

DIN e.V., DKE

Projektbericht Sichere Digitale Identitäten (SDI)

Sachverhalts- und Situationsanalyse inkl.
Ermittlung des Handlungsbedarfs

Umsetzungsempfehlungen zur Definition und
Etablierung Sicherer Digitaler Identitäten als
Vertrauensanker in der digitalisierten Welt

Projektbericht zur Förderung durch das Bundesministerium für Wirtschaft und
Energie (BMWi) vom 1. Januar 2017 bis 31. Oktober 2017

Dr. Michael Stephan, Dr. Stefan Weisgerber, Volker Jacumeit, Benjamin Helfritz,
Sven Müller, Christian Seipel, Dr. Dennis Kenji Kipker

Berlin, 01.08.2018

Inhalt

| | |
|--|----|
| Abkürzungsverzeichnis | 7 |
| A Management Summary | 10 |
| B Aufbau des Projektberichts | 17 |
| 1 Projektbeschreibung..... | 20 |
| 1.1 Projektinitiierung und -antrag..... | 20 |
| 1.2 Projektbearbeitende DIN und DKE | 22 |
| 1.2.1 DIN als Projektdurchführender..... | 22 |
| 1.2.2 DKE als Unterauftragnehmer aufgrund Alleinstellungsmerkmals | 22 |
| 1.3 Zielerfüllung – Gegenüberstellung Arbeitspakete und Aktivitätendarlegung | 24 |
| 2 Analyseprozess..... | 27 |
| 2.0 Auswertung des Analyseprozesses..... | 28 |
| 2.1 Konsultation/Einbindung von Experten und Stakeholdern..... | 29 |
| 2.1.1 Beirat..... | 29 |
| 2.1.2 Vorgespräche..... | 30 |
| 2.1.3 Umfrage mit Fragebogen | 32 |
| 2.1.4 Experten-Interviews..... | 34 |
| 2.1.5 Themen-Workshop, 22. Juli 2017 bei DIN | 35 |
| 2.1.6 Stakeholder-Workshop, 10. Juli 2017 im BMWi | 36 |
| 2.1.7 Zwischen- und Folgegespräche / Kontakte etc. | 38 |
| 2.2 Recherche allgemein..... | 40 |
| 2.2.1 Initiativen / Aktivitäten / Gremien / Akteure..... | 40 |
| 2.3 Recherche Normung..... | 43 |
| 2.3.1 Grundlage der Recherchearbeit..... | 43 |
| 2.3.2 Relevante Organisationen im Normungs- und Standardisierungsumfeld | 44 |
| 2.3.3 Umfassende Ergebnisse | 48 |
| 2.3.4 Resümees..... | 63 |
| 2.4 Recherche Recht..... | 65 |
| 2.4.1 Ziele, Aufbau und Vorgehen..... | 65 |
| 2.4.2 Darstellung der gefundenen Ergebnisse..... | 66 |
| 2.4.3 SDI als Impulsgeber in den Bereichen IT-Sicherheit und Datenschutz: IT-SiG, EU DS-GVO, eIDAS-VO..... | 73 |
| 2.4.4 Zusammenfassung / Rückschlüsse / Interpretation / Resümees | 74 |
| 3 Ergebniszusammenführung zur Sach- und Prozessbeschreibung & Beispiele..... | 76 |
| 3.1 Relevante Dimensionen des Gesamtsachverhalts | 78 |

| | | |
|-------|---|-----|
| 3.1.1 | Die zwei Interessenspole – Schutz des Identitätsgebers und Identitätsabfragenden..... | 78 |
| 3.1.2 | Lebenszyklus | 80 |
| 3.1.3 | Einsatz- und Verantwortungsbereich von Identitätslösungen..... | 80 |
| 3.1.4 | Der Anwendungsfall ist maßgebend – Faktoren, die das benötigte Sicherheitslevel determinieren | 83 |
| 3.2 | Schrittweiser Aufbau des Schaubilds des Gesamtsachverhalts an den Schritten des klassischen Lebenszyklus von Digitalen Identitäten..... | 87 |
| 3.2.1 | Entitäten - unbegrenzt mannigfaltiger Ausgangspunkt..... | 89 |
| 3.2.2 | Feststellen der Identität – Governance-Strukturen..... | 90 |
| 3.2.3 | Abbilden der Identität..... | 91 |
| 3.2.4 | Einrichten der Identität | 92 |
| 3.2.5 | Verwalten der Identität | 100 |
| 3.2.6 | Nutzen der Identitätslösung..... | 101 |
| 3.2.7 | Löschen, Archivieren, Reaktivieren der Identität..... | 104 |
| 3.3 | Schaubild Gesamtsachverhalt..... | 105 |
| 3.4 | Strategische Beispiele..... | 106 |
| 3.4.1 | Von Markenrechtsverletzungen bis zu unsicheren Bauteilen – Produkt-fälschungen, durch standardisierte SDI ein Thema von gestern..... | 106 |
| 3.4.2 | SDI - mit Standards potentiellen Sicherheitslücken begegnen..... | 107 |
| 3.4.3 | Fake News den Boden entziehen mit SDI..... | 108 |
| 3.4.4 | Anbieten von „SDI “ als sekundäres Geschäftsmodell, geht das?..... | 109 |
| 3.4.5 | SDI sind der Enabler von Industrie 4.0 und anderen Zukunftsprojekten..... | 111 |
| 3.4.6 | Vom Smart Meter Gateway lernen - jedem Anwendungsfall seine SDI..... | 113 |
| 4 | Ergebniszusammenführung zu Kernaussagen und Schlussfolgerungen zur Situationsbestimmung und Herleitung der Handlungsbedarfe | 116 |
| 4.1 | Relevanz | 117 |
| 4.2 | Hebel für digitale Sicherheit | 119 |
| 4.3 | Handlungsdruck | 120 |
| 4.4 | Keine One-Fits-All-Lösung möglich..... | 121 |
| 4.5 | Insellösungen am Markt..... | 122 |
| 4.6 | Insellösungen auch in der Standardisierung | 123 |
| 4.7 | Dreh- und Angelpunkt digitaler Systeme, Produkte, etc..... | 124 |
| 4.8 | Jedes Digitalisierungsprojekt braucht SDI..... | 125 |
| 4.9 | Die Domänen wachsen zusammen..... | 126 |
| 4.10 | Es geht nur international..... | 127 |
| 4.11 | Ein gemeinsames Ziel (Referenzarchitektur / Framework)..... | 128 |

| | | |
|--------|--|-----|
| 4.12 | Fokus Anwendungsfall (Sicherheitslevel, u.a.)..... | 129 |
| 4.13 | Fokus Lebenszyklus (Bestandteile von Identitätslösungen)..... | 130 |
| 4.14 | Anforderungsprofile nach Einsatz- und Verantwortungsbereich..... | 131 |
| 4.15 | Anwendbarkeit der Referenzarchitektur..... | 132 |
| 4.16 | Es wird nicht bei Null angefangen (Grundlagen / Ergebnisse)..... | 133 |
| 4.16.1 | Teil-Ergebnisse der Konzeptionsphase..... | 134 |
| 4.17 | Ein domänenübergreifendes Netzwerk als Alleinstellungsmerkmal..... | 135 |
| 4.18 | Die Antwort auf Internationalisierung: Normung..... | 136 |
| 4.19 | Industrie 4.0 - Potential zum Leitmodell..... | 138 |
| 4.20 | Auswirkungen – über die digitale Welt hinaus..... | 139 |
| 4.21 | Auswirkungen – Forschungs- und Infrastrukturbedarf..... | 140 |
| 4.22 | Auswirkungen – juristischer und gesetzlicher Art..... | 141 |
| 4.23 | Politisches Engagement notwendig..... | 142 |
| 5 | Master- und Strukturplan für Sichere Digitale Identitäten..... | 144 |
| 5.1 | Inhaltliche Koordinierungsaktivitäten..... | 147 |
| 5.1.1 | Koordinierungsthema (1) – Terminologie und Typologisierung..... | 147 |
| 5.1.2 | Koordinierungsthema (2a) – Grundstruktur Referenzarchitektur und systematische Aufgliederung in Spezifikationsvorhaben..... | 148 |
| 5.1.3 | Koordinierungsthema (2b) – parallele Bearbeitung an Referenzarchitektur orientierter Bereichs-Spezifikationen (Group- & Product-Publications)..... | 149 |
| 5.1.4 | Koordinierungsthema (3) – harmonisierte Sicherheitslevel..... | 151 |
| 5.1.5 | Koordinierungsthema (4) – Schnittstellenprojekte / -mapping für kurzfristige Interoperabilität bestehender Systeme..... | 152 |
| 5.2 | Umsetzungsplan - Gesamtvorhaben Sichere Digitale Identitäten..... | 153 |
| 5.2.1 | Strategische Ausrichtung und Anbindung des Gesamtvorhabens..... | 156 |
| 5.2.2 | Steuerung und Lenkung des Gesamtvorhabens..... | 156 |
| 5.2.3 | Bearbeitung der Themen in Task Forces / Arbeitsausschüssen..... | 158 |
| 5.2.4 | Bereitstellung der personellen und sonstigen Ressourcen (Geschäftsführung / hauptamtliche Unterstützung)..... | 159 |
| 5.2.5 | Schirmherrschaft..... | 161 |
| 5.2.6 | Jahreskongress..... | 161 |
| 6 | Anhang..... | 164 |
| 6.1 | Schaubild zum Gesamtsachverhalt SDI (zu Kapitel 3.4)..... | 165 |
| 6.2 | Gesamtverzeichnis Kontaktpersonen..... | 166 |
| | Tabellenverzeichnis..... | 170 |
| | Abbildungsverzeichnis..... | 172 |

Abkürzungsverzeichnis

| | |
|----------|---|
| BMBF | Bundesministerium für Bildung und Forschung |
| BMG | Bundesministerium für Gesundheit |
| BMI | Bundesministerium des Innern |
| BMWi | Bundesministerium für Wirtschaft und Energie |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| CA | Certification Authority |
| CC | Common Criteria |
| CEN | Comité Européen de Normalisation / Europäisches Komitee für Normung |
| CENELEC | Comité Européen de Normalisation Électrotechnique / Europäische Komitee für elektrotechnische Normung |
| DIN SPEC | DIN-Spezifikation |
| DIN | Deutsches Institut für Normung e. V. |
| DKE | Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE |
| eIDAS | electronic IDentification, Authentication and trust Services |
| ETSI | European Telecommunications Standards Institute / Europäisches Institut für Telekommunikationsnormen |
| HSM | Hardware Security Model / Hardware-Sicherheitsmodul |
| IEC | International Electrotechnical Commission / Internationale Elektrotechnische Kommission |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| ISO | International Organization for Standardization / Internationale Organisation für Normung |
| ITU | International Telecommunication Union / Internationale Telekommunikationsunion |
| KMU | Kleine und mittlere Unternehmen |
| KRITIS | Kritische Infrastrukturen |
| LoA | Level of Assurance |
| PKI | Public Key Infrastructure / Public-Key-Infrastruktur |

| | |
|-----|---|
| SDI | Sichere Digitale Identitäten |
| TCG | Trusted Computing Group |
| TNC | Trusted Network Connect |
| TPM | Trusted Platform Module |
| TSS | TCG Software Stack (TSS) Specification |
| VDE | Verband der Elektrotechnik Elektronik und Informationstechnik e. V. |

A Management Summary

Normen und Standards sind das erste Mittel der Wahl, um den digitalen Transfer zu erreichen und mit einer globalen Marktdurchdringung zu verbinden. Sichere Digitale Identitäten sind von grundlegender Bedeutung für die erfolgreiche Digitalisierung bei gleichzeitiger Wahrung der Datensicherheit und -souveränität. Normen und Standards für Sichere Digitale Identitäten, die die Anforderungen von Wirtschaft und Gesellschaft widerspiegeln, sind grundsätzlich geeignet, in der globalen Auseinandersetzung um die Zukunftsmärkte, deutsche Wettbewerbspositionen zu stärken.

Um dies zu erreichen sind insbesondere folgende Maßnahmen erforderlich:

- Auf Basis der Analyse der vorhandenen Normen und Standards sowie einer vorgeschlagenen Referenzarchitektur ist schnellstmöglich eine Normungs-Roadmap zu konzipieren und schrittweise weiterzuentwickeln, die branchen- und dimensions-übergreifende Lösungen vorsieht und gleichzeitig Interoperabilität auf globaler Ebene sicherstellt.
- Normen und andere Spezifikationen müssen mit der notwendigen Agilität unter Beteiligung bestehender Gremien, Netzwerke und weiterer betroffener Kreise entwickelt werden. Diese Normen und sonstigen Spezifikationen müssen unterschiedlichen Erfordernissen nach Usability, Sicherheit und Aufwand (Kosten) gerecht werden.
- Um umfangreichen und unterschiedlichen Koordinierungserfordernissen gerecht zu werden, wird eine domänenübergreifende Kooperationslösung vorgeschlagen.

Auftrag

Vor dem Hintergrund der voranschreitenden Digitalisierung und dem Bewusstsein, dass Sichere Digitale Identitäten (SDI) bei der Gestaltung der digitalen Welt eine maßgebliche Rolle spielen, wurde zum 01.01.2017 im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) das Projekt Sichere Digitale Identitäten (SDI) von DIN und DKE gestartet. In einer ersten Konzeptionsphase wurde nun der Sachverhalt und die Markt- und Standardisierungssituation untersucht. Im Projektbeirat, in zahlreichen Experteninterviews sowie in Umfragen und Workshops waren über 100 Experten aus Forschung und Wirtschaft eingebunden.

Erste Ergebnisse

Im Kern zeigen die Ergebnisse eine ausgesprochene Fragmentierung der Entwicklungen, des Marktes sowie der Standardisierung. Zukunftsfähige Strukturen sind derzeit nicht erkennbar. Es fehlt ein koordinierendes Element, das diverse Einzelaktivitäten zu einem sinnvollen Ganzen, das Interoperabilität und Kompatibilität gewährleistet, zusammenführt. Erhebliche Kosten für Wirtschaft und Gesellschaft und längerfristige Wettbewerbsnachteile sind nach Auffassung der Experten die logischen Folgen.

Die außerordentliche Relevanz des Themas ist unstrittig

Über 80% der im Projekt befragten Experten sehen eine hohe bis elementare Bedeutung für Gesellschaft, Wirtschaft und Politik. Gleichzeitig adressierten die Beteiligten dringenden Handlungsbedarf. Wenn dem Thema nicht sinnvoll begegnet wird, droht massiver wirtschaftlicher und gesellschaftlicher Schaden. Die Entwicklung Sicherer Digitaler Identitäten hat unmittelbare Wirkung auf die:

- Geschwindigkeit der Digitalisierung in Deutschland (inkl. Einbindung von KMU)
- Kosten von domänenübergreifenden Digitalisierungsprojekten
- Umsetzbarkeit von Zukunftsprojekten (Industrie 4.0, eMobility, Smart City, etc.)
- Abhängigkeit der deutschen Wirtschaft von einzelnen internationalen Konzernen
- Souveränität über die eigenen Daten
- Umsetzung von Rechtsvorschriften
- Gewährleistung der IT-Sicherheit und somit auch der Zivilen Sicherheit

Der zu gestaltende Gesamtsachverhalt ist ausgesprochen komplex

Die Digitalisierung ist nicht nur eine Technik oder Technologie. Sie erweitert unsere bisherige Realität. Der Sachverhalt ist komplex und vielschichtig. Digitale Identitäten sind Dreh- und Angelpunkt für ein geordnetes Leben in der digitalen Gesellschaft. Sichere Digitale Identitäten helfen technologiebedingte Risiken zu mindern und zu beherrschen.

Strategische Herangehensweise erforderlich

Das Thema wurde einer ganzheitlichen Betrachtung unterzogen. Dabei wurden u.a. folgende Sachverhalte identifiziert:

- *Zwei Interessenspole - Zwei Definitionen*

Es gibt zwei zwar zusammengehörende aber unterschiedliche Sichtweisen auf SDI. Auf der einen Seite geht es um die Sicherheit des die Identität Abfragenden. Zum anderen ist die Identität einer natürlichen oder juristischen Person zu schützen (Sicherheit des Identitätsgebers). Bei der Entwicklung Sicherer Digitaler Identitäten sind stets beide Sichtweisen zu berücksichtigen.

- *Vielfalt der Entitäten*

Jedliches Ding oder Person, die im digitalen Raum Subjekt oder Objekt einer Interaktion sein soll, braucht eine Digitale Identität. Somit gibt es eine unbegrenzte Vielfalt an Entitätstypen. Sie können abstrakt sein, wie News, Patente, Software oder konkret (physisch), z.B. Mensch, Bauteil, Maschine etc. Dies determiniert wesentlich die Identitätslösung.

- *Vielschichtigkeit von Identitätslösungen*

Eine Identitätslösung besitzt diverse technische, wie organisatorische Gestaltungsebenen. Der Lebenszyklus einer Entität kann ein erstes Raster vorgeben (z.B. Feststellen, Abbilden, Einrichten, Verwalten, Nutzen, Löschen). Alle Ebenen können unterschiedlich gestaltet und mit unterschiedlichen Lösungskomponenten kombiniert werden. Gegebenenfalls sind weitere Variable zu berücksichtigen. Aus der Gesamtheit der Gestaltungsebenen ergibt sich die konkrete Identitätslösung.

- *Unterschiedliche Einsatzbereiche*
3 Perspektiven prägen grundsätzlich die Bedürfnisse der Sicherheit von Identitätslösungen. Diese unterscheiden sich in: (1) Identitätslösungen im eigenen Verantwortungsbereich (bspw. eigenes Unternehmen), (2) Identitätslösungen, die in den eigenen Verantwortungsbereich integriert werden (bspw. Anforderungen an Bauteile), sowie (3) Identitätslösungen für eine freie Interaktion über verschiedene Verantwortungsbereiche hinweg (bspw. Interaktion von Maschinen bei Industrie 4.0).
- *Primat des Anwendungsfalls*
Der konkrete Anwendungsfall und das damit verbundene Sicherheitsbedürfnis bestimmen die Identitätslösung. Zu berücksichtigen sind dabei insbesondere:
 - Schnelligkeit / Usability ...die beim Anwendungsfall benötigt wird
 - Sicherheit / Risiko ...das mit dem Anwendungsfall zusammenhängt
 - Kosten / Aufwand ...die mit dem Einsatz der Lösung verbunden sind

Hieraus ergibt sich bereits, dass es eine Vielzahl von Identitätslösungen gibt und braucht. Ebenso ist nicht immer die höchste Sicherheit möglich oder notwendig.

Eine Sichere Digitale Identität steht folglich immer für eine Identitätslösung bezogen auf den konkreten Anwendungsfall. Festzuhalten bleibt: SDI sind der Hebel zu einer grundlegend sicheren Gestaltung der Digitalisierung. SDI ermöglichen die Zurechenbarkeit, Verfolgbarkeit und Zuweisung bestimmter Eigenschaften digitaler Vorgänge. Sie sind damit Voraussetzung für ein sicheres Zugangsmanagement und für diverse Schutzmaßnahmen. Zum anderen erlangen sie zunehmende Bedeutung bei Schuld- und Haftungsfragen.

