# Was ist und zu welchem Zweck braucht man eine „Sichere Identität“?

## Grundlagen, Akzeptanzfragen und Gestaltungsaspekte des Identitätsmanagements

**Georg Rainer Hofmann**

information management institut
mainproject
EUROPÄISCHE UNION
EUROPÄISCHER SOZIALFONDS
ESF IN BAYERN
WIR INVESTIEREN IN MENSCHEN
TH Aschaffenburg
university of applied sciences

**Autor:**
Prof. Dr. Georg Rainer Hofmann, Information Management Institut IMI,
Technische Hochschule Aschaffenburg

**Lektorat:**
Meike Schumacher und Katja Leimeister, Information Management Institut IMI,
Technische Hochschule Aschaffenburg

**Herausgegeber:**
Georg Rainer Hofmann, E-Mail: hofmann@th-ab.de
Wolfgang Alm, E-Mail: wolfgang.alm@th-ab.de
Information Management Institut (IMI), Technische Hochschule Aschaffenburg

**Die Deutsche Bibliothek - CIP Einheitsaufnahme**
Was ist und zu welchem Zweck braucht man eine „Sichere Identität“?
Grundlagen, Akzeptanzfragen und Gestaltungsaspekte des Identitätsmanagements

Aschaffenburg, 27. Oktober 2021

**ISBN 978-3-9823413-0-9**

**TECHNISCHE HOCHSCHULE ASCHAFFENBURG**
**INFORMATION MANAGEMENT INSTITUT**

Würzburger Straße 45
D-63743 Aschaffenburg

Die Publikation entstand im Rahmen des Projektes „mainproject hybrid“ - Eine Maßnahme des Europäischen Sozialfonds in Bayern.



Aus Gründen der besseren Lesbarkeit des Textes wird auf die gleichzeitige Verwendung von geschlechtsspezifischen Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

## Vorwort

Ambitionierte Initiativen wie das europäische Dateninfrastrukturprojekt GAIA-X oder die International Data Spaces (IDS) haben den Aufbau von sicheren domänenübergreifenden Digitalen Ökosystemen zum Ziel, welche die souveräne Bewirtschaftung der sogenannten Datengüter ermöglicht.

Eine zentrale Komponente in Digitalen Ökosystemen ist das Identitätsmanagement. Natürliche und juristische Personen, Organisationen im Allgemeinen, aber auch Sachen, wie Geräte und technische Vorrichtungen müssen „sicher" identifizierbar sein, wenn sie in Digitalen Ökosystemen „sicher" agieren wollen beziehungsweise verwendet werden sollen. Die Wichtigkeit einer sicheren Identität ist für die Betrugsprävention im Handel oder auch im Gesundheitswesen direkt evident.

Nicht zuletzt nach Maßgabe der Ambivalenz von Sicherheit einerseits und einfacher Handhabbarkeit und geringen organisatorischen Anforderungen andererseits werden die Erfolgsaussichten für die verschiedenen Ansätze eines Identitätsmanagements gemischt beurteilt – ihre aktive Akzeptanz oder ihre wenigstens passive Duldung sind nicht immer in dem Maß gegeben, wie dies wünschenswert wäre.

Zu den Akzeptanzdefiziten scheint nicht zuletzt eine für Endnutzer relativ unklare Terminologie mit der branchenüblichen, fortwährenden pseudo-innovativen Erfindung neuer anglistischer Vokabeln beizutragen. Für Investitionen der gewerblichen Wirtschaft wären wiederum belastbare offizielle Standards sehr wünschenswert. Eine überzeichnete aktivistische Akzeptanz von einzelnen Buzz-Words wie denen der „Blockchain", der „Verified Credentials" oder der „Self-Souvereign Identity" hat bedauerlicherweise bereits zu einigen fehlgeleiteten Investitionen mit entsprechenden Schäden geführt.

Vor diesem Hintergrund ist dieser Beitrag entstanden; er versucht eine holistische Sicht auf das für die Digitale Transformation absolut relevante Thema der „Sicheren Identität" zu geben.

Prof. Dr. Georg Rainer Hofmann

Aschaffenburg, im Oktober 2021

**Inhalt**

## Motivation

Bei (Digitalen) Geschäfts- und Verwaltungsprozessen können Betrug und anderes ungesetzliches Verhalten durch die „sichere Identität" der Beteiligten, Bürger, Kunden und Geschäftspartner erschwert werden. Bei der „Sicheren Identität" spielen die „Vertrauensvolle Identität" und die „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 sicheres *Verbergen* und damit (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 sollen auch nicht-technische Aspekte aufgegriffen und Hinweise zum Identitätsmanagement und einigen aktuellen Fragestellungen gegeben werden.

## Eine im Jahr 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 gewisse 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 Lohns" geht. Ähnliche Unsicherheiten sind zum Begriff „Geld" zu beobachten [Helm07] – und so auch beim Begriff der „Identität". [Förs03]

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 Familiennamen geändert haben. Er dürfte sich in den Jahrzehnten körperlich in seiner Statur und im Auftreten geändert haben. Er könnte gar das Attribut seiner individuellen und unverwechselbaren Fingerabdrücke durch einen bedauerlichen Unfall verloren haben.

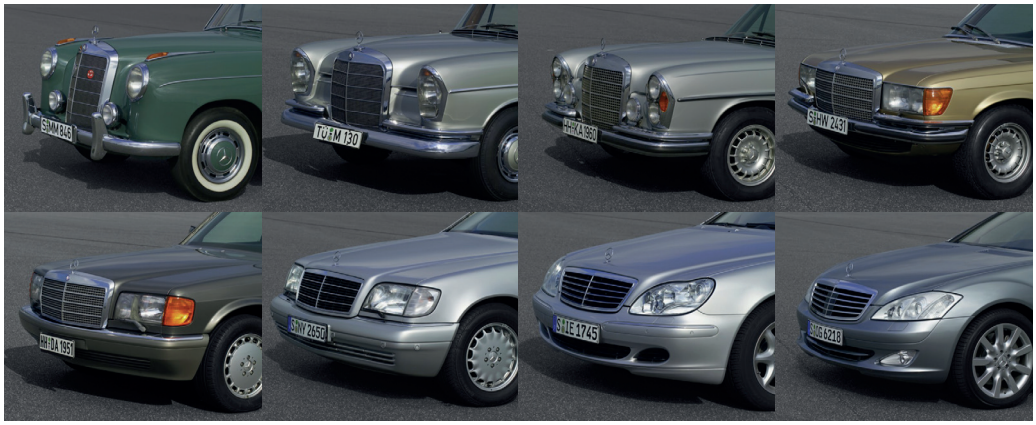
Auch wenn sich eine Person im Aussehen im Laufe ihres Lebens sehr verändert - so bleibt sie doch „dieselbe“ Person. (Bild: Freepik)

Der Mensch kann sich auch 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 – wenn sich die individuellen Attribute nicht allzu sehr oder unstetig ändern [Förs03].

> ▶ 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. Alle möglichen Komponenten des Motorrads könnten ja per technischer Wartung im Lauf der Jahre 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?




