2. Aufl., wbg, Darmstadt, 2013

[Brun21] Brunzel, Marco: „Sichere Identitäten als Fundament digitaler Identität“, AWV-Informationen 3/2012, Eschborn, 2021

[Clae10] Claes, Thomas: „Passkontrolle! – Eine kritische Geschichte des sich Ausweisens und Erkanntwerdens“, Vergangenheits Verlag, Berlin, 2010

[eco21] eco netTALK „Potenzial von SSI & Blockchain“, 14. Juni 2021, https://www.eco.de/event/eco-nettalk-potenzial-von-ssi-blockchain/

[Groe04] Groebner, Valentin: „Der Schein der Person. Steckbrief, Ausweis und Kontrolle im Europa des Mittelalters“, Verlag C.H. Beck, München 2004

[Hart11] Hartmann, Martin: „Die Praxis des Vertrauens“, Suhrkamp, Frankfurt am Main, 2011

[Idid21] ID-Ideal Schaufensterregion Sachsen, 2012, https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/IDideal/IDideal.html

[Jime11] Jiménez, Fanny: „Warum wir Gesichter blitzschnell erkennen können“, Welt digital, 10. Dez. 2011, https://www.welt.de/wissenschaft/article13759042/Warum-wir-Gesichter-blitzschnell-erkennen-koennen.html

[Lisch13] Lischka, Konrad: „Dinge mit Gesicht: Die Welt steckt voller Lächeln“, Hoffmann und Campe, 2013 eine Variante auch online unter https://dingemitgesicht.de/

[Pirs78] Pirsig, Robert M.: „Zen und die Kunst ein Motorrad zu warten. Ein Versuch über Werte“, Fischer-Taschenbuch-Verlag, Frankfurt am Main, 1978

[Rüru00] Rürup, Bert: „Die Zukunft der Erwerbsarbeit in der globalisierten Informationsgesellschaft“, Vortrag gehalten in Karlsruhe am 12. Mai 2000

[Toma10] Tomasello, Michael: „Warum wir kooperieren“, 4. Auflage, edition unseld, Suhrkamp, Frankfurt am Main, 2010

[VSDI19] Verband Sichere Digitale Identität e. V., Berlin, 2019, https://vsdi.de/sichere-identitaet/was-ist-eine-sichere-identitaet/

[Zime92] Zimen, Erik: „Der Hund: Abstammung – Verhalten – Mensch und Hund“, Goldmann Verlag, 1992

Kontaktdaten und Anschrift

Prof. Dr. Georg Rainer Hofmann
Information Management Institut IMI

TH Aschaffenburg
Würzburger Straße 45
64743 Aschaffenburg

+49 6021 4206-700
hofmann@th-ab.de

https://www.th-ab.de/
https://www.imi.bayern/