Insellösungen in Markt und Standardisierung

Die Untersuchung hat gezeigt, dass vorhandene Initiativen zur Entwicklung von Identitätslösungen in verschiedene Branchen und Unternehmen unterschiedlich weit fortgeschritten sind und häufig an der Unternehmens- oder Branchengrenze haltmachen. Auch im Rahmen von Forschungsprojekten entstehen häufig Insellösungen. Ursache hierfür ist eine mangelnde Koordination der unterschiedlichen Initiativen. Obwohl die Herausforderungen vergleichbar sind und zumeist keine typische Wettbewerbssituation herrscht, findet derzeit kaum ein Informationsaustausch oder eine Zusammenarbeit über Unternehmens- und Branchengrenzen hinweg statt. Unterschiedliche Definitionen, Verständnisse und Wissensstände sind die Folge. Es wird redundant gearbeitet, öffentliche und private Forschung/Entwicklung werden nicht koordiniert und Synergie- und Innovationspotentiale liegen brach. Die Situation in der Standardisierungslandschaft spiegelt das im Bericht aufgezeigte Bild am Markt wieder. Es gibt im Kontext „Sichere Digitale Identitäten“ diverse Normen- und Standardisierungsprojekte, die jedoch meist auf konkrete Anwendungsfälle begrenzt sind. Bestehende Grundlagennormen erfüllen nicht die aktuellen und künftigen Erfordernisse. Bezogen auf ein Konzept der Sicherheitslevel existieren mindestens 6 unterschiedliche Modelle.

Es braucht ein gemeinsames Ziel

Um im Sinne der zuvor genannten Wirkungsdimensionen positiv auf die Marktsituation Einfluss zu nehmen, braucht es eine Vision: das Ziel eines domänenübergreifenden möglichst international interoperablen Frameworks für Sichere Digitale Identitäten, in dem sich die eigenen (jeweiligen) Bestrebungen einfügen können.

Es wird eine Referenzarchitektur (s. Abb. 1) vorgeschlagen, die allen Aktivitäten, technischen Entwicklungen und Standardisierungsbestrebungen eine gemeinsame Grundlage gibt. Ein Baukasten, bestehend aus vorhandenen Normen, konkreten Lösungen und Anwendungsbeispielen würde im ersten Schritt ein erstes Grundgefüge bilden und damit den Markteintritt erleichtern, die Interoperabilität langfristig erhöhen sowie notwendigen Normungs- und Standardisierungsbedarf aufzeigen.

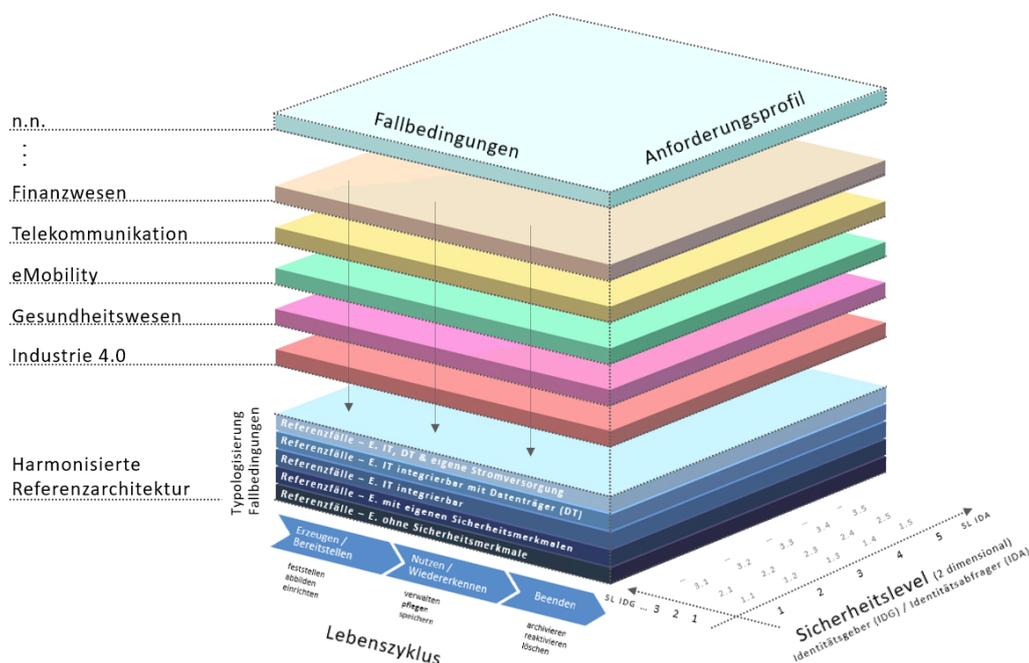


Abbildung 1 – beispielhafte domänenübergreifende Referenzarchitektur SDI

Diese Referenzarchitektur wäre sukzessive hinsichtlich Interoperabilität, Effektivität und Qualität anzupassen und weiterzuentwickeln. Neben dem Lebenszyklus werden wesentliche Dimensionen der Referenzarchitektur Entitätstypen, Anwendungsfälle, Sicherheitslevel und Branchen sein. Einzelne Teilbereiche voranzutreiben ist sinnvoll, wenn sie sich im Gesamtgebilde wiederfinden.

Die Referenzarchitektur ist die maßgebliche Grundlage für ein Normungs- und Standardisierungsprogramm (Roadmap). Im engen Dialog mit der Wirtschaft sind Prioritäten bei der Entwicklung notwendiger Normen und Standards festzulegen.

Eine domänenübergreifende Kooperation

Die Studie hat deutlich gemacht, dass deutschen Anforderungen und Interessen in der globalen Auseinandersetzung nachhaltig mehr Gewicht zu verleihen ist. Dies kann nur durch konzertiertes Handeln erfolgen. Es bedarf der Vernetzung bestehender Initiativen und Gremien. Hierzu wird der Aufbau einer domänenübergreifenden Kooperation „Sichere Digitale Identitäten “ (s. Abb. 2) vorgeschlagen. Zu diskutieren ist noch, wie diese sich in bestehende Strukturen zur Digitalisierung einordnen lässt.

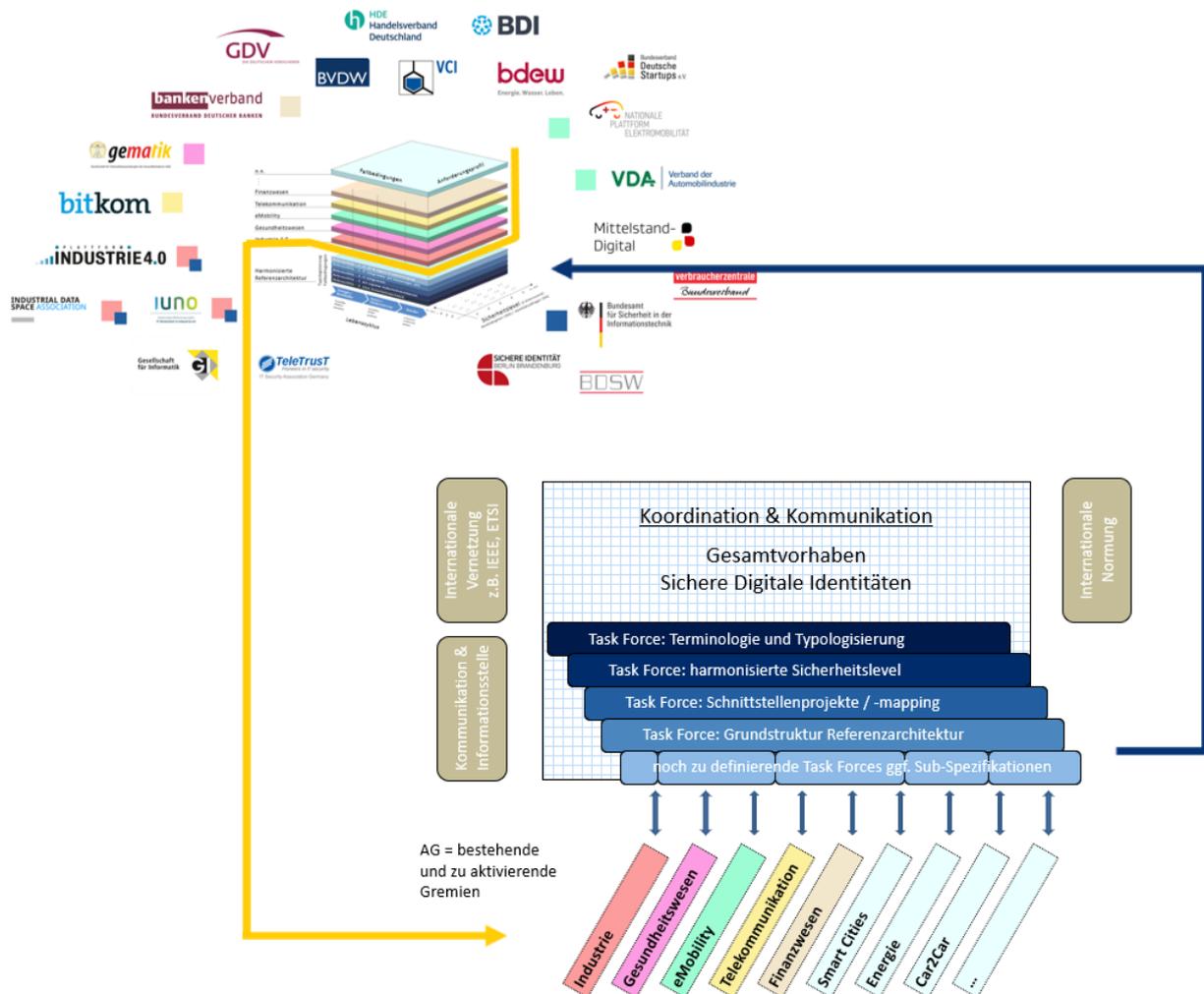


Abbildung 2 – Vernetzung bestehender Gremien zur Entwicklung einer Referenzarchitektur SDI

Nächste Schritte

DIN und DKE regen an, die Studienergebnisse nach ihrer Vorstellung im Bundesministerium für Wirtschaft und Energie auch einer breiteren Fachöffentlichkeit zu präsentieren und den vorgeschlagenen Lösungsweg zu diskutieren. In einem Workshop mit potentiellen Kooperationspartnern und gegebenenfalls weiteren interessierten Kreisen sollten die Gestaltung einer Referenzarchitektur und darauf aufbauende Arbeitsschritte diskutiert werden.

Die weiteren Anstrengungen sind zunächst darauf zu richten, die Referenzarchitektur so zu gestalten und weiterzuentwickeln, dass sie eine hinreichende und verlässliche Arbeitsgrundlage bildet. Eine Veröffentlichung als DIN SPEC könnte in Erwägung gezogen werden. Eine nationale Spezifikation könnte

wiederum die Grundlage für die Initiierung entsprechender europäischer und/oder internationaler Standardisierungsprojekte sein.

Die weiterentwickelte Referenzarchitektur ist Grundlage zur Entwicklung und regelmäßigen Fortschreibung einer Normungs-Roadmap. Vorausgesetzt die relevanten Projektpartner beteiligen sich an den erforderlichen Arbeiten, sollte im Jahresverlauf 2018 eine erste Version der Roadmap konzipiert und veröffentlicht werden.

DIN und DKE werden erste branchenübergreifende Normungsprojekte, die der Struktur der Referenzarchitektur folgen, mit den potentiellen Kooperationspartnern initiieren.

Maßgeblich für den Erfolg wird die Einbindung bestehender Gremien, wichtiger Netzwerke, Organisationen und Vertretern der Wirtschaft sowie gegebenenfalls weiterer Interessengruppen sein. Mit diesen sind konkrete Organisationslösungen auszuloten und kurzfristig so umzusetzen, dass effizient und agil die aufgezeigten Herausforderungen kooperativ gemeistert werden können.

DIN, DKE und zahlreiche Experten sehen weiterhin das Erfordernis einer politischen und finanziellen Unterstützung durch die Bundesregierung.

B Aufbau des Projektberichts

Im 1. Kapitel erfolgt die Projektbeschreibung, beinhaltend die Ausgangslage, Motivation und Ziel, die zu dem Projektantrag geführt haben, sowie die Definition der Ziele und Aufgaben bzw. Arbeitspakete des Projektes. Ferner werden die das Projekt bearbeitenden Organisationen DIN und DKE kurz vorgestellt. Es folgt im Sinne der Zielerfüllung die Gegenüberstellung der Arbeitspakete zur Aktivitätendarlegung verweisend auf die einzelnen Kapitel und Anhänge.

Das 2. Kapitel legt die verschiedenen Mittel zur Generierung von Informationen dar und zeigt in Teilen die hieraus gewonnenen Ergebnisse oder den weiteren Analyseprozess beeinflussenden Teilergebnisse. Hierbei wird unterschieden in die Konsultation bzw. Einbindung von Experten und Stakeholder und die Informationsbeschaffung über Desk-Research-Tätigkeiten.

Zur Expertenkonsultation gehörten die Beiratssitzung, Vorgespräche, der Fragebogen, umfassendere Interviews, Themen-Workshop, Stakeholder-Workshop, Zwischen- und Folgegespräche/Kontakte. Diesbezügliche Ergebnisse wurden aufgrund des umfassend zu strukturierenden Informationsgehalts nicht in Kapitel 2 dargestellt sondern wurden logisch in Kapitel 3 und 4 zusammengeführt.

Schwerpunkte der Desk Research Tätigkeiten und In-House-Befragung waren die Normenrecherche und die Recherche zum Thema Recht. Erstere beinhaltet neben der Auflistung vom Thema potentiell tangierter Normen und der jeweiligen Gremien sowie Organisationen, die Identifikation und Kurzbeschreibung der zentralen bereits zum Thema existierenden Normenwerke. Die Recherche Recht beinhaltet die Dar- und Auslegung der wesentlichen juristischen Grundlagen und Vorgaben und vollzieht darüber hinaus eine Relevanzbeurteilung derselben.

Im 3. Kapitel erfolgt eine logische Zusammenführung der erarbeiteten im Wesentlichen nicht wertenden Informationen aus Expertenkonsultation und Desk-Research im Sinne einer ganzheitlichen Sach- und Prozessbeschreibung des Themas und dessen im Analyseprozess herausgearbeiteten Dimensionen. Die Auffächerung der Betrachtungsebenen und Identifizierung der unterschiedlichen Handlungsebenen dienen als Grundlage zum Erfassen des Gesamtsachverhalts und zum Entwerfen einer Strategie zur Gestaltung des Themas und diesbezüglicher Handlungsempfehlungen im Speziellen.

Zunächst werden die unterschiedlichen aus dem Analyseprozess ableitbaren Sichtweisen / Betrachtungsebenen beschrieben. Orientierung und Systematisierung geben hierbei u.a. die Interessenspole Identitätsgeber und des Identitätsabfrager, die Einsatz- und Verantwortungsbereiche von Identitätslösungen, sowie das vom Anwendungsfall ableitbare Sicherheitslevel, die bereits in unterschiedlichen Ansätzen existieren, und die dahingehend determinierenden Faktoren, wie Schnelligkeit, Kosten, Risiko und Anwendbarkeit.

Im Anschluss werden sukzessive orientiert am Lebenszyklus einer Digitalen Identität die verschiedenen Handlungsebenen erläutert und ein Einblick in die je Schritt relevanten Sachverhalte, Herausforderungen und Lösungen gegeben. Diese Schritt-für-Schritt-Erklärung baut ein Schaubild auf, welches sowohl die

Dimensionen adressiert, wie die Handlungsfelder in den Gesamtzusammenhang setzt. Das Kapitel schließt mit strategischen Anwendungsbeispielen, die für das Verständnis hilfreich sind und die Breite des Themas SDI deutlich machen.

Das Kapitel 4 bringt die wertenden Aussagen und die Feststellungen zur Situation der in Kapitel 2 dargestellten Analyse und die logische Betrachtung des Sachverhalts aus Kapitel 3 resümierend zu Kernaussagen und Schlussfolgerungen zusammen, welche für den handlungspolitischen Umgang mit dem Thema grundlegend sind. Wesentliche Grundlage ist hierbei die Expertenkonsultation, die zudem mit einzelnen quantitativen Ergebnissen zu den Aussagen der Experten und exemplarischen Auszügen aus Befragung und Gesprächen dargestellt wird. Die Schlussfolgerungen beziehen sich zunächst auf Aussagen zur Relevanz und Bedeutung des Themas, der aktuellen Marktsituation und der Bedürfnisse bzgl. SDI. Daraufhin adressieren sie ein erstes Referenzmodell als verbindendes Element der fragmentierten Lösungs- und Standardisierungslandschaft. Es folgen Ableitungen aus dem Kapitel 2 und 3 zum Inhalt des Referenzmodells und zur Herangehensweise an die Entwicklung desselben und mögliche Auswirkungen. Hierbei thematisiert das Kapitel 4.16 welche Grundlagen bereits bestehen und welche weiteren in der bisherigen Förderphase geschaffen wurden.

Kapitel 5 entwickelt den Master- und Strukturplan / Umsetzungsplan, der für die Erstellung einer SDI-Referenzarchitektur und die Etablierung Sicherer Digitaler Identitäten als Vertrauensanker in der digitalisierten Welt den Aufbau eines domänenübergreifenden Aktionsnetzwerkes SDI und die Koordinierung der Zusammenarbeit durch einen neutralen Akteur vorschlägt. Hierbei sind die identifizierten Initial-Themen, die Terminologie und Typologisierung, die Grundstruktur Referenzarchitektur und systematische Aufgliederung in Spezifikationsvorhaben, die an Referenzarchitektur orientierte Sub-Spezifikationen (Group- & Product-Publications), eine Harmonisierung der Sicherheitslevel, das Schnittstellenmapping für kurzfristige Interoperabilität bestehender Systeme.

Der Anhang in diesem Dokument ist aufgrund der Größe des Berichts und der Dokumente auf einzelne Anlagen beschränkt. Zusätzliche Anhänge befinden sich in einer separaten PDF-Datei.

1 Projektbeschreibung

1.1 Projektinitiierung und -antrag

Das Projekt Sichere Digitale Identitäten wurde vor dem Hintergrund initiiert, dass im Rahmen der voranschreitenden Transformation der Wirtschaft und Gesellschaft durch die Digitalisierung dem Thema Sichere Digitale Identitäten offenbar eine immer größere Bedeutung beizumessen ist. Sichere Digitale Identitäten (SDI) hat sich inzwischen zu einem Schlagwort entwickelt, das von unterschiedlichsten Akteuren mit großen Erwartungen verbunden wird. Die neuen Möglichkeiten in der digitalen Vernetzung und für digitale Dienstleistungen führen in allen Bereichen von Wirtschaft, Gesellschaft und Politik zu immer tiefer greifenden systemischen Veränderungen und lösen so u.a. in Fragen der Rechts- und Investitionssicherheit steigende Ansprüche an die Grundregeln und -struktur aus. Der Prozess der Identifikation von Menschen und Objekten ist diesbezüglich eine Grundvoraussetzung, der im Sinne der Sache und aller Beteiligten sicher zu gestalten ist. Er betrifft sowohl sämtliche Bereiche der Wirtschaft, Gesellschaft, wie auch unmittelbar die des Bundes. So wie es eine politische Aufgabe ist, in der analogen Welt eine Infrastruktur zu gestalten, in der sich alle sicher auf der Basis von Rahmenbedingung und Regeln bewegen können, so muss dies heute auch für die digitale Welt gelten. Folglich ist es die Aufgabe von Politik und den entsprechenden administrativen Stellen, auf eine solche Infrastruktur hinzuarbeiten.

Zu berücksichtigen ist hierbei, dass die digitale Welt vom Grundsatz her neue Sichtweisen erfordert. So kommunizieren und interagieren in ihr bzw. durch sie nicht nur Menschen miteinander, sondern zunehmend Menschen mit Maschinen und Programmen sowie Maschinen mit Maschinen. Digitale Identitäten machen hierbei jede Entität im digitalen Raum erst existent. Die Sicherheit derselben scheint damit eine Schlüsselrolle bei der Realisierung der wachsenden Digitalisierung einzunehmen. Das Thema muss daher umfassend auf Basis klarer politischer Rahmenbedingungen des Bundes behandelt werden. Branchenbezogene Ansätze führen bisher offenbar zu verschiedensten spezifischen Lösungen, deren Sicherheit nicht geklärt ist und welche eine domänenübergreifende Vernetzung erschweren. Es ist davon auszugehen, dass diese unterschiedlichen Lösungen, die zudem teilweise redundant entwickelt werden, nicht zu einem Gesamtkonzept führen, welches Effektivität, Interoperabilität, Sicherheit und Investitionssicherheit sowie gesellschaftliche Verantwortung gewährleistet. Die Situation wird daher dem Thema insgesamt nicht gerecht.