Auch abstrakte Objekte - wie der Typ eines Autos - werden wiedererkannt, auch wenn sich deren materielle Basis völlig verändert. (Bildkollage zusammengestellt aus https://5komma6.mercedes-benz-passion.com/das-gesicht-der-s-klasse-im-wandel-der-zeit/)

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. Es hat aber eine sehr große lebenspraktische 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 der beiden Begriffe dürfte sich etwa aus dem Szenario des Gebrauchtwagenhandels allgemein erschließen, 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 dahingehend widersprüchlich – zu hinterfragen.

## Ein 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 weiß sich ein Betroffener zu orientieren, weil er seine Mitmenschen anhand alternativer Attribute, wie dem Klang ihrer Stimme, oder der Art, wie sie sich bewegen, ebenfalls sicher erkennen kann.

Selbst ein Hund kann sowohl „seine Leute“ (Frauchen, Herrchen, etc.), als auch „seine Sachen“ (Fressnapf, Spielzeug, Leine, etc.) sicher erkennen [Zime92]. Das archetypische Erkennen von Personen oder Sachen ist also kein für die Menschen exklusives Spezifikum. So schrieb schon 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 diese Tiere gar nicht vorkommen. Eine Darstellung der Weihnachtsgeschichte wird – paradoxerweise – an Attributen erkannt, die diese eigentlich gar 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 Identifikation funktioniert ohne Ausweise oder anderweitige technische Ausstattungen. Diese Identifikationen basieren auf dem psychosozialen Phänomen des Vertrauens.

Das Erkennen von Sachen ist kein für die Menschen exklusives Spezifikum. Auch höher entwickelte Säugetiere erkennen ihre „Sachen“ und Menschen, die zu ihnen gehören. (Bild: susanne906, Pixabay)

Wird die archetypische vertrauensvolle Identifikation durch eine Identifikation durch Ausweise oder anderweitige Technik abgelöst, so kann das durchaus irritierend sein und einen entsprechenden sozialen Kredit kosten. 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 soziale Problem wohl auch mit einer formalen Ausweiskontrolle nicht zufrendstellend gelöst werden kann.

## 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, oder auch Amtsketten, Sheriffsterne, etc. Insignien können aber auch Gegenstände sein, so etwa ein Zepter, Marschallstab, Kriminaldienstmarke, und anderes mehr, 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 sowohl ein Insignie als auch ein Instrument für einen befugten Zugang – sie werden aber nicht von Menschen, sondern von Sachen – den passenden Schlössern – quasi „anerkannt“.

Insignien wie die Uniform, Bewaffnung, Polizeifahrzeug, und auch der Dienstausweis spielen beispielsweise bei der Polizei eine entscheidende Rolle für das Erkennen der Identität der Ordnungskräfte und die Ausübung ihrer dienstlichen Befugnisse. (Bild: https://www.polizei.bayern.de/)

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 (zu dürfen). Insofern ist das Identitätsmanagement eng verknüpft mit Zugangsberechtigungen. Das Access Management ist eine wichtige Anwendung des Identitätsmanagements. 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.

▶ Es ist ein generelles Merkmal von Identitätszeichen und Identitätsdokumenten, dass sie anerkannt werden müssen – sonst läuft ihre Bedeutung ins Leere. Die Anerkennung – oder Akzeptanz – 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?“ Und er führt weiter aus: „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 willkürlichen und 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 „Judaslohn“. 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 sie 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“.

Demonstrierende Personen, die zu ihrer Sicherheit per Vermummung anonym bleiben wollen. (Bild: [wiki11])

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, wer die von ihnen gesuchte Person ist. Judas verstößt nicht gegen ein damals geltendes Gesetz oder Gebot, er hat nicht einmal gelogen. Das Vorgehen des Judas ist – in perfider Weise – juristisch völlig korrekt; er hat sich eigentlich nichts zuschulden kommen lassen.

▶ Ein spezieller Aspekt des „zuverlässigen“ und „vertrauensvollen“ Identitätsmanagements 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 vertrauenvernichtenden Hinweis für die Tempelpolizei nachhaltig zerstört.

## Identitätsdokumente und Idiosynkrasie


Der vom Verlust seiner Anonymität betroffene Ludwig XVI., der angeblich aufgrund dieser Abbildung auf einer Kupfermünze im Jahr 1791 auf der Flucht gefasst wurde. (Bild: [Wiki21])

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 seiner Verurteilung zu entkommen. Es wird erzählt, dass Ludwig XVI. auf der Flucht aber anhand einer Münze erkannt wurde, auf der er abgebildet war. Die französische Revolutionsregierung verlangte in der Konsequenz für das Passieren der Grenzen ins Ausland nun generell 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 ein abstraktes (zuverlässiges) Dokument, als „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 des 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 sind oft nur dann sinnvoll, 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 – 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
- Zertifikat – als Herkunfts- oder Echtheitszertifikate, Digitales Zertifikat, Qualitätszertifikat
- Marke – 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. Identitätsdokumente sind als Modelle prinzipiell immer abstrakt und unvollständig: *Nicht alle Eigenschaften* einer Person können in einem Ausweisdokument aufgeführt werden. In Personalausweisen – beispielsweise – stehen als Komponenten (nur) der Name, das Geburtsdatum, die ladefähige Anschrift, etc. In einem Bahnfahrschein finden wir die Fahrstrecke, das Datum, die Klasse, den Preis,

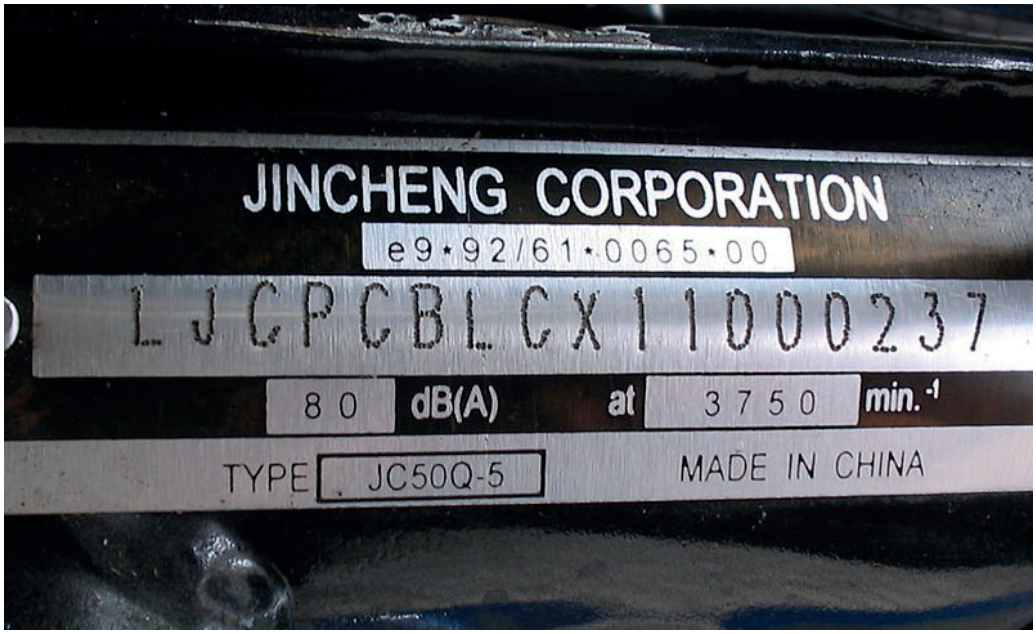
etc. Ein Fahrzeugbrief enthält die Fahrzeugnummer, eine Reihe technischer Merkmale, die diversen Eigentümer (Halter) des Fahrzeugs etc. pp.