Um dieser Situation zu begegnen, wurde das Projekt Sichere Digitale Identitäten mit einer 10-monatigen Konzeptionsphase initiiert, um im Wesentlichen einen Projekt-Master- und Strukturplan für eine Roadmap „SDI “ auszuarbeiten. Hierzu wurde avisiert

- das aktuelle Umfeld zu beschreiben
- relevante Aktivitäten und Akteure am Markt zu identifizieren
- Handlungsbedarfe in den Anwendungsbereichen (Domänen) zu identifizieren
- den Handlungsbedarf zur Etablierung „Sicherer Digitaler Identitäten “ zu beschreiben
- die relevanten Normen und Standards aufzulisten
- Empfehlungen für die Gestaltung von „Sicheren Digitalen Identitäten “ zu geben

- und eine Organisationsform zu definieren sowie notwendige Gremien und deren Aufgaben für die Umsetzung eines Konzepts Roadmap „Sichere Digitale Identitäten “ in einer anschließenden Verstetigungsphase zu beschreiben

Die Notwendigkeit das Thema SDI ganzheitlich zu betrachten und die Konzeptionsphase zu initiieren, basierte auf den Annahmen,

...dass SDI grundlegend sind für das:

- Sicherstellen von Vertrauen, Integrität und Verfügbarkeit von Entitäten im digitalen Raum
- Absichern technischer und organisatorischer Prozesse
- Absichern rechtlicher und kaufmännischer Prozesse
- Herstellen von Transparenz
- Schaffen kritischer Voraussetzungen zur Anwendung konvergenter Technologien
- Sichern der digitalen Souveränität

...dass SDI hierbei folgende Rahmenbedingungen bilden bzw. bedienen:

- Sicherheits-Infrastruktur im digitalen Raum
- Gültigkeit für Personen, Maschinen, Produkte und Organisationen sowie Datensätze, Dateien, Patente und Zertifikate
- Multidisziplinarität, Branchenunabhängigkeit, Diskriminierungsfreiheit
- auf internationalen Regelungen basieren

...dass Hindernisse und Lücken möglicherweise folgendes sein können:

- fehlende internationale Regelungen
- fehlendes Bewusstsein bzw. fehlender Wille für interdisziplinäres, von Branchen unabhängiges Vorgehen
- viele Insellösungen und dynamische Entwicklungen (schnelle Lösungen vs. langfristiges Konzept)
- fehlender „trusted enabler“, der Stakeholder orchestriert und dem die Kompetenz und Verantwortung für die Gestaltung des Prozesses übertragen wird

Ergebnis der Gesamtinitiative (Konzeptions- und Verstetigungsphase) soll eine Deutsche Roadmap „Sichere Digitale Identitäten “ sein, die sowohl politische, rechtliche als auch technologische Herausforderungen und Ziele definiert sowie Themen wie z. B. Governance und Management von sicheren Identitäten, einschließlich Sachidentitäten, behandelt.

1.2 Projektbearbeitende DIN und DKE

1.2.1 DIN als Projektdurchführender

Das Deutsche Institut für Normung e.V. (DIN) führt das Projekt „Sichere Digitale Identitäten“ gefördert durch das Bundesministerium für Wirtschaft und Energie durch. DIN ist eine unabhängige Plattform für Normung und Standardisierung in Deutschland und weltweit. Als Partner von Wirtschaft, Forschung und Gesellschaft trägt DIN wesentlich dazu bei, Innovationen zur Marktreife zu entwickeln und Zukunftsfelder wie Industrie 4.0 und Smart Cities zu erschließen. Rund 32.000 Experten aus Wirtschaft und Forschung, von Verbraucherseite und der öffentlichen Hand bringen ihr Fachwissen in den Normungsprozess ein, den DIN als privatwirtschaftlich organisierter Projektmanager steuert. Die Ergebnisse sind marktgerechte Normen und Standards, die den weltweiten Handel fördern und der Rationalisierung, der Qualitätssicherung, dem Schutz der Gesellschaft und Umwelt sowie der Sicherheit und Verständigung dienen. DIN wurde 1917 gegründet und feierte 2017 sein 100-jähriges Bestehen.

1.2.2 DKE als Unterauftragnehmer aufgrund Alleinstellungsmerkmals

Die vom VDE getragene DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE erarbeitet Normen und Sicherheitsbestimmungen für die Elektrotechnik, Elektronik und Informationstechnik. Sie vertritt die deutschen Interessen im Europäischen Komitee für Elektrotechnische Normung (CENELEC) und in der Internationalen Elektrotechnischen Kommission (IEC). Rund 5.500 Experten aus Wirtschaft, Wissenschaft und Verwaltung erarbeiten das VDE-Vorschriftenwerk in der DKE. Die VDE-Bestimmungen basieren heute größtenteils auf Europäischen Normen, die zu etwa 80 Prozent das Ergebnis der internationalen Normungsarbeit der IEC sind.

Eine wesentliche Aufgabe des Projektes ist es, die bestehenden Normen und Standards sowie laufende bzw. beantragte Normungsverfahren auf nationaler, europäischer und internationaler Ebene zu sichten und im Hinblick auf die Nutzbarkeit für Digitale Identitäten zu bewerten. Für die elektrotechnische Seite kann ausschließlich die DKE, in Form eines Unterauftrages, die hierzu in den einzelnen Arbeitspaketen anfallenden Aufgaben ausführen.

In diesem Sinne wurde eine freihändige Vergabe durchgeführt, da nur ein Unternehmen in Betracht kommt (§ 3 Abs. 5 I VOL/A). Die DKE ist gemäß Ziffer 4 des Vertrags zwischen DIN und VDE Normungsorgan von DIN (Ziffer 2.2. der Satzung von DIN); die wirtschaftliche organisatorische Einbindung (Trägerschaft) der DKE liegt beim VDE e.V.

In Ziffer 1.3 der Geschäftsordnung der DKE wird präzisiert, dass die DKE ein Normenausschuss entsprechend der Richtlinie für Normenausschüsse von DIN ist. Die DKE ist die Normungsorganisation, die für die Normungsarbeiten des Bereichs Elektrotechnik, Elektronik auf nationaler, europäischer und internationaler Ebene in den entsprechenden Organisationen CENELEC, ETSI und IEC verantwortlich ist.

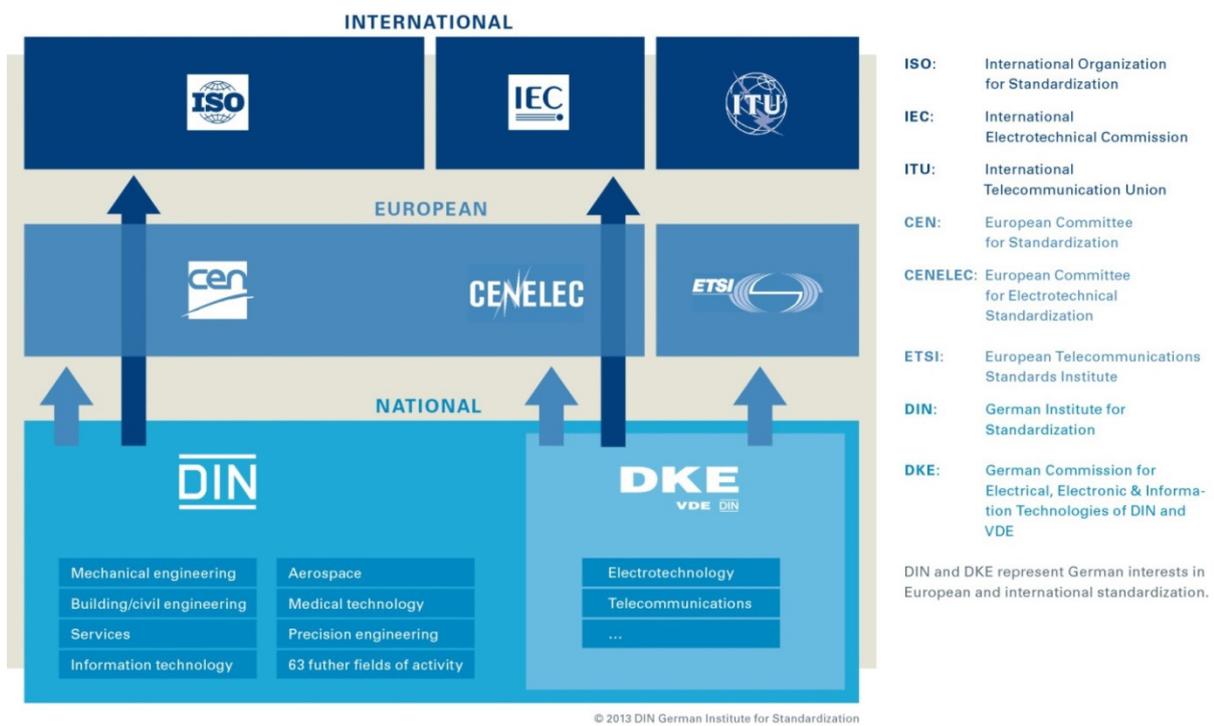


Abbildung 3 – Aufteilung der Verantwortungsbereiche in der Normung

1.3 Zielerfüllung – Gegenüberstellung Arbeitspakete und Aktivitätendarlegung

Tabelle 1 - Gegenüberstellung Arbeitspakete und Resultate/Aktivitäten gemäß Projektantrag

| | Arbeitspaket | Ziel bzw. Ergebnis | Zielerfüllung siehe |
|---|--|---|---------------------------------------|
| 1 | Projekt-Master- und Strukturplan für die Roadmap | 1a. DIN-DKE Projektplan für die Vorbereitungsphase abgestimmt | Anhang 6.3 und Kapitel 1.3, Tabelle 1 |
| | | 1b. Projekt-Master- und Strukturplan für die Roadmap dokumentiert | Kapitel 5 |
| 2 | Identifikation/Einbindung der Key-Player | 2a. Repräsentanten für den Projektbeirat festgelegt | Kapitel 2 und Anhang 6.3 |
| | | 2b. Repräsentanten für Fragebogen und Alignment-Phase festgelegt | Kapitel 2.1 und Anhang 6.3 und 6.4 |
| | | 2c. Repräsentanten für den Key Stakeholder Workshop eingeladen | Kapitel 2 und Anhang 6.7 |
| | | 2d. Key-Player für die Verstetigungsphase identifiziert | Kapitel 2.3, 5 und Anhang 6.2 und 6.3 |
| 3 | Einbindung laufender Aktivitäten/Initiativen | 3a. Erstellung einer Übersicht aller relevanten Normungsaktivitäten | Kapitel 2.3 |
| | | 3b. Auflistung von Aktivitäten anderer Organisationen | Kapitel 2.2 |

| | | | |
|---|---|--|-----------------------------------|
| | | 3c. Auswertung der Fragebögen & Alignment-Interviews | Kapitel 2.1.3, 3 und 4 |
| | | 3d. Abschlussbericht aus Fragebögen & Alignment-Interviews | Kapitel 2.1, 3 und 4 |
| 4 | Unterstützung für das BMWi für die Gestaltung der Verstetigungsphase | 4a. Aufbau einer Homepage bei DIN für öffentliche Informationen zum Projekt | Anhang 6.11 und Anhang 6.12 |
| | | 4b. Aufgaben in Abstimmung mit dem BMWi | Kapitel 5, div. |
| 5 | Definition & Beschreibung der Organisationsform und der notwendigen Gremien/Aufgaben für die Verstetigungsphase | 5a. Organigramm für die Verstetigungsphase | Kapitel 5.2 |
| | | 5b. Beschreibung der Gremien und deren Aufgaben und Verantwortlichkeiten in der Verstetigungsphase | Kapitel 5.2.1 - 5.2.6 |
| | | 5c. Konzept zur Beteiligung der dt. Wirtschaft in der Verstetigungsphase | Kapitel 5.2 und 5.2.1 |
| 6 | Key Stakeholder Workshop und Abgleich der Interessen | 6a. Veranstaltung im BMWi | Kapitel 2.1.6 und Anhang 6.7, 6.8 |
| | | 6b. Ergebnisse des Workshops zusammengefasst | Kapitel 2.1.6 und Anhang 6.9 |
| 7 | Feinjustierung des Projekt-Master- und Strukturplans und Dokumentation | 7a. Überarbeiteter Projekt-Master- und Strukturplan für die Roadmap (Dok. 1b.) | Kapitel 5 |
| 8 | Vorbereitungen für die Verstetigungsphase | 8a. Handlungsempfehlungen für die Verstetigungsphase | Kapitel 5 |

2 Analyseprozess

Zur Analyse des Themas und der Sachlage wurden verschiedene Instrumente zur Generierung von aktuellen Informationen sowohl wertender, wie deskriptiver Art gewählt. Hierbei ist zu unterscheiden in die

- Konsultation bzw. Einbindung externer Experten und Stakeholder in Kapitel 2.1 u. 2.2
 - o Beirat
 - o Vorgespräche
 - o Umfrage mit Fragebogen
 - o Experten-Interviews
 - o Themen-Workshop
 - o Stakeholder-Workshop im BMWi
 - o Zwischen- und Folgegespräche / Kontakte etc.

- Informationsbeschaffung via Desk-Research-Tätigkeiten und Inhouse-Befragung in Kapitel 2.3 u. 2.4
 - o Allgemeine Recherche
 - o Normenrecherche
 - o Rechtsrecherche

Der Analyseprozess stellt eine Momentaufnahme dar. Mit den Erkenntnissen aus dem Analyseprozess, insbesondere der logischen Zusammenführung und Betrachtung des Gesamtsachverhaltes in Kapitel 3, induzieren für eine Verstetigung eine Anpassung des Scopes.

2.0 Auswertung des Analyseprozesses

Insbesondere aufgrund des umfassend zu strukturierenden Informationsgehalts der Expertenkonsultation bedarf es zur Auswertung und zum Verständnis der logischen Zusammenführung und Aggregation der Inhalte. Das Kapitel 2.1 stellt daher keine unmittelbaren Ergebnisse vor, bzw. begrenzt sich maximal auf für den weiteren Prozess relevante Teilergebnisse. Die ausführliche Ergebnisdarlegung, -zusammenführung und -interpretation erfolgt mit Kapitel 3 und 4, welche in diesem Sinne nicht nur auf das Kapitel 2 verweisen, sondern auch unmittelbar aus Fragebögen und Interviews etc. zitieren. Die Zitate und Erhebungen sind anonymisiert aus Rücksichtnahme darauf, dass diverse Experten offizielle Statements (zumindest in Teilen) durch die Geschäftsführung und oder Unternehmenskommunikation hätten freigeben lassen müssen oder teilweise nicht in der Art und Weise kommuniziert hätten. Einige Befragte machten dahingehend auch die Anonymisierung explizit zur Vorbedingung der Teilnahme.

In dem Sinne, dass das Herausarbeiten der Informationen interdependent erfolgte, stellt Kapitel 2.2 einen Teil der Erkenntnisse der Expertenkonsultation dar. Die Kapitel 2.3 und 2.4 enthalten ebenso einzelne Erkenntnisse aus der Expertenkonsultation. Allerdings war die Expertenkonsultation und Auswertung zeitlich versetzt und die logische Zusammenführung und Gesamtbetrachtung machen in der weiteren Bearbeitung des Themas eine Ausweitung des Fokus für die Rechts- und Normenthemen sinnvoll. Die Teilergebnisse der Normen-, Rechts- und allgemeinen Recherche finden sich direkt in den Unterkapiteln 2.3 und 2.4. Die Interpretation im Gesamtzusammenhang erfolgt allerdings auch mit Kapitel 3 und 4.

In Kapitel 3 und 4 werden zudem statistische Auswertungen der Expertenkonsultationen gemacht. Da mit einzelnen Experten mehrere Gespräche (bspw. Vorgespräch und ausführliches Interview) geführt wurden, wurden diese als ein Gespräch in die Wertung miteinbezogen, um die statistischen Aussagen nicht zusätzlich zu verzerren. Beantwortete Fragebögen wurden gesondert gezählt. Mehrere Fragebögen wurden durch mehrere Beteiligte bzw. durch eine Verbandsabfrage also unterschiedliche Unternehmen ausgefüllt. Hier wurde der Fragebogen maximal doppelt gewichtet. Die Expertenaussagen im Beirat, Themen-Workshop und Stakeholder-Workshop wurden nicht gewertet, es sei denn sie waren unmittelbar zurechenbar und nicht doppelt mit späteren Beteiligungen der Experten an der Analyse. Die statistische Auswertung ist nur bedingt aussagekräftig. Sie bedient sich weder einer ausgewogenen Grundgesamtheit der von der Digitalisierung betroffenen Wirtschaft / Gesellschaft, noch sind die zugeschriebenen Aussagen stets als gesichert anzusehen. Insbesondere bei den Expertenkonsultationen durch Interviews / Gespräche unterlag die Feststellung der Aussagen dem Interviewer und konnte oftmals nur nach bestem Wissen und Gewissen getroffen werden. Hinsichtlich der Clusterung zu den aggregierten Aussagen blieb in vielen Bereichen Interpretationsspielraum. Beim Fragebogen ist dies u.a. darin begründet, dass mit offenen Fragen gearbeitet wurde und die geclusterten Antworten zudem an unterschiedlichen Stellen gegeben wurden. Bei den Gesprächen und Interviews ging es vornehmlich, um das gemeinsame Erarbeiten eines breiten Profils von Sichtweisen und die Aufdeckung von relevanten Sachverhalten. Viele nun im Nachhinein definitive Fragen / zu bewertende Annahmen konnten zu Anfang gar nicht klargestellt bzw. gemacht werden, sondern sind vielmehr das Ergebnis der Analyse. Insgesamt wurde sich daher bei den statistischen Aussagen auf solche beschränkt, die klare oder besondere Trends in der gesamten Untersuchung darstellten.

2.1 Konsultation/Einbindung von Experten und Stakeholdern

2.1.1 Beirat

Zur Begleitung und Unterstützung des Projekts wurde ein Beirat gegründet. Seine Aufgaben waren die beratende Begleitung mit inhaltlicher/strategischer Ausrichtung und die Funktion der Beiratsmitglieder als Multiplikatoren. Die Zusammenstellung des Beirates erfolgte im Januar 2017. Avisiert war hierbei eine Zusammensetzung im Sinne eines engen Kreises von Vertretern fachlich relevanter Bundesministerien und Behörden sowie Verbänden und Forschungsorganisation. Um Neutralität zu wahren, wurde in der Konzeptionsphase bewusst auf Industrievertreter im Beirat verzichtet.