> ▶ 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 ein Teil des normalen 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 die Person oder Sache (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 Identitätsdokumente im engeren Sinn. Ein Personalausweis gehört eineindeutig zu einer ganz bestimmten Person – und zu keiner anderen. Ein Fahrzeugbrief gehört zu genau einem bestimmten Fahrzeug.




Die am Fahrzeug angebrachte und „unentfernbare“ Fahrzeugnummer verbindet eineindeutig die Zulassungsdokumente mit dem konkreten Fahrzeug (Bild: [wiki05])

Andere Identitäten sind hingegen personenneutral, aber nicht personenunabhängig. 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 – personenneutrale – Identitätsdokumente auffassen. Sie weisen ihrem – jeweiligen – 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 Autorisierungskomponente 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 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 einem entsprechenden 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 Autorisierungsmerkmale, wie TANs, sind nur einmal (für den einen aktuellen 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 in der Regel im Rahmen eines spezifischen *Registrierungsprotokolls.*

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

und
- von *Akzeptanz-Stellen (Akzeptoren)*
- im Rahmen eines weiteren spezifischen *Übermittlungsprotokolls*

anerkannt – oder zurückgewiesen.

Dabei bilden Emittent und Akzeptor ein symmetrisches Verhältnis: Der Emittent wird das Identitätsdokument so zu gestalten versuchen, dass es – gemäß einer entsprechenden Vereinbarung oder eines entsprechenden Standards –

von einem Akzeptor über das Übermittlungsprotokoll 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 selbst-souveräne Identitäten (Self-Sovereign Identity – auch „Selbstbestimmte Identität“ – SSI) 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 *Registrierungsprotokoll* regelt, wie der Inhaber ein Identitätsdokument erhält. Das erfolgt auf aktiven Antrag, etwa im Fall eines Reisepasses oder eines Führerscheins oder als passive Zuteilung, der sich die Betroffenen kaum entziehen können, wie dies etwa bei Werks- oder Studierendenausweisen der Fall ist. Eine Vielzahl von Digitalen Nutzungsidentitäten wird – so im Handel – als Kundenausweis oder – etwa im E-Commerce – als digitale Registrierung mit Nachdruck offeriert. Nur mit einer Registrierung, oft mit der Verwendung einer E-Mail-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 Registrierungsprotokolls gestaltet sein. Ist der Aufwand zu hoch, leidet die Verbreitung der Identitätsdokumente.
- Die *Aufbewahrung* ist – im einfachen Fall der physischen Ausweise – eine verlustsichere Aufbewahrung der materiellen Dokumente durch die 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 – eventuell einige Dutzend – 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 ersetzt und durch die Emittenten erneut ausgegeben, nach Maßgabe entsprechender Regelungen. Software-Systeme haben dafür eine „Passwort vergessen“-Funktion.
- Das *Übermittlungsprotokoll* – siehe hierzu die Ausführungen weiter unten.

Im wichtigsten Spezialfall ist eine *amtliche Stelle* der Emittent eines Identitäts-

dokuments. 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 sich wider 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 „Selbstbestimmten Identität" (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:

- Einfache 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.


Personenneutrale Identitätsdokumente, die bei Benutzung nicht ungültig werden, wie z. B. Banknote, Haustürschlüssel, Tür-Chip


Personenneutrale Identitätsdokumente, die bei Benutzung ungültig werden, wie z. B. Eintrittskarten, Gutscheine, U-Bahnkarte


Personenabhängige Identitätsdokumente, die bei Benutzung ungültig werden, wie. z. B. Flugschein


Personenabhängige Identitätsdokumente, die bei Benutzung nicht ungültig werden, wie z. B. diverse Ausweise und Kundenkarten

▶ 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 Bahntickets. 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. Dies wird etwa bei den komplizierten Prozessen von Visaerteilungen bei Reisepässen deutlich.

Mit den Identitätsdokumenten sind Übermittlungsprotokolle 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, Eintragungen in Impfpäs-

sen, Anbringen von Stempelzeichen in Kunden-Treue-Rabattkarten im Einzelhandel, Stempelzeichen zur Hauptuntersuchung in Fahrzeugscheinen.
- *Elektronisches Lesen* von Digitalen Identitätsnachweisen: Die Idiosynkrasien sind als Daten auf Magnetstreifen, RFIDs, Chips mit Kontakten, Optischen Mustern etc. gespeichert und können entsprechend maschinell – elektronisch oder optisch – erfasst werden.
- *Kombiniertes Elektronisches Lesen mit Autorisierungen*: Das elektronische Lesen von Digitalen Identitätsnachweisen wird kombiniert mit der Autorisierung des Besitzers: Zum ausgelesenen Datensatz muss ein Passwort, eine PIN, oder eine auf separatem Weg übermittelte TAN eingegeben werden, um den Datensatz als für den Besitzer authentisch zu validieren. Diese Übermittlungsprotokolle müssen dafür mit einem vorherigen Registrierungsprotokoll kombiniert werden. In den Registrierungsprotokollen werden neben den Datensätzen der Identifier und den Datenträgern auch die zusätzlichen Mechanismen (Passwörter, PINs, TANs, etc.) festgelegt.

Die Übermittlungsprotokolle 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 Übermittlungsprotokolle, inklusive der vorher nötigen Registrierungsprotokolle, 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 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 – dann allerdings 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 zur MSN eine „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 auch 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 Knappheitseigenschaft verlieren und wertlos werden.

Das Anstreben von Fälschungssicherheit hat zweitens juristische Gründe. Bei den nicht personenneutralen 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.


Der deutsche Personalausweis ist mit diversen Sicherheitsmerkmalen versehen, die das Dokument fälschungssicher machen sollen. Dazu gehören beispielsweise das holografische Porträt, optisch variable Farben, die maschinell prüfbare Struktur oder das Laserkippbild. [Bund14]

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. im jeweils machbaren Maß 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 in der Regel 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 Drucktechnik 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 eigenhändige Unterschrift der agierenden 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 Passwort in Verbindung mit einem User-Namen (Benutzername-Kennwort-Systemzugänge) – oder auch die PIN bei der Benutzung einer girocard oder Kreditkarte. Das Passwort 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 der Emission des Identitätsdokuments und der Benutzerregistrierung angelegt.