1. Sitzung am 2. März 2017

Die Definition, Konstitution und 1. Sitzung des Beirats des Projektes „Sichere digitale Identitäten“ (SDI) wurde am Donnerstag, den 2. März 2017, von 13:00 bis 16:00 Uhr bei DIN in einem Kick-off Workshop umgesetzt. Es nahmen 21 Personen teil. Hierbei wurde das Projekt mit den 2 Bewilligungsphasen Konzeptions- und Verstetigungsphase vorgestellt, die Motivation und Erwartungen der Beiratsmitglieder abgefragt, Projektplan und Umfeldanalyse vorgestellt, diskutiert und angenommen und ein Brainstorming zu Chancen und Risiken Erwartungen und Empfehlungen vorgenommen sowie eine Liste von Key-Player für den weiteren Prozess diskutiert und ergänzt. Details, siehe:

- ➔ Anhang 6.3 Kapitel 2.1.1 - Bericht 1. Beiratssitzung 2017-03-02 mit ausgewählten Präsentationen

2. Sitzung innerhalb des Stakeholder-Workshops am 10. Juli 2017

Zur 2. Beiratssitzung wurde im Anschluss zum Stakeholder-Workshop am 10. Juli im Bundesministerium für Wirtschaft und Energie (BMWi) geladen. Die Ergebnisse liefen in den Zwischenbericht mit ein. Details, siehe:

- ➔ Anhang 6.7 Kapitel 2.1.6 - Einladungsschreiben (Mail) und Agenda für Stakeholder-Workshop
- ➔ Anhang 6.9 Kapitel 2.1.6 - Zwischenbericht - Zusammenfassung der Diskussion der Zwischenergebnisse

Für den weiteren Analyseprozess relevante Teilergebnisse

In der 1. Beiratssitzung war für die weitere Gestaltung der Konzeptionsphase u.a. maßgeblich, dass beschlossen wurde, statt wie ursprünglich geplant, nur Leitfaden-Interviews durchzuführen, zunächst einen Fragebogen aufzusetzen und diesen an die Key-Player zu senden.

Ergebniszusammenführung

Im Sinne des Kapitels 2.0 „Auswertung des Analyseprozesses“ wurden aufgrund des umfassend zu strukturierenden Informationsgehalts die Erkenntnisse der unterschiedlichen Expertenkonsultationen in den Kapitel 3 und 4 aggregiert und zu einer logischen Gesamtbetrachtung und Gesamtbewertung zusammengeführt. Hierzu wurden auch die Aussagen aus den Beiratssitzungen hinzugezogen und die oben genannten Zwischenberichte genutzt.

2.1.1.1 Personen - Mitglieder im Beirat

In den Beirat berufen wurden:

| Bereich | Anrede | Titel | Vorname | Name | Organisation |
|-------------|--------|-------|---------|------|--------------|
| Umsetzung | Frau | | | | |
| Ministerien | Herr | | | | |
| Verbände | Herr | | | | |
| Forschung | Herr | | | | |
| Behörden | Herr | | | | |
| Umsetzung | Herr | | | | |
| Verbände | Herr | Dr. | | | |
| Verbände | Herr | | | | |
| Umsetzung | Herr | | | | |
| Forschung | Herr | | | | |
| Ministerien | Frau | | | | |
| Umsetzung | Herr | | | | |
| Plattformen | Herr | | | | |
| Ministerien | Herr | | | | |
| Behörden | Herr | | | | |
| Verbände | Herr | | | | |
| Verbände | Herr | Dr. | | | |
| Verbände | Herr | | | | |
| Ministerien | Herr | | | | |
| Umsetzung | Herr | Dr. | | | |
| Verbände | Herr | | | | |
| Umsetzung | Herr | | | | |
| Umsetzung | Herr | Dr. | | | |
| Verbände | Herr | | | | |
| Ministerien | Herr | Dr. | | | |
| Verbände | Herr | | | | |

Darüber hinaus an der ersten Sitzung am 2. März 2017 beteiligt waren:

| Bereich | Anrede | Titel | Vorname | Name | Organisation |
|-----------|--------|-------|---------|------|--------------|
| Umsetzung | Herr | | | | |
| Behörden | Herr | | | | |
| Behörden | Herr | | | | |

2.1.2 Vorgespräche

Vor und während der Erstellung und zu Beginn des Versands der Fragebögen wurden einige Vorgespräche geführt. Diese Vorgespräche werden hier separat von den Interviews aufgeführt, da sie nicht den intendierten Charakter zur umfassenden Informationsgewinnung hatten. Zum Teil waren diese Vorgespräche nur sehr kurz und geschahen spontan (bspw. auf der CEBIT und der Hannover Messe), dienten aber insgesamt als Grundlage für die Einschätzung bzw. Orientierung, wie das Thema wahrgenommen und verstanden wird und hatten somit Einfluss auf die Entwicklung des Fragebogens, der

Website, die Gestaltung der Interviews etc. Einige Gespräche hatten aber trotzdem inhaltlich den Charakter der später angesetzten Interviews und werden damit doppelt aufgeführt.

Für den weiteren Analyseprozess relevante Teilergebnisse

1. Erklärungsbedarf zu SDI
Es hat sich gezeigt, dass der Begriff „Sichere Digitale Identitäten “ bei einzelnen Befragten IT-Spezialisten assoziationsfrei war und somit, um das Thema diskutieren zu können, zunächst einmal Erklärungsbedarf bestand. Daraufhin waren aber klare Vorstellungen und Positionen vorhanden.
2. Klare Vorstellungen, aber unterschiedliche Perspektiven/Anwendungsfälle
Die Gespräche bzw. angesprochenen Sachverhalte zeigten unterschiedliche Perspektiven auf das Thema. Zeigte man weitere mögliche Perspektiven auf (bspw. vom Einsatz von Digitalen Identitäten im eigenen Unternehmen hin zur Frage nach der Nutzung bei der Interaktion mit anderen Unternehmen), eröffnete dies in der Regel unmittelbar ein weiteres Diskussionsfeld, welches für die Befragten nicht zwingend weniger relevant war.
3. Vielfalt der Sachverhalte je Anwendungsfall
Die angesprochenen Sachverhalte, Herausforderungen, Probleme, etc. waren auch je Anwendungsfall unterschiedlichster Art. Im Sinne des Lebenszyklus einer SDI wurden unterschiedliche Besonderheiten, Schwierigkeiten, Lösungswege etc. adressiert.
4. Vielfalt der Entitäten
Unabhängig von Perspektiven und Sachverhalten wurden von den Personen unterschiedlichste Entitäten genannt, für die Digitale Identitäten Relevanz haben.
5. Relevanzeinschätzung nach gedanklicher Auseinandersetzung
Nach dem gemeinsamen Eruiieren von Definition und möglicher Anwendungsbereiche wurde die Relevanz deutlich anders eingeschätzt.

Ergebniszusammenführung

Im Sinne des Kapitels 2.0 „Auswertung des Analyseprozesses “ wurden aufgrund des umfassend zu strukturierenden Informationsgehalts die Erkenntnisse der unterschiedlichen Expertenkonsultationen in den Kapitel 3 und 4 aggregiert und zu einer logischen Gesamtbetrachtung und Gesamtbewertung zusammengeführt. In diesem Sinne wurden auch die Vorgespräche, in denen relevante Aussagen gemacht wurden, qualitativ und quantitativ einbezogen.

2.1.2.1 Personen - Gesprächspartner

Zu den Personen mit denen Vorgespräche geführt wurden, zählten u.a. die folgenden.

| Bereich | Anrede | Titel | Vorname | Name | Organisation |
|-------------|--------|----------|---------|------|--------------|
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Plattformen | Herr | Dr.-Ing. | | | |

| Bereich | Anrede | Titel | Vorname | Name | Organisation |
|-------------|--------|-----------|---------|------|--------------|
| Unternehmen | Herr | | | | |
| Forschung | Frau | | | | |
| Behörden | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Frau | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Unternehmen | Herr | | | | |
| Forschung | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Forschung | Herr | Prof. Dr. | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Verbände | Herr | | | | |
| Unternehmen | Herr | | | | |
| Verbände | Herr | | | | |
| Unternehmen | Herr | | | | |

Personenbezogene Daten aus Gründen des Datenschutzes hier nicht sichtbar

2.1.3 Umfrage mit Fragebogen

Auf der Beiratssitzung am 2. März 2017 wurde beschlossen, dass zur Analyse des Themas zunächst ein Fragebogen an die identifizierten Key Player versandt werden sollte. Die entsprechenden Key-Player und Empfänger des Fragebogens wurden zunächst auf der Beiratssitzung und in der Diskussion mit dem Wirtschaftsministerium ermittelt. Hierbei ergab sich eine Liste von etwa 100 Institutionen und Personen. Diese ergänzte sich später um die in Zwischengesprächen und Interviews genannten weiteren möglichen Ansprechpartner. Zudem wurde der Fragebogen durch Multiplikatoren oder in Verbänden weiterverteilt.

Der unmittelbare schriftliche Rücklauf erfolgte in 18 Fragebögen. Bei der Beantwortung der Fragebögen waren aber je Fragebogen meist mehrere Personen oder sogar Unternehmen beteiligt. In Teilen wurden diese auch mit Abgabe des Fragebogens genannt. Hieraus resultiert eine beteiligte Personenanzahl von 31 Fragebogenteilnehmern (siehe 2.4.1.1).

Über die schriftliche Beteiligung hinaus erwirkte der Versand der Fragebögen diverse Interessensbekundungen. Hieraus resultierten weitere Zwischengespräche und teils umfassende Interviews. Für letztere diente der Fragebogen generell mehrfach als Grundlage oder zur Vorbereitung. Die Interviews erweitern somit die Beantwortungsrate. Die Ergebnisse wurden auch daher in Kapitel 3 und 4 zusammengeführt.

Erstellung / Aufbau des Fragebogens

Aufgrund der Erkenntnisse aus den Vorgesprächen (vgl. Kapitel 2.1.2 – bestehender Erklärungsbedarf zum Thema), wurde dem Fragebogen ein längerer Einleitungsteil vorweggestellt, um die Befragten zunächst „abzuholen“. Um Zugang zu möglichst vielen verschiedenen auch technischen Bereiche des Themas zu erhalten, wurde der Sachverhalt und somit die Frageblöcke aufgebrochen in Phasen des Lebenszyklus und nochmal in drei Betrachtungswinkel, i.S.v. Einsatz- und Verantwortungsbereichen. Die Fragen wurden gänzlich offen gestellt und wurden, so wie das Design des gesamten Fragebogens, dahingehend gestaltet,

den Befragten möglichst viele Ansatzpunkte für weitere Überlegungen zu geben. Gleichzeitig wurde gebeten, im Zweifel auch die gemachten Aussagen/Annahmen in Einleitung etc. zu hinterfragen oder zu kritisieren. Ziel war es sowohl die unterschiedlichen Verständnisse aufzudecken, falls vorhanden, wie aber auch eine gewisse Tiefe der Informationen zum Sachverhalt und der Umsetzung zu erreichen. Details, siehe:

→ Anhang 6.5 Kapitel 2.1.3 - Fragebogen

Ergebniszusammenführung

Im Sinne des Kapitels 2.0 „Auswertung des Analyseprozesses “ wurden aufgrund des umfassend zu strukturierenden Informationsgehalts die Erkenntnisse der unterschiedlichen Expertenkonsultationen in den Kapitel 3 und 4 aggregiert und zu einer logischen Gesamtbetrachtung und Gesamtbewertung zusammengeführt. Die Beantwortung der Fragebögen stellte für die Informationsgenerierung und die quantitative und qualitative Bewertung neben den Interviews die wesentliche Grundlage dar.

2.1.3.1 Personen - bei Beantwortung involvierte Personen

Bei der Beantwortung der 18 schriftlich zurückgesandten Fragebögen beteiligten sich folgende 31 Personen (Einzelne Fragebögen wurden zum Teil durch mehrere Personen ausgefüllt.).

| Bereich | Anrede | Titel | Vorname | Name | Organisation |
|-------------|--------|-----------|---------|------|--------------|
| Unternehmen | Herr | | | | |
| Verein | Frau | | | | |
| Unternehmen | Frau | | | | |
| Verbände | Herr | Prof. Dr. | | | |
| Unternehmen | Herr | | | | |
| Forschung | Frau | Prof. Dr. | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Forschung | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Unternehmen | Herr | Dr. | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Frau | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Frau | | | | |
| Unternehmen | Herr | Dr. | | | |
| Plattformen | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Unternehmen | Herr | | | | |
| Forschung | Herr | Prof. Dr. | | | |
| Unternehmen | Herr | Dr. | | | |
| Forschung | Frau | Dr. | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |

Personenbezogene Daten aus Gründen des Datenschutzes hier nicht sichtbar

| Bereich | Anrede | Titel | Vorname | Name | Organisation |
|-------------|--------|-------|---------|------|--------------|
| Verbände | Herr | | | | |
| Unternehmen | Herr | | | | |
| Forschung | Herr | Dr. | | | |

2.1.4 Experten-Interviews

Mit ausgewählten Experten wurden tiefergehende Interviews zum Thema geführt. Hierbei wurden unterschiedliche Experten aus Forschung, Wirtschaft, Unternehmen, Verbänden, Anwender, Lösungsanbieter etc. geführt. Die Interviews waren zwischen einer halben Stunde bis zu 5 Stunden lang. Sie wurden weitestgehend offen geführt und hatten unterschiedliche Schwerpunkte. Es wurden sowohl technische Sachverhalte diskutiert, als auch gemeinsam eruiert, wie ein weiteres Vorgehen aussehen könnte.

Ergebniszusammenführung

Im Sinne des Kapitels 2.0 „Auswertung des Analyseprozesses “ wurden aufgrund des umfassend zu strukturierenden Informationsgehalts die Erkenntnisse der unterschiedlichen Expertenkonsultationen in den Kapitel 3 und 4 aggregiert und zu einer logischen Gesamtbetrachtung und Gesamtbewertung zusammengeführt. Die Experteninterviews stellte für die Informationsgenerierung und die quantitative und qualitative Bewertung neben der Beantwortung der Fragebögen die wesentliche Grundlage dar. Wesentliche Teile der Expertenkonsultation gestalteten sich dahingehend als ein gemeinsames Eruiere / Nachdenken darüber, wie dem Sachverhalt SDI begegnet werden kann. In diesem Sinne sind auch die Ausführungen zur Gestaltung in Kapitel 4 maßgeblich unmittelbar in oder aus der Expertenkonsultation entstanden und Teil der Ergebniszusammenführung.

2.1.4.1 Personen - Interviewpartner

Für tiefergehende Interviews standen zur Verfügung:

| Bereich | Anrede | Titel | Vorname | Name | Organisation |
|-------------|--------|-----------|---------|------|--------------|
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Forschung | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Plattformen | Herr | | | | |
| Behörden | Herr | | | | |
| Forschung | Frau | | | | |
| Unternehmen | Herr | | | | |
| Verbände | Herr | | | | |
| Unternehmen | Herr | | | | |
| Verbände | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Forschung | Herr | Prof. Dr. | | | |

Personenbezogene Daten aus Gründen des Datenschutzes hier nicht sichtbar

| Bereich | Anrede | Titel | Vorname | Name | Organisation |
|-------------|--------|-------|---------|------|--------------|
| Unternehmen | Herr | | | | |
| Verbände | Herr | | | | |
| Verbände | Herr | | | | |
| Forschung | Herr | Dr. | | | |
| Forschung | Herr | Dr. | | | |
| Unternehmen | Herr | Dr. | | | |
| Verbände | Herr | | | | |

2.1.5 Themen-Workshop, 22. Juli 2017 bei DIN

Eines der zentralen Zukunftsvorhaben der deutschen Wirtschaft für dessen Umsetzung SDI Grundvoraussetzung sind, ist das Thema Industrie 4.0. Hier finden sich wesentliche Treiber des Themas SDI bzw. Interoperabilität bringender Strukturen und Lösungen. Zur Analyse und Entwicklung eines möglichen konkreteren Vorgehens für die Industrie 4.0 und einer diesbezüglichen Einbettung und Nutzung desselben für den Gesamtsachverhalt wurde daher ein Workshop umgesetzt/begleitet. Genutzt wurde die Idee aus einem der Vorgespräche „sich mit einer kleinen Gruppe zentraler Player für einen Tag zusammzusetzen, um einen pragmatischen Blueprint für die Industrie 4.0 “ zur weiteren Diskussion zu entwerfen. In den Überlegungen für das weitere Vorgehen wurden bestehende konkrete Projekte eingeladen, mit denen standardisierte Lösungen ggf. unmittelbar in die Anwendung gebracht werden können. In diesem Sinne wurden u.a. die Projekte Plattform Industrie 4.0, der Industrial Data Space und das Projekt IUNO zusammengebracht. Der Austausch fand am 22.06.2017 im Hause DIN statt.

Teilergebnisse mit Einfluss auf den weiteren Analyseprozess und Einflusssschwerpunkte auf die Ergebniszusammenführung

Erkenntnisse aus dem Workshop finden sich in allen Bereichen der Ergebniszusammenführung in Kapitel 3 und 4 wieder. Hierbei sei insbesondere auf das Kapitel 4.19 „Industrie 4.0 – Potential zum Leitmodell “ verwiesen. Die weitere Analyse des Themas und somit auch die Gestaltung weiterer Gespräche war durch das Treffen aber maßgeblich durch die Erkenntnis geprägt, dass es keine einfache Lösung gibt, dass das Thema außerordentlich vielschichtig ist und eine Zusammenarbeit zum Knowhow-Transfer zwingend erforderlich sein wird, aber auch die Bereitschaft vorhanden scheint. Ein „Blueprint “ in dem Sinne war nicht erreichbar, aber ein möglicher Weg / ein beispielhaftes anwendungsbezogenes Lösungskonzept einer zentralen Arbeitsgruppe der späteren Verstetigung. Nach dem Workshop wurde ein Ergebnispapier erarbeitet, welches in Teilen zum Stakeholder-Workshop am 10. Juli 2017 durch Herrn Jochem (AG3 Plattform Industrie 4.0) vorgestellt wurde. Details, siehe anbei:

→ Anhang 6.6 Kapitel 2.1.5 - internes Ergebnispapier Themen-Workshop - 22. Juli 2017

Es ist noch festzuhalten, dass spätere Gespräche mit den Beteiligten zeigten, dass der Workshop auch nur einen Teilbereich des Sachverhaltes adressieren konnte und die Notwendigkeit einer Erweiterung und Differenzierung des Sachverhaltes bleibt. Aus Industrie 4.0 Sicht ist ein sehr breites Spektrum an Anwendungsfällen anzugehen, wodurch Industrie 4.0 auch in der weiteren Gestaltung eine Sonderrolle zukommen kann, wie in Kapitel 4 adressiert. Hierzu ist eine domänenübergreifende Einbindung zwingend.

2.1.5.1 Personen - Teilnehmer

An dem Workshop nahmen, unter Begleitung von Vertretern von DIN und DKE, folgende Personen teil:

| Bereich | Anrede | Titel | Vorname | Name | Organisation |
|-------------|--------|-----------|---------|------|--------------|
| Ministerien | Herr | | | | |
| Forschung | Herr | | | | |
| Behörden | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Forschung | Herr | | | | |
| Plattformen | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Forschung | Herr | Prof. Dr. | | | |
| Unternehmen | Herr | Dr. | | | |

Personenbezogene Daten aus Gründen des Datenschutzes hier nicht sichtbar

2.1.6 Stakeholder-Workshop, 10. Juli 2017 im BMWi

Am 10. Juli 2017 fand auf gemeinsame Einladung von Ministerialdirigent Helge Engelhard, Bundesministerium für Wirtschaft und Energie (BMWi), Herrn Dr. Michael Stephan, Geschäftsführer, Deutsches Institut für Normung e. V. (DIN) und Michael Teigeler, Geschäftsführer, Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE) der Stakeholder-Workshop zur Präsentation der Zwischenergebnisse statt. Eine erste Vorstellung und Diskussion der Zwischenergebnisse der Gesamtbetrachtung aus Expertenkonsultation, sowie Rechts- und Normenrecherche erfolgte. Details, siehe:

- ➔ Anhang 6.7 Kapitel 2.1.6 - Einladungsschreiben (Mail) und Agenda für Stakeholder-Workshop
- ➔ Anhang 6.8 Kapitel 2.1.6 - Präsentation Stakeholder-Workshop – Begrüßung und Allgemein / Normenrecherche / Rechtsrecherche
- ➔ Anhang 6.9 Kapitel 2.1.6 - Zwischenbericht - Zusammenfassung der Diskussion der Zwischenergebnisse

Ergebniszusammenführung

Der aus dem Stakeholder-Workshop hervorgegangene Zwischenbericht ist als erster Schritt zur in Kapitel 2.0 adressierten Strukturierung des umfassenden Informationsgehalts zu einer logischen Gesamtbetrachtung und -bewertung zu verstehen. Die Erkenntnisse finden sich in Kapitel 3, 4 und 5 wieder.

2.1.6.1 Personen - Teilnehmer

Für die Veranstaltung am 10. Juli 2017 hatten sich 70 Teilnehmer angemeldet, anwesend waren:

| Nr. | Anrede | Titel | Vorname | Name | Organisation |
|-----|--------|-------|---------|------|--------------|
| 1. | Herr | | | | |
| 2. | Herr | | | | |
| 3. | Herr | | | | |
| 4. | Herr | | | | |

| Nr. | Anrede | Titel | Vorname | Name | Organisation |
|-----|--------|-----------|---------|------|--------------|
| 5. | Frau | | | | |
| 6. | Herr | Dr. | | | |
| 7. | Herr | Dr. | | | |
| 8. | Herr | | | | |
| 9. | Frau | | | | |
| 10. | Herr | | | | |
| 11. | Frau | | | | |
| 12. | Herr | | | | |
| 13. | Herr | | | | |
| 14. | Herr | | | | |
| 15. | Herr | | | | |
| 16. | Herr | | | | |
| 17. | Herr | Dr. | | | |
| 18. | Herr | Dr. | | | |
| 19. | Herr | | | | |
| 20. | Frau | Dr. | | | |
| 21. | Herr | | | | |
| 22. | Herr | | | | |
| 23. | Herr | | | | |
| 24. | Herr | Dr. | | | |
| 25. | Frau | | | | |
| 26. | Herr | | | | |
| 27. | Frau | | | | |
| 28. | Herr | | | | |
| 29. | Herr | | | | |
| 30. | Herr | | | | |
| 31. | Herr | | | | |
| 32. | Herr | Dr. | | | |
| 33. | Herr | | | | |
| 34. | Herr | Dr. | | | |
| 35. | Herr | | | | |
| 36. | Herr | | | | |
| 37. | Herr | | | | |
| 38. | Herr | Dr. | | | |
| 39. | Herr | | | | |
| 40. | Herr | Dr. | | | |
| 41. | Herr | | | | |
| 42. | Herr | | | | |
| 43. | Herr | | | | |
| 44. | Herr | Prof. Dr. | | | |
| 45. | Herr | Dr. | | | |
| 46. | Herr | | | | |
| 47. | Herr | | | | |
| 48. | Herr | | | | |
| 49. | Herr | | | | |
| 50. | Herr | | | | |
| 51. | Frau | | | | |
| 52. | Herr | Dr. | | | |
| 53. | Herr | | | | |
| 54. | Herr | | | | |

Personenbezogene Daten aus Gründen des Datenschutzes hier nicht sichtbar

| Nr. | Anrede | Titel | Vorname | Name | Organisation |
|-----|--------|-------|---------|------|--------------|
| 55. | Herr | | | | |
| 56. | Herr | | | | |
| 57. | Herr | | | | |
| 58. | Herr | Dr. | | | |
| 59. | Herr | Dr. | | | |
| 60. | Herr | | | | |
| 61. | Herr | | | | |
| 62. | Herr | Dr, | | | |
| 63. | Herr | | | | |

Angemeldet jedoch kurzfristig verhindert waren:

| Bereich | Anrede | Titel | Vorname | Name | Organisation |
|---------|--------|-------|---------|------|--------------|
| - | Herr | Dr. | | | |
| - | Herr | | | | |
| - | Herr | | | | |
| - | Herr | | | | |
| - | Frau | | | | |
| - | Herr | | | | |
| - | Herr | | | | |

2.1.7 Zwischen- und Folgegespräche / Kontakte etc.

Die Zwischen- und Folgegespräche / Kontakte sind wie die Vorgespräche hier separat von den Interviews aufgeführt, da sie nicht den intendierten Charakter zur umfassenden Informationsgewinnung hatten. Es sind nur Kontakte aufgeführt, die eine Informationserweiterung bedeuteten. Sie entstanden im Rahmen des Projektes in unterschiedlichen Situationen, bspw. bei der Vorstellung des Projektes in Gremien, bei der Auslotung möglicher und Einleitung von zukünftiger Zusammenarbeit zum Thema, bei der öffentlichen Kommunikation des Projektes, bei Interaktionen auf Veranstaltungen und Messen, bei der Teilnahme an Podiumsdiskussionen etc. Es handelt sich zudem auch um Personen, bei denen eine tiefergehende Konsultation beabsichtigt, aber zeitlich nicht einzurichten war oder eben im Rahmen des Projektes nicht mehr möglich war und somit über den Erstkontakt nicht hinaus kam. Mit mehreren Interviewpartnern aus Kapitel 2.1.4 wurden ebenfalls Zwischen- und Folgegespräche geführt. Diese Kontakte sind aber nicht wiederholt aufgeführt, sondern wurden im Sinne des Kapitels 2.0 mit denen der Experteninterviews zusammengeführt.

Ergebniszusammenführung

Die Kontakte lieferten zum Teil nur einzelne Aspekte oder Argumente (die aber entweder Berücksichtigung im Sinne der Gewichtung des Gesamtbildes erfahren sollen oder das Gesamtbild klar erweiterten), teilweise aber auch umfassende / maßgebliche Informationen für die Analyse des Themas. Im Sinne des Kapitels 2.0 „Auswertung des Analyseprozesses“ wurden aufgrund des umfassend zu strukturierenden Informationsgehalts die Erkenntnisse der unterschiedlichen Expertenkonsultationen in den Kapitel 3 und 4 aggregiert und zu einer logischen Gesamtbetrachtung und Gesamtbewertung zusammengeführt. Die

Experteninterviews stellte für die Informationsgenerierung und die quantitative und qualitative Bewertung neben der Beantwortung der Fragebögen die wesentliche Grundlage dar.

2.1.7.1 Personen - Gesprächspartner

| Bereich | Anrede | Titel | Vorname | Name | Organisation |
|-------------|--------|-----------|---------|------|--------------|
| Plattformen | Herr | Dr.-Ing. | | | |
| Unternehmen | Herr | Prof. Dr. | | | |
| Verbände | Herr | | | | |
| Unternehmen | Herr | | | | |
| Behörden | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Unternehmen | Frau | | | | |
| Unternehmen | Herr | Dr. | | | |
| Forschung | Herr | Prof. Dr. | | | |
| Unternehmen | Herr | Dr. | | | |
| Verbände | Herr | | | | |
| Verbände | Herr | | | | |
| Forschung | Herr | Prof. Dr. | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Verbände | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Unternehmen | Herr | | | | |
| Verbände | Herr | | | | |

Personenbezogene Daten aus Gründen des Datenschutzes hier nicht sichtbar

2.2 Recherche allgemein

2.2.1 Initiativen / Aktivitäten / Gremien / Akteure

Digitale Identitäten sind ein Grundlagenthema der Digitalisierung. Wie in Kapitel 3 und 4 noch näher erläutert, ist die Frage nach Sicheren Digitalen Identitäten dabei davon bestimmt, für wen was für eine Art Sicherheit geschaffen werden soll. Zudem besteht das Thema SDI aus unterschiedlichsten Unterbereichen bzw. Dimensionen, die Lösungen bedürfen (siehe hierzu explizit das Kapitel 3). Diese werden aber durchaus einzeln angegangen und das macht auch in diesem Bericht herausgearbeitete Komplexität des Sachverhalts und der Marktsituation aus, denn nur durch das Zusammenfügen der Unterbereiche / Dimensionen entstehen Sichere Digitale Identitäten.

In diesem Sinne werden Aktivitäten, die das Thema betreffen oder nach Ansicht von Experten behandeln, oftmals nicht so genannt bzw. so verstanden. Unter anderem in Kapitel 4.7 und 4.8 wird dargelegt, dass im Prinzip jegliches Digitalisierungsprojekt, sich mit dem Thema Digitale Identitäten beschäftigt und je nach der erwünschten Sicherheit dies gestaltet. Es gibt somit deutlich weniger unmittelbare als mittelbare Initiativen / Projekte, die sich mit dem Thema beschäftigen. Eine vollständige Aufstellung mit dem Thema zusammenhängender Aktivitäten, Gremien oder Initiativen ist in dem Sinne nicht durchführbar.

In diesem Sinne erklärt es auch dass im Rahmen des Fragebogens auf die Frage „Welche Initiativen, Aktivitäten und/oder Forschungsvorhaben zu dem Thema „Sicherer Digitale Identitäten “ kennen Sie? “ Antworten gegeben wurden, die unterschiedlich mit dem Thema verbundene Aktivitäten adressierten, so auch Akteure und Gremien.

- AIM-D e. V.
- AISEC Fraunhofer Institut
- ALESSIO
- APOLI
- ASMONIA
- BITKOM e. V. (hier bspw. AK Sicherheitsmanagement und AK Cyber Physical Systems)
- Bundesversicherungsanstalt - Eckpunkte für die Sicherung von Online-Portalen
- DIN / DIN FOCUS.ICT
- DIPP / Verimi
- DKE
- eCI@ss
- eIDAS
- eID-Funktion / Personalausweis
- Elektronische Gesundheitskarte (GEMATIK)
- e-SENS
- FIDO Alliance
- FutureID (u.a. Fraunhofer IAO)
- Hasso-Plattner-Institut für Softwaresystemtechnik GmbH
- HPI Identity Leak Checker
- ID Kompass, Portal für digitale Identität
- IEC - SyC Smart Cities
- IEC - SyC Smart Energy
- IEC SyC AAL
- IEC TC57 WG 15
- IETF SACM-WG und ACE-WG

- IETF- Trusted Computing Group TCG
- Industrial Data Space (und dessen Ausbaustufen)
- Industrial Internet Consortium (IIC)
- Innovationscluster Next Generation ID der Fraunhofer-Gesellschaft
- ISO TC 292 WG 4
- ISO/IEC 24760 - Identity management framework
- ISO/IEC 29003 - Identity proofing, in Arbeit
- ISO/IEC 29115 - Entity authentication assurance framework
- ISO/IEC 29146 - Access management framework, in Arbeit
- ISO/IEC SC 27
- IUNO (BMBF-Förderprojekt)
- Kantara Initiative
- KOIDA - Kompetenzzentrum Objektidentifikation und Authentisierung
- KRITIS
- Lehrstuhl „Secure Identity “ an der FU Berlin (Stiftungsprofessur)
- Messe OMNICARD / Konferenz OMNISECURE
- Network Working Group - Vectors of Trust
- OpenID Foundation
- PARADISE
- Personalausweis / eID-Funktion
- Plattform Industrie 4.0 / AG3 „ERGEBNISPAPIER - Technischer Überblick: Sichere Identitäten “ / OAG Sichere Identitäten
- PSD2/RTS
- ISO/IEC 29191 - Requirements for partially anonymous, partially unlinkable authentication
- SecurityLab AISEC München
- Security-Labs von Bundesdruckerei und Fraunhofer-Instituten
- SIBASE
- STORK / STORK 2.0
- Taskforce "Geräteidentität und -integrität im Internet der Dinge" (VDE)
- TeleTrusT (Vorgehensweise für PKI-Bridge-Modell / Cross-Zertifizierung von TrustCentern)
- Trusted Computing Group
- VDA - Verband der Automobilindustrie e. V. (AKA Daten)
- VDE (Task Force Trusted Computing / zertifiziert SmartHome Komponenten)
- VDMA - Verband Deutscher Maschinen- und Anlagenbau e. V.
- Verein Sichere Identität Berlin-Brandenburg
- World e-ID and Cybersecurity
- Zukunftsprojekte der Hightech-Strategie (HTS-Aktionsplan) 2012 der Bundesregierung Inhalte (7) Nachhaltige Mobilität, (8) Internetbasierte Dienste für die Wirtschaft, (9) Industrie 4.0, (10) Sichere Identitäten
- ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.

Im Rahmen der Expertengespräche (z.T. Nachgespräche daher in Teilen unberücksichtigt) sind zu sinngemäßen Fragen folgende Nennungen zu ergänzen:

- BMEcat
- CEN BII (1-3)- Business Interoperability Infrastructure für das E-Procurement
- CEN TC440 - Entwicklung des neuen ED-Procurement Standards
- Common Criteria
- DELTA - Projekt "Datensicherheit und -integrität in der Elektromobilität beim Laden und eichrechtkonformen Abrechnen (DELTA)"
- DigiConnect (Referat Cybersicherheit) stellt Konzept von Digital Enablement vor
- Digitales Typenschild (DIN 66277)
- EIF - European Interoperability Framework
- EIRA - European Interoperability Reference Architecture

- elektronische Fallakte
- EMVCO (Standardisierungsorganisation von Kreditkartenunternehmen)
- ENISA ("Ernsip-Report" für Certification von Security von IIC für Kritis)
- GS1 Verbund (u.a. Global Unique Identifiers; Smart Search; Plagiatschutz e.g. Serialization and Product Verification; Traceability; fTRACE)
- HASELNUSS - Projekt "Hardwarebasierte Sicherheitsplattform für Eisenbahn-Leit- und Sicherungstechnik"
- IKOPA - Projekt "Integrated cooperating platform for automated electric vehicles"
- ISAEN
- ISO 20078, 20077, 20080, 26262 Functional Safety (betroffen von DI)
- ISO/IEC 11889 (TPM)
- ISO/IEC 82304 "Health Software, General Requirements for Software Safety"
- IT-Gipfel / Digitaler Gipfel - Fokusgruppe Sichere Mobile Identität
- ITU-T
- Netzconnector Gesundheitswesen
- NIST - National Institute of Standards and Technology
- OPCUA
- openAAS (Projekt)
- OpenPGP-Format IETF RFC 2440 und 4880
- PEPPOL - Technische Infrastrukturen für ein sicheres EU-weites E-Procurement
- RFID
- SAMPL (secure additive manufacturing plattform) (Projekt)
- Smart Meter Gateway
- SWID / COSWID
- SWIFT Netz
- Web of Trust

2.3 Recherche Normung

2.3.1 Grundlage der Rechercharbeit

Die Problemstellung der Normenrecherche ist sehr komplex, da zum Zeitpunkt der Recherche 447580 Normen und Standards¹ weltweit zu Grunde liegen und nicht alle Normen sowie Standards sich mit dem Thema Sichere Digitale Identitäten befassen.

Bei der Recherche wurde 1300 Normen, Richtlinien und Standards identifiziert die das Thema „sichere digitale Identitäten “ direkt oder indirekt beinhalten.

Dabei wurden Organisationen ermittelt die beim Thema sichere digitale Identitäten eine Schlüsselfunktion einnehmen können. Die Abbildung 5 gibt hierbei eine Übersicht in welchen Organisationen das Thema aktuell in Arbeitskreisen thematisiert wird. Dabei kam zum Vorschein, dass viele Normen- und Standardisierungsarbeiten im internationalen Bereich entwickelt werden.

Die Ermittlung der relevanten Normen, Standards und Richtlinien fand im ersten Schritt durch eine Volltextsuche mit der Kombinationen von folgenden Schlagworten wie „sichere digitale Identitäten “; „sichere Identitäten “ und „digitale Identitäten “ in der zur Verfügung stehenden Normendatenbanken, wie zum Beispiel die DITR Datenbank des Deutsches Informationszentrum für technische Regeln (DITR)² und VDE Normenbibliothek³, statt.

Die dabei ermittelten Dokumente wurden ungefiltert zu einer Gesamtübersicht zusammengestellt. Im nächsten Schritt wurde eine Prüfung hinsichtlich der Relevanz für das Thema „Sichere Digitale Identitäten “ durchgeführt. Abbildung 4 veranschaulicht hierbei den Entscheidungsprozess und damit die Priorisierung von relevanten Normen. Dabei wurden 188 Normen, Standards und Richtlinien als relevant eingestuft.⁴

¹ DITR-Datenbankstatistik – Juli 2017, DIN-Mitteilungen August 2017

² <https://www.beuth.de/kampagne/nm-de/unsere-produkte/software-loesungen/ditr-datenservice>

³ <https://www.normenbibliothek.de>

⁴ Anhang 6.10

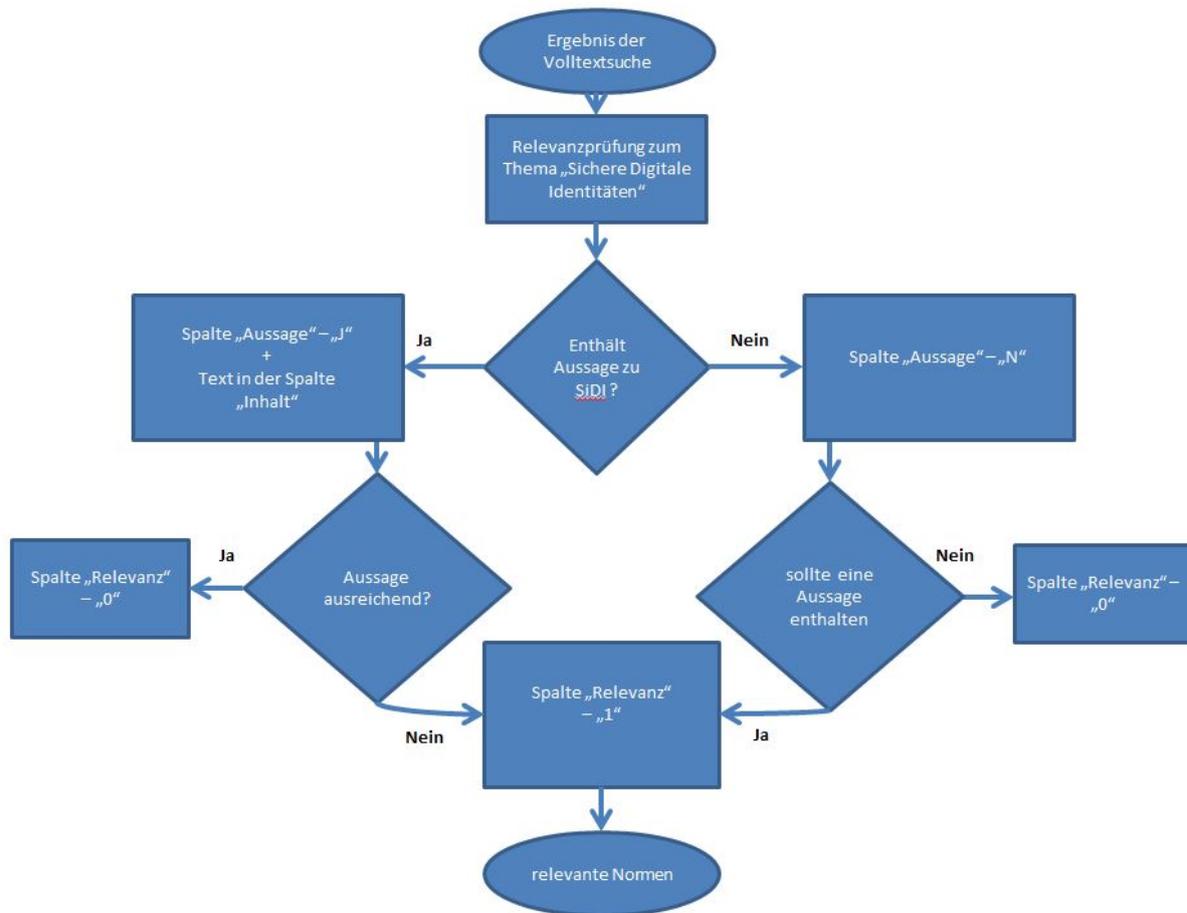


Abbildung 4 – Entscheidungsdiagramm für die Normenrecherche (Quelle: DKE)

Anschließend wurden die zuständigen Normungsreferenten und Projektmanager der als relevant eingestuft Normen zu einer kurzen Einschätzung der Bedeutung der Norm für das Thema „Sichere Digitale Identitäten “ zu Rate gezogen.