### Selbst-Souveräne Identitäten SSIs – nicht zuletzt ein Politikum

Bei [HoPo21] wird eine quasi „kommerzielle" Selbst-Souveräne Identity SSI thematisiert, die insbesondere von Unternehmen wie Google, Facebook und Apple realisiert wird. Neben diesen bei [HoPo21] bereits genannten „Hyperscalern" wäre auch der Versandhändler amazon zu nennen, der schätzungsweise die Identität von 300 Millionen registrierter Kunden verwaltet. Aus dieser

oligopolistischen Marktstruktur folge, so [HoPo21], eine große Abhängigkeit von Wirtschaft und Gesellschaft in der Entwicklung der Digitalen Transformation, da der Cyberraum durch wenige große Identitätsmanager („ID-Provider“) dominiert wird. Zudem nutzten die genannten ID-Provider die sensiblen personenbezogenen Daten ihrer Nutzer für eigene Werbezwecke oder verkauften sie aus ökonomischen Interessen an weitere Unternehmen. Das schwäche die Privatsphäre der Nutzer – wobei diese „Schwächung“ durch eben diese Nutzer selbst verursacht worden ist, etwa durch eine bereitwillige breite Preisgabe von individuellen Daten in den sozialen Netzwerken wie Facebook und dergleichen.

In der Tat kann angemerkt werden, dass die Nutzerdaten von den genannten Hyperscaler-Unternehmen kommerziell ausgewertet werden. Diesem Umstand kann ein einzelner Nutzer nur durch einen „privaten Boykott“ entgegentreten. Konsequenterweise verweigern sich viele Personen einer „Registrierung“ bei den Hyperscalern – soweit dies irgend möglich ist. Zudem ist anzumerken, dass es sich bei den angesprochenen Nutzer-Registrierungen selbstverständlich jeweils um eine SSI handelt, denn die genannten großen Unternehmen sind keinesfalls staatliche Souveräne, die ein amtliches Identitätsdokument auszugeben in der Lage wäre.

Dem SSI-Identitätsmanagement der „zentralen“ großen Hyperscaler stellen nun [HoPo21] eine dahingehend alternative SSI gegenüber, die

- sich auf die Souveränität und den Schutz der Privatsphäre der Nutzer fokussiert
- zugleich deutlich einfacher und nutzerfreundlicher umgesetzt werden kann
- eine einfache und sichere, selbstbestimmte Identität bereitstellen kann
- sicher, vertrauenswürdig, interoperabel, selbstbestimmt, dezentral und souverän ist
- viele Prozesse und Abläufe im Umfeld des Identitätsmanagements einfacher, schneller, dabei auch noch sicherer und vertrauenswürdiger umsetzen in der Lage ist,

wodurch sich für die von [HoPo21] dargestellte SSI eine große gesellschaftliche und politische Relevanz ergibt, wenn es um die Zukunft der digitalen Identitätsverwaltung auf globaler Ebene, sowie in der Europäischen Union und insbesondere in Deutschland geht. Damit gewinnt diese Form der SSI eine politische Relevanz, weil es offenbar darum geht, den US-Amerikanischen Internet-Oligopolen eine Europäische „Internet-Opposition“ gegenüber zu stellen. Es geht sozusagen um einen „Airbus im Internet“, um eine bekannte Analogie aus der Flugzeugindustrie zu strapazieren.

Bei [HoPo21] wird für die SSIs eine konträre Rolle zum traditionellen (amtlichen) Identitätsparadigma gesehen, wo bekanntermaßen eine zentrale Instanz oder Autorität Identitäten erstellt und für die Nutzer verwaltet. Der Fokus läge nach [HoPo21] bei den SSIs auf einem nutzerzentrierten Ansatz und der Datensouveränität des Nutzers. Die Idee sei, dass Nutzer ihre digitalen Identitäten selbst erstellen, weitere digitale Identitätsdaten selbstbestimmt und dezentral verwalten und deren Weitergabe eigenständig kontrollieren. So würden sowohl ein „Single Point of Control“ als auch ein „Single Point of Failure“ vermieden. Da die Identitätsdaten dezentral beim Nutzer liegen, verfügt der Nutzer über die vollständige Kontrolle und Datenhoheit.

Das WWW-Konsortium (W3C-Konsortium) definiert dafür „Offene W3C-Standards“, mit denen „Decentralized Identifier“ (DID) und „Verifiable Credentials“ (VC) realisierbar sind. Es sei an dieser Stelle darauf hingewiesen, dass das W3C-Konsortium kein offizielles Standardisierungsgremium wie die ISO oder IEC ist. Die Organisationsstruktur des W3C-Konsortiums wird wohl, wegen der Dominanz und Einflussnahme großer Mobilfunk- und Softwareunternehmen, zu Recht kritisiert. Gleichwohl ist auf der Basis der „Offenen W3C-Standards“ eine gewisse Interoperabilität zwischen SSI-Lösungen und anderen „Credential“-Systemen gegeben. Bei [HoPo21] wird der Blockchain-Technologie und deren Vorteilen das Wort geredet, da sich so für das SSI-Ökosystem zusätzliches Vertrauen, Flexibilität und Skalierbarkeit generieren ließen. Hier muss angemerkt werden, dass die Blockchain lediglich die Integrität der VCs zu gewährleisten in der Lage ist – mehr nicht.

Als ein Anwendungsbeispiel führt [HoPo21] ein Impfzentrum oder eine Arztpraxis an. Diese könnten als Aussteller einer geimpften Person den digitalen Nachweis einer erfolgreichen Corona-Impfung als ein VC ausstellen, das kryptografisch an das „Link Secret“ der Geimpften gebunden ist. Dieser kann es anschließend lokal in seinem „Wallet“ auf dem Smartphone sicher hinterlegen. Zu hinterfragen ist, ob ein Identitätsmanagement auf Smartphone-Basis nicht einen grundlegenden konzeptionellen Nachteil mit sich bringt. Wenn ein essentielles Identitätsdokument – wie etwa ein Kfz-Führerschein – nur in einer „Wallet“ verfügbar ist, wäre dann ein Ausfall des Smartphones (leerer Akku, keine Funkverbindung) als ein „Fahren ohne Führerschein“ anzusehen?

Der Internationale Standard ISO/IEC 24727 ist hingegen kartenorientiert. Er schafft ein Referenzmodell zur Unterstützung der Interoperabilität von Smartcards – Chipkarten, eCards – für Identifizierungsdienste. In diesem Kontext ist die Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik – BSI TR-03112 Das eCard-API-Framework – zu sehen. Sie greift einen Beschluss des Bundeskabinetts aus dem Jahr 2005 auf, der die Eckpunkte für eine eCard-Strategie festlegt. Wesentliche Stützpfeiler dieser Strategie sind die elektronische Authentisierung und die qualifizierte elektronische Signatur, die auf Chipkarten unterschiedlicher Ausprägung zum Einsatz kommen. Durch das eCard-API-Framework, das eine Reihe von einfachen und plattformunabhängigen Schnittstellen umfasst, soll die Kommunikation zwischen den jeweiligen Anwendungen, wie

- elektronischer Gesundheitskarte (eGK)
- elektronischer Personalausweis (ePA)
- elektronischer Reisepass (ePass)
- elektronischer Steuererklärung (ELSTER)
- elektronischer Einkommensnachweis (ELENA)

und den eingesetzten Chipkarten vereinheitlicht werden. Das Ziel ist das Bereitstellen einer Schnittstelle, um eine einheitliche Nutzung der unterschiedlichen eCards zu ermöglichen.

Für die weitere Akzeptanz des von [HoPo21] dargestellten „dezentralen und autonomen“ SSI-Konzepts ist hingegen zu hinterfragen, inwieweit diese VC eine Beweiserheblichkeit haben? Wie kann sichergestellt werden, dass das VC – neben seiner formalen Korrektheit – auch inhaltlich belastbar ist? Wer darf

das VC ausstellen? Muss der Aussteller (Bank, Arbeitgeber, Arzt, etc.) hierfür eine Lizenz erwerben?

Zur Unterstützung der Akzeptanz der dargestellten SSIs könnte freilich eine entsprechende amtliche Verordnungslage helfen, nicht zuletzt, um die politisch gewollten Infrastrukturen wie GAIA-X und International Data Spaces (IDS) zu fördern. Es muss hier dahingestellt bleiben, inwieweit das einen Widerspruch zum Paradigma der Dezentralität und Selbstbestimmtheit des Identitätsmanagements darstellt.

## 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 ist zu unterscheiden zwischen amtlichen eID 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 (immer noch) attraktiv und sehr verbreitet, weil sie der traditionellen archetypischen Form eines Insignie nahe kommt.

## Legitimationsprüfungen – mit Video-Ident und 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.

In den vom Geldwäschegesetz (GWG) adressierten Fällen 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 des Personalausweises. 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.

Die unmittelbare persönliche Inaugenscheinnahme wie des Personalausweises ist beispielsweise die Grundlage des *Post-Ident-Verfahrens*. Dabei muss der Kunde persönlich in einer Deutsche-Post-Filiale vorsprechen und einen gültigen Personalausweis vorlegen. Damit kann eine Identität bestätigen werden, auf der ein Geschäftsprozess basieren kann.

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 darüber hinaus das Szenario, in dem der prospektive Kunde von der Bank per E-Mail eine URL erhält, die auf die WWW-Page eines unabhängigen Identifizierungsdienstleisters 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 und sich zu erkennen geben. Es muss sowohl die Vorder- als auch die Rückseite seines Personalausweises – lesbar – in die Kamera gehalten werden. Manche Identifizierungs-Dienstleister versenden zusätzlich eine TAN per SMS, die mit eingegeben werden muss. Gilt die Identifikation als erfolgt, könnten aufgrund dieser Legitimation mit einer Bank Geldgeschäfte abgewickelt werden.

> ▶ Das Video-Ident-Verfahren ist 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.

Das Video-Ident-Verfahren wird live per Video-Chat durchgeführt und ist besonders bei Online- und Direktbanken beliebt (Bild: [SSKM21])

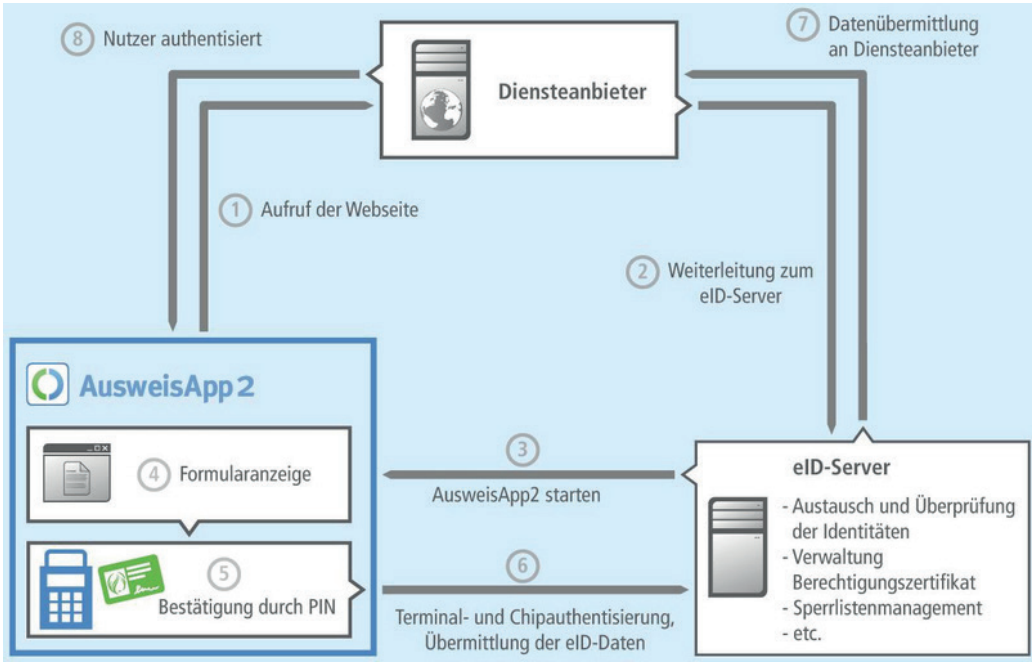
Die Evidenz-basierten Verfahren – Post-Ident und Video-Ident – basieren auf einer Inaugenscheinnahme durch entsprechend geschultes und legitimiertes Personal, also *vertrauenswürdige Menschen*. Es muss ein isochroner *Termin* zur Identifizierung vereinbart werden. Durch den Personal- und Zeit-Aufwand sind Post-Ident und Video-Ident nicht beliebig skalierbar, worunter wiederum deren Verbreitung leidet. Ein Ausweg aus der Terminproblematik könnte sein, dass das Vorzeigen des Ausweises und das Aufnehmen des Videos nicht-isochron, also nicht „live“ vor einer Kamera, erfolgt. Verfahren dieser Art, bei denen zusätzlich der Identifikationsprozess durch eine „intelligente“ KI-Software unterstützt wird, stehen vor der Herausforderung der Zertifizierung der entsprechenden KI-Systeme. Hier müsste ja die Vertrauenswürdigkeit der Inaugenscheinnahme durch Menschen durch die entsprechende Zuverlässigkeit eines KI-Systems ersetzt werden – dies ist ein offenes Problem.

Auf der Grundlage des Gesetzes für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums über eine Karte mit Funktion zum *elektronischen Identitätsnachweis* („eID-Karte-Gesetz“ – eIDKG) können Legitimationen elektronisch und nicht-isochron – offline – auf der Basis des elektronischen Personalausweises erfolgen. Der entsprechende Dienst lässt sich für den Endanwender relativ komfortabel realisieren. Erforderlich ist nur das Auslesen des Ausweises per NFC und die Eingabe der PIN. Dies dürfte die Abbruchquote beim Abschluss rechtssicherer Geschäfte und Verträge – dem „onboarding“ – verringern.

Eine zentrale Rolle spielt beim *elektronischen Identitätsnachweis* Anwendungssoftware, mit der ein elektronischer Ausweis sicher ausgelesen werden kann. Dabei dient ein Smartphone als NFC-Kartenleser und damit als Ausweis-Kartenlesegerät. Ein Beispiel hierfür ist die „AusweisApp2“, die zudem 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 elektronischen Ausweis 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 des Weiteren die PIN des elektronischen Ausweises über das Smartphone abhörsicher eingegeben. Der Gebrauch eines separaten Lesegerätes mit separater Tastatur, ein erhebliches Akzeptanzhindernis, entfällt damit. Der Prozess läuft auf der Seite des Dienstanbieters vollautomatisch und nicht-isochron. Da es keinen großen Personalaufwand gibt, ist der elektronische Identitätsnachweis leichter skalierbar für Massenanwendungen.