Im Kapitel 2.3.3 wird auf die wichtigsten Normen und Standards eingegangen, die auch durch Fachexperten als elementare Dokumente bestätigt wurden.

2.3.2 Relevante Organisationen im Normungs- und Standardisierungsumfeld

Die ermittelten 188 relevanten Normen, Standards und Richtlinien sind in verschiedenen nationalen und internationalen Normungs- und Standardisierungsorganisationen und Konsortien erarbeitet worden. Abbildung 5 zeigt eine Übersicht der betrachteten Organisationen. In den folgenden Unterkapiteln sind diese mit ihrem Arbeitsschwerpunkt kurz erläutert.

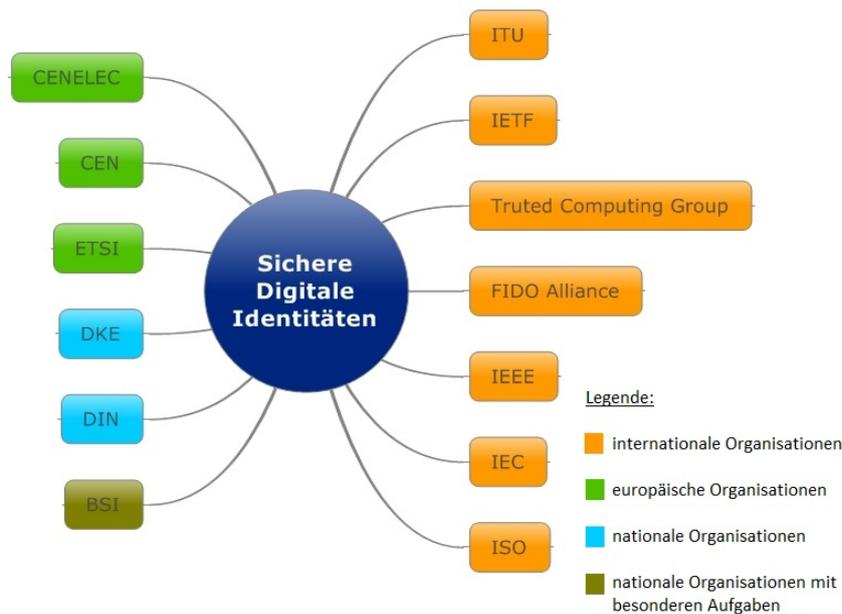


Abbildung 5 – Übersicht der betrachteten Organisationen

Ein Beispiel für eine internationale Organisation ist die Trusted Computing Group⁵ (siehe Kapitel 2.3.2.6), in der bisher 40 Spezifikationen sowie Whitepaper verabschiedet und veröffentlicht wurden. Diese Dokumente wurden in den Arbeitsgruppen „Trusted Platform Module (TPM) Specifications“; „TPM Software Stack (TSS) Specifications“; „Infrastructure Specifications“; „Server Specifications für vertrauenswürdige Computer-Server“ und „Trusted Network Connect (TNC) Specifications“ erarbeitet.

2.3.2.1 ISO – CEN – DIN

Die International Organization for Standardization, kurz ISO⁶, ist die größte internationale Normungsorganisation mit Sitz in Genf, Schweiz. Seit ihrer Gründung im Jahr 1947 hat sie mehr als 21000 internationale Standards und Dokumente veröffentlicht. Die Standards behandeln verschiedenste Themen, von Technik über Lebensmittelsicherheit bis hin zu Landwirtschaft und Gesundheitswesen. Die ISO zählt 162 nationale Normungsorganisationen zu ihren Mitgliedern. Jedes Land kann genau eine ISO-Mitgliedschaft eingehen. In Deutschland repräsentiert das Deutsche Institut für Normung e. V. DIN⁷ diese internationale Normungsorganisation. Auf der europäischen Ebene arbeitet ISO vor allem mit dem European Committee for Standardization (CEN⁸) zusammen. Grundlage hierfür ist das Vienna Agreement aus dem Jahr 1991. Es verhindert Doppelarbeit an Normungsprojekten und ermöglicht die parallele Annahme von internationalen und europäischen Normen.

⁵ <https://trustedcomputinggroup.org>

⁶ <https://www.iso.org>

⁷ <https://www.din.de>

⁸ <https://www.cen.eu>

2.3.2.2 IEC – CENELEC – DKE

Für die Entwicklung von elektrotechnischen Standards auf internationaler Ebene ist die International Electrotechnical Commission, kurz IEC⁹, verantwortlich. Sie wurde 1906 gegründet und hat ihren Sitz in Genf, Schweiz. Ihre Mitglieder setzen sich aus den nationalen elektrotechnischen Komitees zusammen. Für Deutschland ist dies die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, kurz DKE¹⁰. Die europäische Normungsorganisation European Committee for Electrotechnical Standardization (CENELEC¹¹) arbeitet eng mit der IEC zusammen. CENELEC ist für die europäische Normung im Bereich Elektrotechnik zuständig. Das Frankfurt Agreement zwischen IEC und CENELEC regelt unter anderem, dass alle CENELEC-Mitglieder eine internationale Norm, die als europäische Norm übernommen wurde, auch als nationale Norm umsetzen müssen. Widersprechen nationale Normen der neuen Norm, müssen diese zurückgezogen werden.

2.3.2.3 ITU

Die International Telecommunication Union, kurz ITU¹², ist eine Organisation der Vereinten Nationen mit Sitz in Genf. Sie basiert auf der Kooperation von Staaten und Privatwirtschaft. So sind nicht nur 193 Länder Mitglied der ITU, sondern auch nahezu 800 Unternehmen. In der Abteilung Telecommunication Standardization Sector entstehen pro Jahr circa 150 Standards (sogenannte Recommendations). Sie beinhalten unter anderem Regelungen für das Internet, für Datenprotokolle oder für Videokomprimierung und für unzählige weitere Aspekte der Informations- und Kommunikationstechnik. Bekannt sind zum Beispiel die Recommendation T.81 für die JPEG-Bildkompression oder E.164 für das internationale Telefonnummernschema.

2.3.2.4 ETSI

Das European Telecommunications Standards Institute, kurz ETSI¹³, ist neben CEN und CENELEC die dritte offizielle Normungsorganisation in Europa. Sie hat ihren Sitz in Sophia Antipolis, Frankreich. Die gemeinnützige Organisation ist von der Europäischen Union als europäische Normungsorganisation anerkannt und für Normen im Bereich der Informations- und Kommunikationstechnologien zuständig. ETSI verfolgt darüber hinaus das Ziel, weltweit anerkannte und anwendbare Standards zu entwickeln. Im Vergleich zu ISO/CEN bzw. IEC/CENELEC gibt es bei ETSI kein nationales Delegationsprinzip und Firmen können direkt Mitglied werden. Von ETSI erstellte europäische Normen werden durch Kommentierung und Abstimmung nationaler Komitees übernommen.

2.3.2.5 BSI

Die Standards des Bundesamts für Sicherheit in der Informationstechnik, kurz BSI¹⁴, enthalten Empfehlungen und Anforderungen zur Informationssicherheit für Behörden oder Unternehmen. Das BSI

⁹ <http://www.iec.ch>

¹⁰ <https://www.dke.de>

¹¹ <https://www.cenelec.eu>

¹² <https://www.itu.int>

¹³ <http://www.etsi.org>

¹⁴ <https://www.bsi.bund.de>

hat seinen Sitz in Bonn und ist dem Bundesinnenministerium unterstellt. Die technischen Richtlinien des BSI (BSI-TR) ergänzen sowohl die technischen Prüfvorschriften des BSI als auch bestehende Normen und Standards. Sie liefern Kriterien und Methoden zur Konformitätsprüfung sowohl der Interoperabilität von IT-Sicherheitskomponenten als auch der umgesetzten IT-Sicherheitsanforderungen.

2.3.2.6 TCG

Die Trusted Computing Group, kurz TCG¹⁵, ist eine international tätige, gemeinnützige Organisation, die 2003 als Nachfolger der Trusted Computing Platform Alliance (TCPA) gegründet wurde. Sie hat ihren Sitz in Beaverton, USA. Zu ihren mehr als 100 Mitgliedern zählen Hersteller von Computersystemen und -komponenten, Softwareentwickler sowie Netzwerk- und Infrastruktursystemfirmen. Die TCG entwickelt und fördert offene Spezifikationen für vertrauenswürdigen Computing.

2.3.2.7 IETF

Die Internet Engineering Task Force, kurz IETF¹⁶, beschäftigt sich mit der Weiterentwicklung der Internetarchitektur und dem reibungslosen Funktionieren des Internets. Die IETF ist ein international tätiger, gemeinnütziger und freier Zusammenschluss von Interessenten mit Sitz in Fremont, USA. Die Teilnahme an Arbeitsgruppen ist für alle Interessierten möglich. An den dreimal jährlich stattfindenden Treffen nehmen circa 1.500 Personen teil. Die IETF erarbeitet und veröffentlicht sogenannte RFCs (Request For Comments).

2.3.2.8 IEEE

Das Institute of Electrical and Electronics Engineers, kurz IEEE¹⁷, ist ein internationaler, gemeinnütziger Verband für Ingenieure, Wissenschaftler und technische Berufe und hat seinen Sitz in New York, USA. Mit über 423.000 Mitgliedern in über 160 Ländern stellt er weltweit den größten Berufsverband dar. Die IEEE Standards Association (IEEE-SA) hat ein Portfolio von fast 1.300 Industriestandards, zu denen auch sehr bekannte Standards zählen wie zum Beispiel Wireless LAN und Ethernet. Zusätzlich werden zurzeit über 600 Standards entwickelt.

2.3.2.9 FIDO Alliance

Die gemeinnützige FIDO (Fast IDentity Online) Alliance¹⁸ entwickelt seit 2013 offene Industriestandards zur sicheren Authentifizierung im Internet. Das markenrechtlich geschützte Logo FIDO ready kennzeichnet Produkte, die nach FIDO Standards zertifiziert wurden. Der schnell wachsenden FIDO Alliance gehören inzwischen mehr als 250 Unternehmen und Organisationen an.

¹⁵ <https://trustedcomputinggroup.org>

¹⁶ <https://www.ietf.org/>

¹⁷ <https://www.ieee.org>

¹⁸ <https://fidoalliance.org>

2.3.3 Umfassende Ergebnisse

Grundlegend können Dokumente zur Sicherheit nach IEC Guide 120 in fünf Kategorien eingeordnet werden¹⁹:

- Base security standard
- Group security publication
- Product security publication
- Guidance security publication
- Test security publication

Diese Kategorisierung der Dokumente wird in der Abbildung 6 veranschaulicht und im weiteren Text näher erläutert.

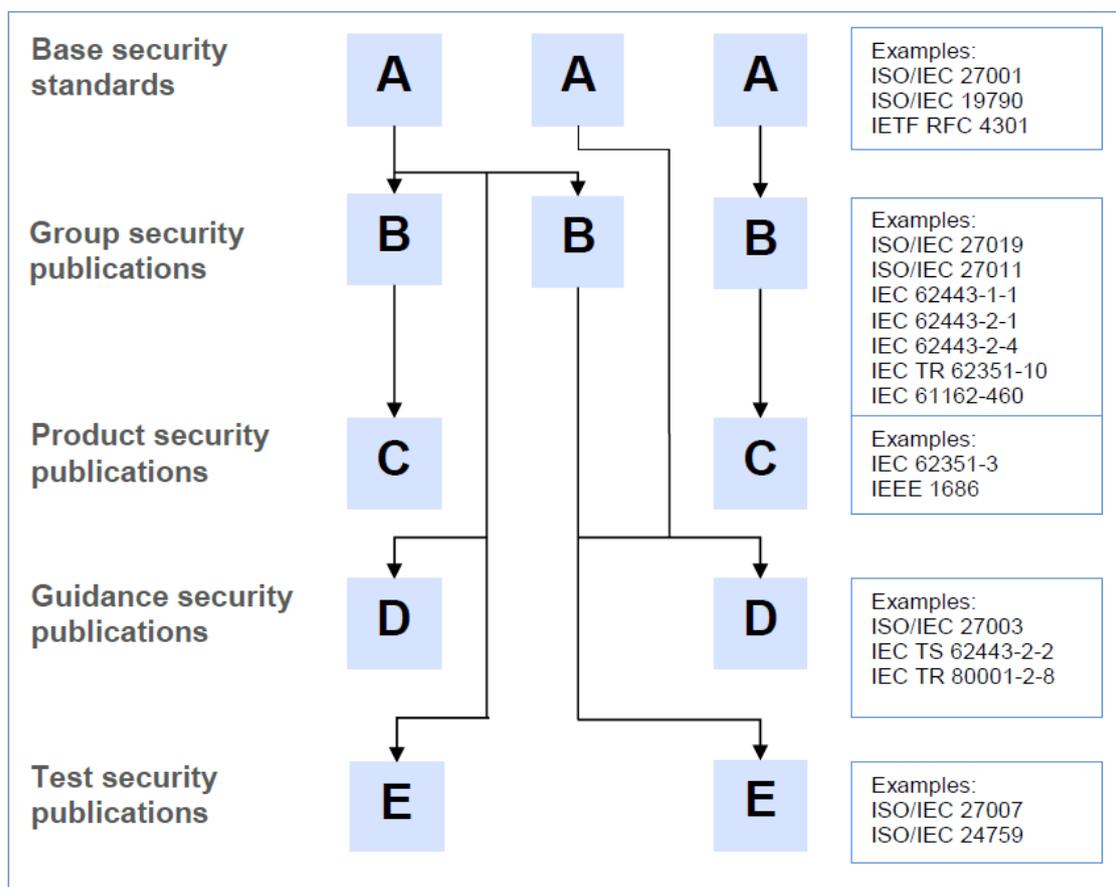


Abbildung 6 – Publikationsarten (Quelle: IEC Guide 120)

Base security standards (Kategorie A) sind Veröffentlichungen, die einen allgemeinen Aspekt der Sicherheit definieren. Diese Sicherheitspublikationen befassen sich mit grundlegenden Konzepten, Prinzipien und Anforderungen hinsichtlich allgemeiner Sicherheitsaspekte, die für eine breite Palette von Produkten und Systemen gelten.

¹⁹ Draft Guide 120 Edition 1, Security aspects – Guidelines for their inclusion in standards

Group security publications (Kategorie B) legen Sicherheitsanforderungen in der jeweiligen Anwendungsdomäne fest. Zu diesem Zweck können diese Dokumente grundlegende Sicherheitsstandards referenzieren oder anpassen. Group security publications können auf viele Produkte oder Systeme oder auf Produkt- sowie Systemfamilien anwendbar sein. Group security publications werden auch als sektorspezifische Sicherheitspublikationen bezeichnet.

Product security publications (Kategorie C) definieren wie base security standards oder group security publications für einen bestimmten Produkttyp angewendet werden können. Sie legen fest wie verschiedene Produkte sicher miteinander interagieren können und wie sie einheitlich gesteuert und verwaltet werden können. Daher sollten product security publications so weit wie mögliche ihre Anforderungen unter Bezugnahme auf base security standards und group security publications definieren.

Guidance security publications (Kategorie D) sollten keine Anforderungen enthalten. Sie erläutern, wie base security standards und group security publications oder product security publications umgesetzt werden können. In einigen Fällen werden guidance security publications nicht verwendet. Stattdessen werden die notwendigen Leitlinien durch informative Anhänge innerhalb des relevanten Anforderungsstandards bereitgestellt.

Test security publications (Kategorie E) definieren Möglichkeiten, um festzustellen, ob die Anforderungen von basis security standards und group security- oder product security publications korrekt implementiert wurden. Test security publications haben typischerweise eine spezialisierte Zielgruppe. Sie können Referenzimplementierungen definieren oder identifizieren, die verwendet werden können, um die korrekte Implementierung durch erfolgreiche Interoperation zu bestimmen.

Die Normen und Standards der nachfolgenden Unterkapitel sind die bestehende Grundlage für eine sichere Kommunikation und legen somit auch die Basis für weitere Normenarbeiten zu sicheren digitalen Identität. Einen Grundsteinbaustein der Informationssicherheit bildet die Common Criteria for Information Technology Security und wird im Kapitel 2.3.3.6. inhaltlich beschrieben.

Die grundlegenden Standards im Bereich der Kommunikation der ITU werden in den Kapiteln 2.3.3.1 und 2.3.3.2 näher betrachtet. Dabei werden die wesentlichen Inhalte der ITU-T X.509 und ITU-T X.1252 vorgestellt. Die Norm DIN EN 419211 Teil 1 beschreibt den Lebenszyklus eines digitalen Signaturverfahrens und damit ein weiterer Baustein im Bereich der sicheren digitalen Identität. Die ISO/IEC 29115:2013 beschreibt die Anforderungsstufen für eine sichere digitale Kommunikation zwischen zwei oder mehreren Kommunikationsteilnehmern. Wie die Kommunikation mit zwei oder vielen Teilnehmern abläuft, wird in der ISO/IEC 24760-3:2016(E) erläutert. Im Kapitel 2.3.3.7. wird die Normenreihe IEC 62443 vorgestellt, die für den industriellen Bereich eine Grundnorm für die sichere Kommunikation auch hinsichtlich der sicheren digitalen Identität darstellt.

Die nachfolgende Tabelle gibt eine Übersicht in welcher Organisation die relevantesten Normen und Standards durch die jeweiligen Gremien bearbeitet werden.

Einen Gesamtüberblick aller relevanten Gremienarbeiten erhält man bei der Betrachtung der im Anhang beigefügten Mindmap „Gremien“²⁰.

²⁰ Anhang 6.10

| Organization | Scope | Normen |
|---|---|--|
| ISO/IEC JTC 1 Information technology | Das Gemeinschaftskomitee von ISO und IEC entwickelt Standards für Informations- und Kommunikationstechnologien (IKT). In 21 Sub-Komitees und mehreren Working Groups bearbeitet das Komitee zurzeit 600 Standards. ISO/IEC JTC 1 hat insgesamt über 3000 Standards veröffentlicht. | ISO/IEC 24760 ISO/IEC 29115 ISO/IEC 15408 ISO/IEC 29003 ISO/IEC 29146 ISO/IEC 29191 |
| CEN TC 244 Persönliche Identifikation, elektronische Signatur, maschinenlesbare Karten sowie zugehörige Geräteschnittstellen und Verfahren | CEN TC 244 entwickelt u. a. Normen, die Schutzprofile für sichere Signaturerstellungseinheiten festlegen. Enthalten sind dort auch die Zertifikatserzeugung und Signaturerstellung. | DIN EN 419211 |
| IEC TC 65 Industrial-process measurement, control and automation | IEC TC 65 entwickelt Standards für Systeme und Komponenten der industriellen Prozesssteuerung inklusive der eingesetzten Software. Dies schließt sowohl die funktionale Sicherheit als auch die IT-Security mit ein. | IEC 62443 |
| ITU-T Study Group 17 Standardization of "Security" | Arbeitet um Vertrauen und Sicherheit im Umgang mit Informations- und Kommunikationstechnik (IKT) zu erhöhen und fördert die Verbreitung von sicheren Netzwerkstrukturen, Services und Anwendungen. Über 170 Standards (ITU-T Empfehlungen und Anhänge) mit dem Fokus auf Sicherheit wurden bisher veröffentlicht. | ITU-T X.509 |
| ITU-T | | ITU-T X.1252 |

Tabelle 1 – Gremien

2.3.3.1 ITU-T X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

In der ITU-T X.509 werden im Allgemeinen digitale Signaturen und dessen Verwendung innerhalb von PKI (Public Key Infrastructure) und PMI (Privilege Management Infrastructure) betrachtet. Dabei werden die Voraussetzungen definiert, mit deren Einhaltung Instanzen der PKI- und PMI-spezifischen Datentypen signiert werden können.

Die folgende Abbildung 7 veranschaulicht den Prozess der digitalen Signatur von Instanzen. Dabei werden aus dem privaten Schlüssel (en: Private Key) des Senders und dem öffentlichen Schlüssel (en: Public Key) des Senders durch PKI/PMI-Datentypen (Public-Key-Zertifikate, Attribut-Zertifikate, Sperrlisten usw.) eine digitale Signatur des Senders erzeugt. Anschließend werden die Daten vor der Übertragung hinzugefügt.

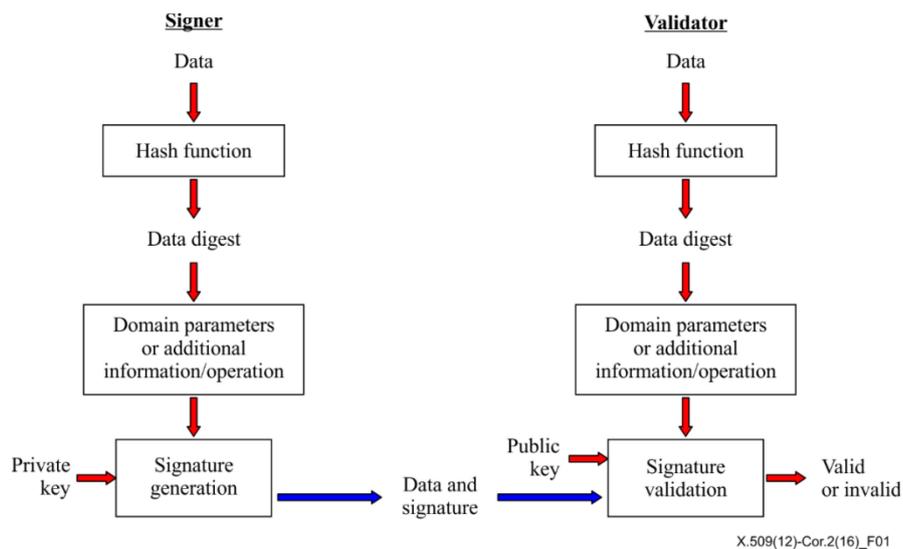


Abbildung 7 – Digitale Signaturgenerierung und Validierung (Quelle: ITU-T X.509)

Der Unterzeichner (en: Signer) in der Rolle des Senders erstellt eine sichere digitale Signatur (en: Hash-Digest) indem er den Hash-Wert mit dem privaten Schlüssel verschlüsselt. Der Hash-Digest kann um zusätzliche Informationen in Vorbereitung für die Erzeugung der digitalen Signatur ergänzt werden, wenn diese zu einer verbesserten Sicherheit führen.

Dieses Ergebnis zusammen mit dem privaten Schlüssel des Unterzeichners und der Verwendung eines Verschlüsselungsalgorithmus führen zu einer Bitfolge, die zusammen mit dem öffentlichen Schlüssel, die digitale Signatur darstellt. Diese wird an die signierten Daten angehängt.

Nach dem Verschicken der Daten an einen Empfänger (Validator) durchlaufen diese dort ein ähnliches Verfahren. Die Vorgehensweise gleicht der in Abbildung 7. Falls die empfangenden Daten unverändert sind, sind die ursprünglichen Daten des Senders das Ergebnis des Verfahrens. Wenn das nicht der Fall ist, wird der „Signature validation“-Schritt fehlschlagen. Das Ergebnis aus dem ersten Schritt zusammen mit dem öffentlichen Schlüssel des Senders, der Bitfolge der Signatur und der Verwendung eines entsprechenden Algorithmus, wertet die digitale Signatur als gültig oder ungültig aus.

Erweist sich die digitale Signatur als gültig, bedeutet dies die Integrität der Daten und die Authentizität des Senders.²¹

2.3.3.2 ITU-T X.1252 Baseline identity management terms and definitions

Die ITU-T X.1252 beschreibt mit dem Begriff der Identität, welcher alle anderen Identitätsmanagementbegriffe bestimmt. In der realen Welt basiert die Identität einer natürlichen Person zwar auf umfangreichen Merkmalen oder einer Vielzahl von Attributen, jedoch aufgrund von persönlichen Ausweisdokumenten ist diese leicht authentifizierbar. Einige von diesen Attributen reichen von körperlichen Merkmale wie das äußere Erscheinungsbild, Verhalten etc. bis hin zu wichtigen Daten der betrachteten Person wie Geburtsdatum, Geburtsort, Heimatadresse oder die Telefonnummer.

²¹ ITU-T X.509 (2012) – Kapitel 6.1 Seiten 9 - 10

In einem Kommunikationsprozess, spielt das Vertrauen eine essentielle Rolle, denn beide Parteien benötigen dieses Vertrauen, um eine sichere Kommunikation zu führen. Dies gilt nicht nur in der realen Welt, sondern insbesondere in der digitalen Welt. Hierbei ist es wichtig sicherzustellen, dass Personen oder Maschinen einerseits auch die sind für die sie sich ausgibt, als auch die sind, die adressiert werden sollen.

Attribute bilden sowohl in der realen Welt als auch in der digitalen Welt eine Identität, jedoch kann in diesem Fall die Identität auf ein einziges Merkmal beschränkt sein, oder viele Merkmale enthalten und hängt somit von dem Kontext ab in dem die Identität erscheint.

In diesem Zusammenhang kann eine Entität eine Anzahl von verschiedenen Identitäten haben, von denen einige eine Untermenge anderer Identitäten sind, wie der Abbildung 8 zu entnehmen ist.²²

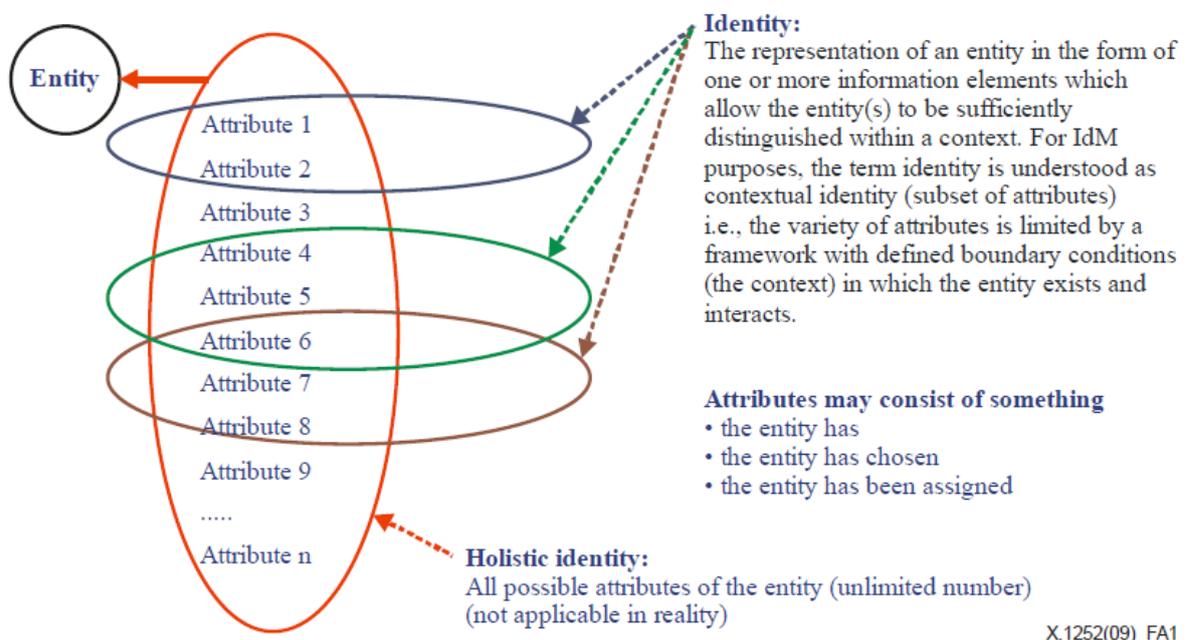


Abbildung 8 – Beziehungen zwischen Entitäten, Identitäten und Attributen (Quelle: ITU-T X.1252)

2.3.3.3 ISO/IEC FDIS 29115 Information technology. Security techniques. Entity authentication assurance framework

Die ISO/IEC FDIS 29115 enthält ein Framework, welches die erforderlichen Anforderungen beschreibt, die eingehalten werden müssen, um eine gewünschte Sicherheitsstufe (en: Level of Assurance, kurz LoA), für jede Phase der sicheren Identitätsauthentifizierung (en: entity authentication assurance framework, kurz EAAF) zu erreichen.

²² ITU-T X.1252 (04/2010), Annex A.1, Seiten 7 und 8

Table 6-1 – Levels of assurance¹

| Level | Description |
|---------------|---|
| 1 – Low | Little or no confidence in the claimed or asserted identity |
| 2 – Medium | Some confidence in the claimed or asserted identity |
| 3 – High | High confidence in the claimed or asserted identity |
| 4 – Very high | Very high confidence in the claimed or asserted identity |

Tabelle 2 – Sicherheitsstufen (Quelle: ISO/IEC FDIS 29115:2012(E))

Sicherheitsstufe 1 (LoA1)

Bei dieser Stufe gibt es ein minimales Vertrauen in die behauptete Identität der Entität. Diese Sicherheitsstufe wird verwendet, wenn mit einer fehlerhaften Authentifizierung ein minimales Risiko verbunden ist. Es gibt keine spezifische Anforderung für den verwendeten Authentifizierungsmechanismus. Diese Sicherheitsstufe erfordert keine Verwendung von kryptographischen Authentifizierungsverfahren.

Sicherheitsstufe 2 (LoA2)

Diese Sicherheitsstufe bietet ein gewisses Maß an Vertrauen in die angenommene Identität des Unternehmens oder der Person. Diese Sicherheitsstufe wird verwendet, wenn ein moderates Risiko mit einer fehlerhaften Authentifizierung verbunden ist. Die Ein-Faktor-Authentifizierung ist eine mögliche Umsetzung. Eine erfolgreiche Authentifizierung ist abhängig von der Entität, das durch ein sicheres Authentifizierungsprotokoll nachgewiesen ist, dass das Unternehmen die Kontrolle über die Berechtigung hat. Die Maßnahmen sollten vorhanden sein, um die Wirksamkeit vor Lauschangriffen oder sogenannter „Online-Guessing-Attacks“ zu reduzieren. Kontrollen sind vorhaben, um vor Angriffen auf gespeicherte Anmeldeinformationen zu schützen.

Sicherheitsstufe 3 (LoA3)

Bei LoA3 besteht ein hohes Vertrauen in die behauptete Identität der Entität. Diese Sicherheitsstufe wird dort verwendet, wo ein erhebliches Risiko mit einer fehlerhaften Authentifizierung verbunden ist. Diese Sicherheitsstufe fordert die Multi-Faktor-Authentifizierung (Multi-Faktor-Authentifizierung nutzt die Kombination von zwei oder mehr Berechtigungsnachweisen für die Prüfung der Identität).

Alle geheimen Informationen, die in Authentifizierungsprotokollen ausgetauscht werden, sind bei der Übertragung und Speicherung kryptographisch geschützt, obwohl diese Sicherheitsstufe nicht die Verwendung eines kryptographischen Protokolls nach dem Aufforderung-Antwort-Verfahren (en: Challenge Response, ein sicheres Authentifizierungsverfahren eines Teilnehmers auf Basis von Wissen) erfordert.

Es bestehen keine Anforderungen an die Erstellung und Speicherung von Anmeldeinformationen, sie können in Personal Computer oder in Spezial-Hardware gespeichert oder generiert werden.

Sicherheitsstufe 4 (LoA4)

Bei der höchsten Sicherheitsstufe gibt es sehr hohes Vertrauen in die behauptete Identität des Unternehmens oder der Person. Diese Sicherheitsstufe wird verwendet, wenn ein hohes Risiko mit einer fehlerhaften Authentifizierung verbunden ist. Diese Stufe bietet die höchste Stufe der Identitätssicherung, die durch die Norm ISO/IEC FDIS 29115:2012(E) definiert wird. Die Sicherheitsstufe 4 ähnelt der Sicherheitsstufe 3, aber diese Stufe fügt die Anforderungen in persönlicher Identitätsnachweise für menschliche Entitäten und die Verwendung von manipulationssicheren Hardware-Geräten für die Speicherung aller geheimen oder privaten kryptografischen Schlüsseln hinzu.

Darüber hinaus sind alle sensiblen Daten, die in den Authentifikationsprotokollen kryptographisch geschützt.²³

2.3.3.4 DIN EN 419211-Teil 1 Schutzprofile für sichere Signaturerstellungseinheiten

In der DIN EN 419211-Teil 1 wird der EVG-Lebenszyklus wie auch die Terminologie definiert.

Der Lebenszyklus des Evaluationsgegenstandes (EVG) unterscheidet die Stufen Entwicklung, Produktion, Vorbereitung und Einsatz. Die Entwicklung und die Produktion des Evaluationsgegenstands bilden zusammen dessen Entwicklungsphase. Diese ist Gegenstand der Common Criteria-Evaluation entsprechend der ALC-Klasse (en: assurance life cycle). Sie endet damit, dass der EVG durch eine sichere Signaturerstellungseinheit (SSEE) (en: secure signature creation device, SSCD) an einen Bereitstellungsdienstleister ausgeliefert wird. Bei dieser Auslieferung muss die funktionale Integrität des EVG geschützt werden.

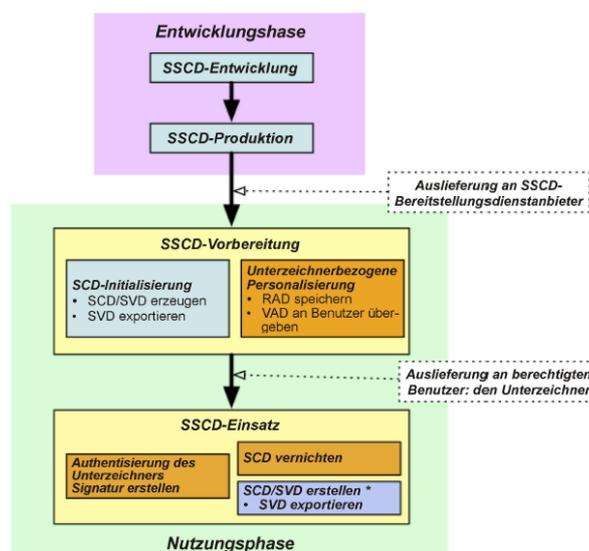


Abbildung 9 – Lebenszyklus des Evaluationsgegenstands (Quelle: DIN EN 419211-1:2014-12)

²³ ISO/IEC FDIS 29115:2012(E), Kapitel 6, Seiten 6 bis 8

Die Einsatzstufe des EVG beginnt, wenn der Unterzeichner die EVG-Operation ausführt, die einen im EVG enthaltenen Signaturschlüssel zur Verwendung bei Signieroperationen aktiviert. Der EVG-Lebenszyklus endet, wenn alle gespeicherten Signaturschlüssel dauerhaft unbrauchbar gemacht wurden. Das Unbrauchbarmachen eines Schlüssels in der sicheren Signaturerstellungseinheit darf das Löschen aller zugehörigen gespeicherten Zertifikatinformationen umfassen.²⁴

2.3.3.5 ISO/IEC 24760 Information technology. Security techniques. A framework for identity management

Identitäts-Föderation (en: identity federations) sind zusammengefasste Identitätsinformationen, die sich über mehrere Systeme erstrecken. Diese Identitäts-Föderation kommt in einer Reihe von Strukturen und Größen vor. Eine einfache Identitäts-Föderation kann eine Mischung aus Akteuren mit unterschiedlichen Rollen haben, wie

- trust framework operator (FO)
- identity information provider (IIP)
- relying party (RP)

Eine Identitäts-Föderation umfasst mindestens zwei Arten von Akteuren, den Identitätsinformationsanbieter (IIP) und die vertrauende Partei (RP). Ein Identitätsinformationsanbieter verwaltet entitätsrelevante Informationen und die vertrauende Partei bietet Dienste für Entitäten an. Die Dienste erfüllen die Richtlinienanforderungen.



Abbildung 10 – zwei Parteien identitäts-Föderation (Quelle: ISO/IEC 24760-3:2016(E))

Das Drei-Parteien-Föderation-Modell findet Anwendung, wenn ein Thema die typische Grundlage eines benutzerorientierten Konsumkontexts bildet. Dieses Föderation-Modell kann aber auch auf vier und fünf Parteien erweitert werden.

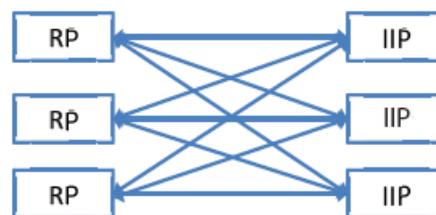


Abbildung 11 – komplexe Identitätsföderation (Quelle: ISO/IEC 24760-3:2016(E))

Viele föderierte Identitäten sind komplexer und beziehen mehrere Akteure ein, um ihre Ziele zu reflektieren, z.B. jene Modelle, die als Speicherarchitektur (en: „Hub-and-Spoke“) bezeichnet werden. Allgemein ist damit gemeint, dass die Verbindung zwischen zwei Endknoten RP und IIP nicht direkt, sondern über einen Zentralknoten Z, die Nabe (en: hub), geführt wird. Die Verbindungen der Endknoten RP, IIP zum Knoten Z bezeichnet man hierbei als Speichen (en: spokes).

²⁴ DIN EN 419211-1:2014-12, Kapitel 6.3, Seiten 12 und 13

Föderationen mit dieser Komplexität und darüber hinaus beginnen, zusätzliche Funktionen zur Unterstützung ihrer Benutzerfreundlichkeit (IIA) bereitzustellen.

Die Rolle des Identitäts-Föderation-Betreibers besteht in der Verwaltung der Angelegenheiten, die sich aus dem Betrieb der Föderation ergeben. Die Rolle kann von einem bestehenden Verbandsmitglied oder einer unabhängigen dritten Partei ausgeführt werden.

Eine Praxis, die für benutzerzentrierte und datenschutzfreundliche Erkennungsprozesse besser geeignet ist, besteht darin, dass der Benutzer im Nachrichtenaustausch zwischen dem RP und dem IIP interagiert, um der Freigabe von Identitätsinformationen durch das IIP explizit zustimmen zu können. Die Föderationen selbst können verschiedene strukturelle Formen annehmen, um ihre Komplexität zu bewältigen. Hub- und Speichenstrukturen wie in der folgenden Abbildung 12 dargestellt, bieten die Vorteile eines zentralen Gateways mit konzentrierter technischer Expertise. Das Gateway hat die Aufgabe, Anonymität, Nicht-Verkettbarkeit und Nicht-Beobachtbarkeit zu verwalten.²⁵

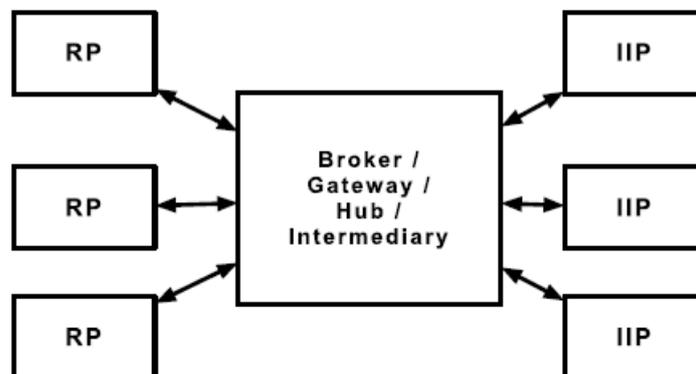


Abbildung 12 – Gateway-Gemeinschaftsmodell (Quelle: ISO/IEC 24760-3:2016(E))

2.3.3.6 ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation

Die Stufen der Vertrauenswürdigkeit (en: Evaluation Assurance Level, EAL) der Common Criteria (ISO/IEC 15408) beschreiben präzise Anforderungen an eine IT-Sicherheitsprüfung. Mit wachsender EAL-Nummer steigen die Anforderungen an den zu prüfenden Umfang, an die Prüftiefe und an die Prüfmethode. Eine niedrigere EAL-Stufe kann vom Prüfumfang als Untermenge des Prüfaufwandes der nächst höheren Stufe angesehen werden. Daher macht das Vorgehen Sinn, mit niedrigeren EAL-Stufen den Evaluierungsprozess zu starten, da so ein erstes verwertbares Prüfergebnis in Form eines Zertifikates mit ausführlichem Report schneller erreicht werden kann.