Der Dienstanbieter stellt – in Vorbereitung der Legitimation – einen zu 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 freigeben 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. Damit sollten mit dem Jahr 2027 nur noch eID-fähige Personalausweise in Deutschland existieren. Im Notfall kann der Ausweisinhaber über ein Sperrkennwort die eID-Funktion zentral sperren lassen.




Die Überprüfung und verschlüsselte Übermittlung der Daten durch die AusweisApp erfolgt über den eID-Server mit dem Dienstanbieter. (Bild: [Gowe21])

▶ 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, seit dem 29. September 2018 die elektronische Identifizierung, die in einem der EU-Mitgliedstaaten ausgestellt wurde.

## Identitätsmanagement 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 psycho-sozialen Vertrauens zu realisieren [Brun21]. Die zu adressierenden sozialen und ökonomischen Kontexte sind zu umfangreich geworden – man kann in der täglichen Lebenspraxis nicht mehr alle an einem Handelsgeschäft beteiligten Personen persönlich kennen.

Ein Identitätsmanagement ist kein Selbstzweck. Es sind durchaus die allgemeinen Prinzipien des Informationssystem-Managements anwendbar, es gilt auch hier die bekannte Hierarchie in der Planung:
1. Welches (Unternehmens )Ziel soll mit
2. welchen Szenarien und Nutzwerten,
3. welchen Prozessen und mit
4. welcher Technologie erreicht werden?
5. Mit welchen Projekten lassen sich diese Ziele erreichen?
6. Wie lassen sich die Systeme betreiben?

Es kann zu 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“) der Idiosynkrasie gibt es? Warum ist der Zugriff auf Daten der amtlichen Identitätsdokumente berechtigt und begründet?
- Welche Benutzer benutzen welche Verfahren – Video-Ident, eID – um SSI-Identitätsdokumente geeignet 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 Fokus muss auf der Akzeptanz des gesamten Szenarios liegen. Man kann hier drei kritische Aspekte sehen:

1. Wie die Inhaber in den Besitz der Identitätsdokumente gelangen, wie sich die Verbindung mit den amtlichen Ausweisdokumenten möglichst „einfach" gestalten lässt.
2. Wie die Identitätsdokumente aufbewahrt werden können. Wie Inhaber bei einem Verlust sicher vor unbefugter Benutzung durch Dritte sein können und wie ein Ersatz-Identitätsdokument erlangt werden kann.
3. Welche Akzeptanzverfahren und Protokolle die sichere Übernahme der Daten aus den Identitätsdokumenten in die Systeme der Akzeptoren und Händler ermöglichen. Wie eine sichere Autorisierung der Inhaber erfolgt.

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 beispielsweise die Rechnungsanschrift oder die Lieferanschrift nicht korrekt sind. Eine Forderung ist nicht werthaltig, wenn sie auf einem dahingehend nichtigen Kaufvertrag basiert, weil eine unbefugte Person eine Bestellung vorgenommen oder einen Kaufvertrag abgeschlossen hat. Eine Forderung ist auch dann nicht werthaltig und wird zurückgewiesen, weil der ordnungsgemäße Eingang oder Erhalt einer Ware bestritten wird. Ein entsprechendes Identitätsmanagement 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 Rechnungsbeträge und Umsatzvolumina nicht.

Sowohl im B2B als auch im B2C haftet in Betrugsfällen 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 ist 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 Identitätsökosysteme – 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.

## Eine Herausforderung an das Identitätsmanagement: Die EU-Whistleblower-Richtlinie (EU-RL 2019/1937)

Collage bekannt gewordener Whistleblower (v.l.): Daniel Ellsberg, Edward Snowden, Chelsea Manning, Mark Felt und Antoine Deltour. (Bilder [Sued17] und [Wiki17])

Vereinfacht ausgedrückt sind Hinweisgeber („Whistleblower") solche Personen, die als Mitarbeiter von Unternehmen oder Behörden, oder als anderweitig Betroffene, Missstände oder Rechtsverstöße ihrer (Arbeitgeber-) Organisation gegen geltendes Recht an die Öffentlichkeit oder zur Anzeige bringen. Solche

Hinweisgeber waren in der Vergangenheit der allgemeinen Gesellschaft nützlich, wenn es etwa um die Aufdeckung von schädlichen Produkten, Umweltschädigungen, oder auch um Korruption ging. Hinweisgeber können mithin wichtige Beiträge zur Aufdeckung und Ahndung von Missständen leisten. Hinweisgeber sind aber in der Folge einer derartigen Offenlegung von Missständen nicht selten Repressalien ausgesetzt.

Mit der EU-Richtlinie 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 soll der Schutz von Personen, die Verstöße gegen das (Unions-) Recht melden, umgesetzt werden. Die Umsetzung der EU-Richtlinie in innerstaatliches Recht muss entsprechend erfolgen. In der Bundesrepublik ist daher ein neues Gesetz zum Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz – HinSchG) zu erlassen, um Hinweisgebern eine der EU-Richtlinie entsprechende Rechtssicherheit zu geben. Es ist im Wesentlichen ein einheitliches Schutzsystem für hinweisgebende Personen mit den folgenden zentralen Regelungselementen [HinG20]:

- Der persönliche Anwendungsbereich umfasst alle Personen, die in ihrem beruflichen Umfeld Informationen über Verstöße erlangt haben.
- Für hinweisgebende Personen werden mit internen und externen Meldekanälen zwei gleichwertig nebeneinanderstehende Meldewege vorgesehen, zwischen denen sie frei wählen können.
- Es werden die Voraussetzungen festgelegt, unter denen eine hinweisgebende Person Informationen über Verstöße öffentlich zugänglich machen darf.
- Sofern hinweisgebende Personen die Anforderungen an eine Meldung oder Offenlegung einhalten, werden sie umfangreich vor Repressalien wie Kündigung oder sonstigen Benachteiligungen geschützt.

Nicht unähnlich der Betrugsprävention hat auch das „Hinweisgeberwesen“ eine große Bedeutung in der unternehmerischen Praxis. Die Offenlegung etwa der diversen „Dieselskandale“ in der Automobilindustrie zeigt eindrücklich deren ökonomische Relevanz. Die Missstände dieser Größenordnung können durchaus eine Beeinträchtigung der nachhaltigen Existenz von Unternehmen bedeuten. Die Richtlinie 2019/1937 adressiert nur Verstöße gegen EU-Recht. In der unternehmerischen Praxis dürften aber auch Hinweise über andere „Missstände und Delikte“, die für ein Unternehmen rufschädigend sein können, letztlich Einfluss auf seine ökonomische Basis haben können. Bei der Realisierung der betrieblichen Hinweisgebersysteme sollte daher nicht nur auf die justiziablen „Verstöße“ der EU-Richtlinie eingegangen werden.

Eine gewisse Herausforderung stellt das berechtigte Interesse der Hinweisgeber an Anonymität dar, die sich in einem Dilemma mit der Notwendigkeit einer Rückmeldung an eben dieselben befindet. Der Hinweisgeber hat ein Recht zu erfahren, dass der Hinweis quasi eine „Wirkung“ gezeigt hat – es ist zu fragen, auf welchem Weg den anonymen Hinweisgeber diese Rückmeldung erreichen kann. Für letztere müsste die Identität des Hinweisgebers „irgendwie“ bekannt sein.

Eine weitere Herausforderung ist die vorgesehen „Beweisumkehr“, wenn es um die Vermeidung von Repressalien für Hinweisgeber geht. So könnte ein

Beschäftigter sein Unternehmen beschuldigen, dass ihm eine Beförderung nur aufgrund eines – von ihm eigentlich anonym gegebenen, aber „durchgesickerten“ – Hinweises versagt wurde. Es ist zudem die Frage zu stellen, inwieweit der Begriff der „Repressalie“ noch weiterer Definition bedarf.

Eine dritte Herausforderung stellen einige Spezialprobleme dar. Wie kann mit parallelen oder seriellen Mehrfachmeldungen umgegangen werden, oder auch mit reinen „Me-Too“-Hinweisen, die nur einen dahingehend unbilligen Schutz vor prospektiven „Repressalien“ zum Ziel haben. Auch der Umgang mit unbegründeten, falschen oder böswillige Hinweisen, bis hin zum Denunziantentum und Mobbing, bedarf weiterer Ausgestaltung. Für die Ahndung von Missbrauch müsste die Identität des Hinweisgebers ebenfalls „irgendwie“ hinreichend bekannt sein.

## Die Rolle einer „Trusted Third Party“ als Identitätsmanager für Whistleblower

Die oben dargestellten Herausforderungen bei der Umsetzung der EU-Whistleblower-Richtlinie (EU-RL 2019/1937) scheinen durch vollständig automatische algorithmische Lösungen kaum lösbar zu sein. Insofern ist eine berufsverschwiegenen „Trusted Third Party“ als ein „Identitätsmanager“ bedenkenswert. Der Identitätsmanager realisiert einen betreuten Hinweisgeber-Meldekanal gemäß der EU-Richtlinie. Der Meldekanal kann analog per Telefon oder „Zettelkasten“, insbesondere aber als digitale Plattform implementiert werden. In Deutschland könnte die Rolle des Identitätsmanagers durch fachlich entsprechend ausgewiesene, berufsverschwiegene und unabhängige Rechtsanwälte wahrgenommen werden.

Aufgrund der anwaltlichen Berufsverschwiegenheit wäre eine – wenn anwendbar – vollständige Wahrung der Anonymität der Hinweisgeber gewahrt, auch im Rahmen sich anschließender Verfolgung der Vorwürfe. Eine gewisse Analogie zum Beichtgeheimnis ist nicht von der Hand zu weisen: Allfälligen Opfern einer Untat kann geholfen werden, ohne die Anonymität der Täter zu verletzten. Die Hinweise werden von den anwaltlichen Identitätsmanagern entgegengenommen und quasi qualitätssichernd erstbearbeitet. Es wird geprüft, ob der Hinweis substanziell ist, es sich um einen Mehrfachhinweis handelt, ob es nur um Denunziation geht etc. Im Gegenzug kann der Hinweisgeber unter dem besonderen Vertrauensschutz der Identitätsmanager eine geforderte Rückmeldung entgegennehmen und sich gegebenenfalls mit deren Hilfe gegen Repressalien wehren.

## 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 Jahr 2021 sind viele Identitäten (noch) nicht digitalisiert – und es sollte in diesem Beitrag gezeigt werden, dass insbesondere die vertrauensvol-

len Identitäten nicht formaler Natur sind und daher nicht digitalisiert werden können. Die auf Benutzernamen und Passwort basierenden Mechanismen sind wohl die am häufigsten verwendeten digitalen Lösungen. Andere Techniken konnten sich in der von diesen Lösungen erreichten Breite bislang noch nicht durchsetzen. Im privaten Bereich sind SSIs wie Single-Sign-On-Dienste wie „Shibboleth“ etwas weiter verbreitet: Hier melden sich Benutzer nur einmal an, um auf ein Portfolio von Anwendungen verschiedener Anbieter Zugriff zu haben.

Nach [eco21] und insbesondere [HoPo21] 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].

Dezentrale Systeme, wie die SSIs, haben per definitionem keinen Bezug auf die amtlichen staatlichen, zentral emittierten Identitäten: Letztere sind für eine Betrugsprävention und Gerichtsverwertbarkeit allerdings unabdingbar. Die Bezugnahme der SSIs auf die Distributed-Ledger-Technologien wie Blockchain ist lediglich für die Integrität der Identitätsdokumente hilfreich.

Es kann weiter nicht verkannt werden, dass Identitätsdokumente in der Betrachtung des größeren historischen Kontextes stets zunehmend zentralisiert worden sind. So wurden die alten lokalen standesherrschaftlichen Ausweise durch nationale deutsche, und diese wiederum durch Europäische Ausweise abgelöst. Insofern stellen sich die SSIs einem langfristigen, offenbar nützlichen und seitens der Nutzer hochgradig akzeptierten Trend entgegen.

Für die weitere Verbreitung digitaler Identitätsdokumente sind jeweils die Aufwände von ganz entscheidender Bedeutung, die einerseits von den Emissionsstellen dem Besitzer oder Benutzer im Rahmen der Registrierungsprotokolle zugemutet werden, andererseits die Aufwände für eine geeignete Aufbewahrung der digitalen Identitätsdokumente durch deren Besitzer, und drittens die Aufwände, die die spezifischen Übermittlungsprotokolls 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 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 bloße funktionale Komponente der Geschäftsprozesse. Zum Teil wird ein Zugriff auf den persönlichen Bereich – wie etwa die Preisgabe einer E-Mail-Adresse – schon aus fast nichtigen Gründen verlangt. Die persönlichen ma-

teriellen 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 3/2021, Eschborn, 2021

[Bund14] Bundesdruckerei GmbH: „Sicherheitsmerkmale des Personalausweises“, Januar 2021, https://www.kartensicherheit.de/media/pdf1/Flyer_Bundesdruckerei_Sicherheitsmerkmale_nPA.pdf

[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/

[Förs03] Förster, Johanne: „Identität von Personen“, Dissertation, Mannheim, 2003

[Gowe21] Governikus GmbH & Co. KG - im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik: „AusweisApp2: Online-Ausweisfunktion“, https://www.ausweisapp.bund.de/online-ausweisen/online-ausweisfunktion/

[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

[Helm07] Helmedag, Fritz: Geld: Einführung und Überblick, Knapps Enzyklopädisches Lexikon des Geld-, Bank- und Börsenwesens, Auflage 2007, Fritz Knapp Verlag, Frankfurt am Main, 2007

[HinG20] Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz. Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden. 26. November 2020.

[HoPo21] Hoang, Johnny und Pohlmann, Norbert: „Was Self-Sovereign Identity (SSI) unverzichtbar macht“, in: IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, 4/2021, pp 78ff.

[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. Dezember 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

[SSKM21] Stadtsparkasse München: „Das Video-Ident-Verfahren“, https://www.sskm.de/de/home/service/videoident-verfahren.html

[Sued17] „Die wichtigsten Enthüller vor und nach Chelsea Manning“, Süddeutsche Zeitung, Ausgabe 18. Januar 2017, online abrufbar unter https://sz.de/1.3337802

[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/

[Wiki05] Abbildung einer Fahrgestellnummer, Wikimedia Commons, https://commons.wikimedia.org/wiki/File:Framenummer_voorbeeld.jpg, Upload 04. Oktober 2005

[Wiki11] A member of the group known by the pseudonym Anonymous, at the Wall Street occupation protest in New York on September 17, 2011. https://commons.wikimedia.org/wiki/File:Occupy_Wall_Street_Anonymous_2011_Shankbone.JPG

[Wiki17] Wikipediaeintrag zu „Chelsea Manning“, Upload am 18. Mai 2017, https://de.wikipedia.org/wiki/Chelsea_Manning

[Wiki21] Wikiwandeintrag zu „Ludwig XVI.“, https://www.wikiwand.com/de/Ludwig_XVI.

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

## Weitere Publikationen aus dem IMI-Verlag


**Titel: Agile berufliche Weiterbildung im Digitalen Wandel — Rahmenbedingungen und Anforderungen an zeitgemäße Modelle**
**Autoren**: Hofmann, Georg Rainer, Joachim Schmitt, Meike Schumacher, Katja Leimeister, Lucia Falkenberg, Percy Scheidler
**Verlag**: IMI Verlag, Aschaffenburg, 09/2020
**ISBN:** 978-3-9818442-4-5

**Inhalt:**
Die Arbeitswelt befindet sich in einem unaufhaltsamen Wandel – sie wird kurzlebiger, digitaler und agiler. Längst schon reicht es nicht mehr aus, sich zum Beginn des Berufslebens mit einer Ausbildung oder Studium für die weitere berufliche Tätigkeit zu qualifizieren. „Lebenslanges Lernen“ ist das Gebot der Gegenwart und Zukunft der Arbeitswelt und hierfür gilt es, passende Angebote für Betriebe und deren Beschäftigte zu gestalten.

Der vorliegende Text basiert auf den Ergebnissen des „New Work“-Symposiums im März 2020 und einem Fachgespräch im August 2020 an der TH Aschaffenburg. Neben den Ergebnissen aus diesen Veranstaltungen flossen in diese Publikation eine Vielzahl von Erkenntnissen ein, die in zahlreichen Gesprächen mit Akteuren aus dem Weiterbildungsumfeld gewonnen wurden und Impulse zur Gestaltung der Weiterbildung in der „Neuen Arbeitswelt“ geben können. Die Publikation kann kostenfrei heruntergeladen werden unter: https://www.mainproject.eu/mainproject-digital/studien/


**Titel: Nachhaltigkeit — als Orientierungsmarke für Wirtschaft und Technik -**
**Autoren**: Katja Leimeister, Joachim Schmitt, Meike Schumacher
**Verlag**: IMI Verlag, Aschaffenburg, 03/2021
**ISBN:** 978-3-9818442-5-2

**Inhalt:**
Nachhaltigkeit wird gefordert: In der Ökonomie stellt sich die Frage nach der richtigen Balance im immerwährenden Wechselspiel von Investitionen und Gewinnabschöpfungen. Die Ökologie fragt nach einer Schonung der natürlichen Ressourcen. Die Qualifikation der Belegschaften und aller Erwerbsstätigen muss laufend nachhaltig weiterentwickelt werden. In den Systemen der sozialen Sicherung wird nach zukunftsfähigen Konzepten gesucht.

Im Rahmen der Ringvorlesung „Nachhaltigkeit“ wurden die Dimensionen der Nachhaltigkeit von unterschiedlichen Referenten beleuchtet. Diese Publikation fasst die einzelnen Vorträge der Ringvorlesung „Nachhaltigkeit“ zusammen, die im Wintersemester 2020/2021 an der Technischen Hochschule Aschaffenburg stattfand.


**Titel: Ethik und Akzeptanz — als Orientierungsmarke für Wirtschaft und Technik -**
**Autoren**: Joachim Schmitt mit einem Gastbeitrag von Prof. Dr. h.c. Günter Koch
**Verlag**: IMI Verlag, Aschaffenburg, 05/2021
**ISBN:** 978-3-9818442-6-9

**Inhalt:**
In dieser Publikation werden die Ergebnisse des Fachgesprächs „Ethik und Akzeptanz am 25. Februar 2021 an der Technischen Hochschule Aschaffenburg dargestellt. Im Fachgespräch wurde gefragt, welche spezifischen Akzeptanz-Aspekte Ethik heute bereits aufgreifen kann. Wo und wie werden einst nur „Soft Factors“ der Ethik nun auch ökonomisch relevant? Wo wird die abstrakte Diskussion um „Vertrauen“, „Verantwortung“, „Nachhaltigkeit“, „soziales Verhalten“, etc. ökonomisch konkret, wenn es um die Akzeptanz von Technologien, Produkten und Dienstleistungen geht? Lassen sich Handlungslinien zur Verbesserung der Akzeptanz identifizieren?

Hierzu wurden vier Perspektiven in Impulsvorträgen ausgeleuchtet, ein textlicher Zwischenruf eingebunden und in einer abschließenden Podiumsdiskussion verknüpft.


**Titel: Wissenstransfer und Weiterbildung - Erfahrungen und Perspektiven zu digitalen und hybriden Formaten.**
**Autoren**: Joachim Schmitt, Katja Leimeister, Meike Schumacher
**Verlag**: IMI Verlag, Aschaffenburg, 05/2021
**ISBN:** 978-3-9818442-7-6

**Inhalt:**
Am 11. März 2021 wurde von mainproject digital ein virtuelles Symposium „Hybrid-digitaler Wissenstransfer in Netzwerken Hochschule-Wirtschaft – Neue Erfahrungen und Perspektiven der Weiterbildung“ ausgerichtet.

Referenten aus Aschaffenburg, Bayreuth und Würzburg stellten Praxis-Beispiele für den Wissenstransfer in Netzwerken von Hochschule und Wirtschaft vor.
In kleineren Workshop-Gruppen wurde die Theorie dann in die Praxis umgesetzt: Ausgehend von unterschiedlichen Milieus, Lerntypen und dem Umgang mit digitalen Medien wurde mit den Teilnehmern konkrete „Lern“-Personas - in Anlehnung an die Konzepte der Buyer Persona erstellt. Für die einzelnen Personas wurden typgerechte Wissenstransfer- und Weiterbildungsangebote erarbeitet und mit den vorhandenen Konzepten aus den Praxisbeispielen abgeglichen. Es ging also um die Frage, wie sich unterschiedliche Zielgruppen für hybrides Lernen begeistern lassen.

Diese Dokumentation fasst die gehaltenen Vortrage sowie die wesentlichen Ergebnisse aus den Workshops des Symposiums zusammen.

mainproject

Nachhaltigkeit

Digitalisierung

New Work

Agilität

## Wissenstransfer und Weiterbildung für Ihren Erfolg von heute und morgen

**analog – digital – hybrid**

*immer aktuell informiert*

www.mainproject.eu

EUROPÄISCHE UNION | ESF IN BAYERN

TH Aschaffenburg university of applied sciences

information management institut

Medienpartner:

www.primavera24.de

**Information Management Institut (IMI)**

**Technische Hochschule Aschaffenburg**
**Würzburger Straße 45**
**63743 Aschaffenburg**

**www.imi.bayern**
**www.mainproject.eu**

**ISBN 978-3-9823413-0-9**