Darauf aufbauend müssen die nächsten EAL-Stufen "nur noch" den zusätzlichen Prüfaufwand umfassen. Bei EAL4 muss beispielsweise der Quellcode evaluiert werden. Entsprechend hoch ist der Dokumentationsaufwand für das Produkt. Ab EAL5 kommen formale Spezifikations- und Verifikationsmethoden hinzu, denen herkömmliche Entwicklungsmethoden nicht mehr genügen.

²⁵ ISO/IEC 24760-3:2016(E), Kapitel A.2, Seiten 16 und 17

Ziel einer Common Criteria-Evaluierung ist die Bestätigung, dass die vom Hersteller behauptete Sicherheitsfunktionalität wirksam ist. Da die Sicherheitsleistung insbesondere durch die Ausnutzbarkeit vorhandener Schwachstellen unwirksam werden kann, ist bei allen Evaluierungsaspekten die Analyse der Schwachstellen ein zentrales Prüfziel.

Mit wachsenden EAL-Stufen wird erreicht, zunehmend komplexer ausnutzbare Schwachstellen zu entdecken. Wie viel ein EAL4-Zertifikat besser ist als ein EAL2-Zertifikat, kann nur aus dem Zertifizierungsreport ersehen werden. Wenn das Produkt eine nicht zu beseitigende Schwachstelle enthält, kann das zu einer erheblichen Einschränkung seiner Nutzungsmöglichkeiten führen. Beispielsweise könnte eine mit EAL4 nachgewiesene Sicherheitsfunktionalität nur unter Einhaltung massivster Restriktionen an die Nutzung wirksam sein, etwa dadurch, dass durch einzuhaltende Auflagen an den Betrieb des Produktes jegliche Angriffsmöglichkeit auf ein Netzwerk auszuschalten ist und so eine vorhandene Schwachstelle nicht mehr ausnutzbar wird. Wer das Produkt trotzdem anders betreibt, weiß immerhin, dass er angreifbar ist – trotz EAL4-Zertifikat²⁶.

2.3.3.7 IEC 62443

Die Norm IEC 62443 ist in vier thematisch zusammenhängende Abschnitte gegliedert, die jeweils aus mehreren Dokumenten bestehen.

In dem ersten Abschnitt werden übergeordnete Aspekte behandelt wie allgemeine Konzepte, Terminologien und Methoden.

Der zweite Abschnitt definiert organisatorische Maßnahmen und Prozesse, die als Bestandteil eines Defense-in-Depth-Konzepts relevant sind. Das Defense-in-Depth-Konzept basiert auf der Erkenntnis, dass beim Schutz der Industrieanlage die Beteiligung aller Stakeholder erforderlich und eine einzige Maßnahme nicht ausreichend ist.

Der dritte Abschnitt ist vorwiegend technischer Natur. Eines der Dokumente spezifiziert IT-Sicherheitsrelevante Anforderungen an die funktionalen Fähigkeiten der Automatisierungssysteme. Die Segmentierung des Kommunikationsnetzwerks ist eine wichtige Maßnahme zum Schutz gegen Cyberangriffe, um die Auswirkungen innerhalb der Automatisierungslösung einzuschränken. Sie muss in enger Zusammenarbeit zwischen Betreiber und Integrator festgelegt werden. Auf Basis einer Risikoanalyse legt man ein zu erreichendes Level der Schutzmaßnahmen für jede Zone und jeden Kanal fest. Dies ist Gegenstand eines weiteren Dokuments, das Methoden und Mittel beschreibt, um die Automatisierungslösung in Zellen und Kommunikationskanälen, sog. „Zonen und Conduits“, zu strukturieren. Unter anderem ist in diesem Abschnitt ein technischer Bericht über aktuelle Schutztechniken gegen Cyberangriffe enthalten.

Der vierte Abschnitt richtet sich an die Hersteller von Komponenten, die in Automatisierungslösungen eingesetzt werden. Allgemein gilt, dass die IT-Sicherheit integraler Bestandteil des Entwicklungsprozesses sein sollte. Damit sollen möglichst das Entstehen von Schwachstellen vermieden und Maßnahmen zur Stärkung der Robustheit bei Automatisierungskomponenten gegen Cyber-Bedrohungen vorgenommen

²⁶Common Criteria for Information Technology Security Evaluation

werden. Dies wird in einem der beiden Dokumente dieses Abschnittes behandelt. Das zweite Dokument (DIN IEC 62443-3-3) spezifiziert Anforderungen an funktionale Fähigkeiten von Komponenten.

Einzelne Teile der Normenreihe IEC 62443 sind schon verabschiedet sowie veröffentlicht und weitere Teile dieser Normenreihe sind aktuell in Bearbeitung. Die Inhalte der wesentlichen Dokumente sind ausreichend stabil, um als Basis zur Erstellung eines Schutzkonzepts für industrielle Anlagen genutzt werden zu können.²⁷

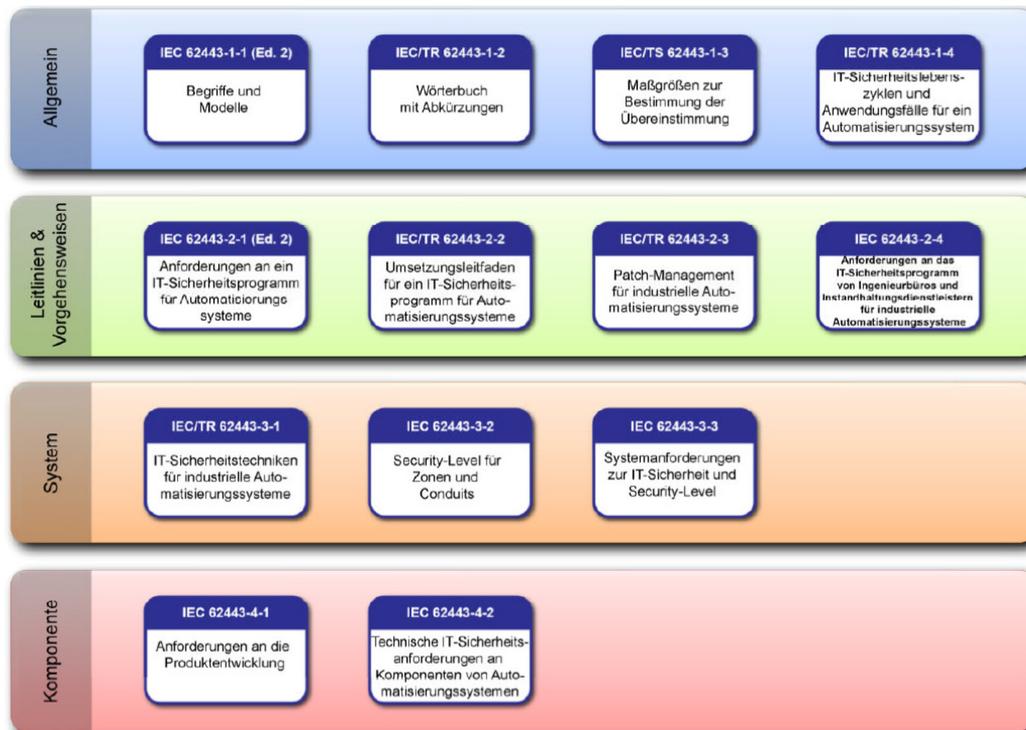


Abbildung 13 – Aufbau der Normenreihe IEC 62443 (Quelle: E DIN IEC 62443-3-3 (VDE 0802-3-3))

In E DIN IEC 62443-3-3 (VDE 0802-3-3) werden die SLs (en: Security level, Sicherheitsstufe) in fünf verschiedenen Stufen (0, 1, 2, 3 und 4), die jeweils ein erhöhtes Sicherheitsniveau aufweisen, definiert. Das aktuelle Modell zur Definition von SLs hängt vom Schutz einer zunehmenden komplexeren Bedrohung ab und unterscheidet sich je nach SL-Typ geringfügig. Für SL-C bedeutet dies, dass eine bestimmte Komponente oder ein bestimmtes System durch einen Anlagenbesitzer oder Systemintegrator konfiguriert werden kann, um sich vor einer zunehmend komplexen Art von Bedrohungen zu schützen.

Für SL-T bedeutet dies, dass der Anlagenbesitzer oder Systemintegrator durch eine Risikobewertung ermittelt hat, dass diese Zone, dieses System oder diese Komponente vor diesem Bedrohungsgrad geschützt werden müssen. Für SL A bedeutet dies, dass der Anlagenbesitzer, Systemintegrator,

²⁷ Leitfaden Industrial Security, VDE-Verlag, Kapitel 3, Seite 13

Produktlieferant und oder eine Kombination aus diesen die Zone, das System oder die Komponente so konfiguriert hat, dass sie die speziellen Sicherheitsanforderungen erfüllen, die für diesen SL definiert sind.

Die Sprache, die für jede SL verwendet wird, verwendet Begriffe wie zufällig, einfach, anspruchsvoll und erweitert. Diese Sprache ist absichtlich vage, um die gleiche Basissprache für alle Dokumente der IEC 62443 Serie zu verwenden. Jedes der einzelnen Dokumente in der Serie definiert die Anforderungen für die SLs, die für ihren speziellen Zweck gelten.

Während die Anforderungen für alle SLs in der IEC 62443 Serie unterschiedlich sein müssen, muss ein allgemeines Verständnis dafür vorliegen, wovon jedes der SLs schützen soll. Die nächsten Abschnitte enthalten einige Hinweise zur Unterscheidung zwischen den SLs.

SL0: Keine spezifischen Anforderungen oder Sicherheitsschutz notwendig

Dieses Level hat mehrere Bedeutungen, abhängig von der Situation, in der es angewendet wird. Bei der Definition von SL-C würde es bedeuten, dass die Komponente oder das System einige der SL 1 Anforderungen für bestimmte FR (en: Foundational requirements, grundlegende Anforderungen) nicht erfüllt. Dies würde höchstwahrscheinlich für Komponenten oder Systeme gelten, die Teil einer größeren Zone wären, in der andere Komponenten oder Systeme kompensierende Gegenmaßnahmen bereitstellen würden. Bei der Definition von SL-T für eine bestimmte Zone bedeutet dies, dass der Anlagenbesitzer festgestellt hat, dass die Ergebnisse seiner Risikoanalyse darauf hindeuten, dass für diese bestimmte FR auf dieser Komponente oder diesem System weniger als die vollständigen SL 1 spezifischen Anforderungen erforderlich sind. Dies würde eher für einzelne Komponenten innerhalb eines Systems oder einer Zone passieren, die in keiner Weise zu den FR spezifischen Anforderungen beitragen.

SL1: Schutz gegen zufällige Verletzung

Zufällige Verletzungen der Sicherheit sind in der Regel durch die lockere Anwendung von Sicherheitsrichtlinien verbunden. Diese können von wohlmeinenden Mitarbeitern ebenso leicht verursacht werden wie durch eine Außenseiter-Bedrohung. Viele dieser Verstöße werden im Zusammenhang mit Sicherheitsprogrammen stehen und werden durch Durchsetzung von Richtlinien und Verfahren behandelt. Unter Verwendung von Abbildung 14 wäre ein einfaches Beispiel ein Operator, der einen Sollwert auf der Engineering Station in der BPCS-Zone (en: Basic Process Control System, Betriebs- und Überwachungseinrichtung) auf einen Wert außerhalb bestimmter vom Techniker festgelegter Bedingungen ändern kann. Das System erzwingt die korrekte Authentifizierung nicht und verwendete Kontrollbeschränkungen, um die Änderung durch den Operator zu verhindern. Die der genannten Abbildung 14 wird ein weiteres Beispiel dafür verwendet, dass ein Kennwort im Klartext über die Leitung zwischen der BPCS-Zone und der DMZ (en: demilitarized zone, Demilitarisierte Zone) gesendet wird, sodass ein Netzwerktechniker das Kennwort bei der Fehlerbehebung des Systems einsehen kann. Das System erzwingt keine angemessene Vertraulichkeit der Daten, um das Passwort zu schützen.

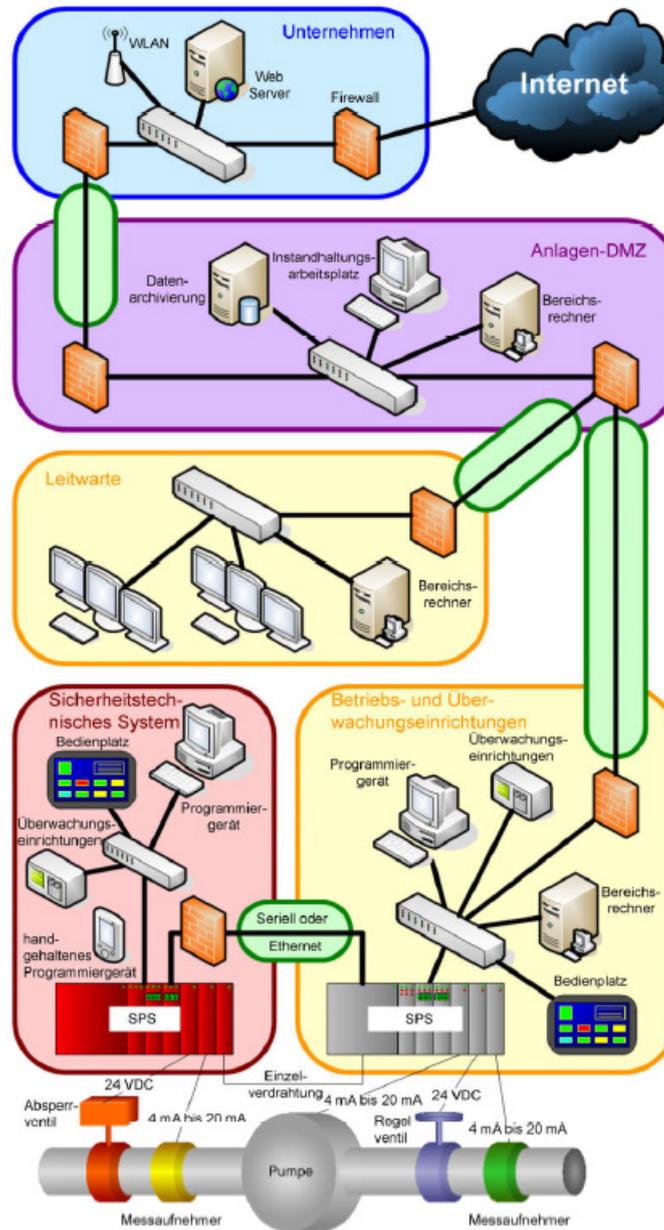


Abbildung 14 – Beispiel aus der verfahrenstechnischen Industrie mit Zonen und Conduits

Ein drittes Beispiel wäre in Abbildung 15 ein Ingenieur, der auf die Speicherprogrammierbare Steuerung (SPS) im Industriellen Kommunikationsnetz #1 (en: Industrial Network #1) zugreift, aber tatsächlich auf die SPS im Industriellen Kommunikationsnetz #2 (en: Industrial Network #2) zugreift. Das System erzwang nicht die ordnungsgemäße Einschränkung des Datenflusses, so dass der Ingenieur nicht auf das falsche System zugreifen konnte.

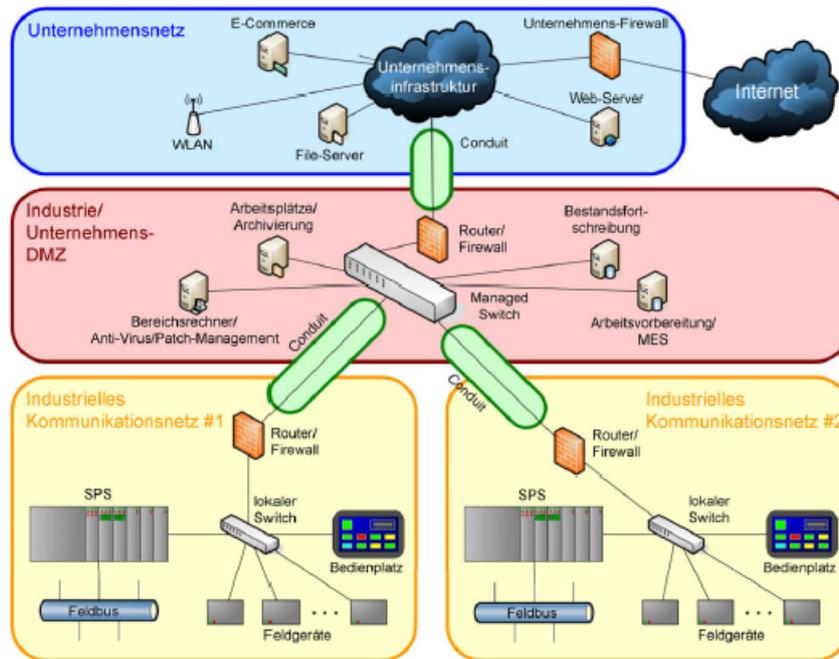


Abbildung 15 – Beispiel aus der Fertigungsindustrie mit Zonen und Conduits

SL2: Schutz vor vorsätzlichen Verstößen mit einfachen Mitteln mit geringen Ressourcen, generischen Fähigkeiten und geringer Motivation

Einfache Mittel erfordern nicht viel Wissen seitens des Angreifers. Der Angreifer benötigt keine detaillierte Kenntnis der Sicherheit, der Domäne oder des betroffenen Systems. Diese Angriffsvektoren sind bekannt und es können automatisierte Werkzeuge zur Unterstützung des Angreifers vorhanden sein. Sie sind auch dafür ausgelegt, eine große Anzahl von Systemen anzugreifen, anstatt auf ein bestimmtes System zu zielen, so dass ein Angreifer keine nennenswerte Motivation oder Ressourcen benötigt.

Mit Abbildung 14 zeigt eine Beispiel für ein Virus, das die Wartungsarbeitsstation in der Plant DMZ infiziert, die sich auf die BPCS-Engineering-Workstation ausbreitet, da beide das gleiche allgemeine Betriebssystem verwenden. In der Abbildung 14 ist ein Angreifer, der einen Webserver im Unternehmensnetzwerk durch ein kleines Schadprogramm bzw. eine Befehlsfolge kompromittiert (Exploits), der aus dem Internet für eine öffentlich bekannte Schwachstelle im allgemeinen Betriebssystem des Webserver heruntergeladen wird. Der Angreifer verwendet den Webserver als Drehpunkt bei einem Angriff auf andere Systeme im Unternehmensnetzwerk sowie im industriellen Netzwerk. Ein drittes Beispiel wäre auch ein Operator, der eine Website auf dem HMI (en: Human Maschine Interface, Mensch-Maschinen-Schnittstelle) im Industrial Network #1 sieht, in dem ein Trojaner heruntergeladen wird, dein einen Bereich in den Routern und Firewalls in das Internet öffnet.

SL3: Schutz vor vorsätzlichen Verstößen mit ausgefeilten Mitteln mit moderaten Ressourcen, Industrial Automation Control Systems (IACS)-spezifischen Fähigkeiten und moderater Motivation. Der Begriff IACS

umfasst alle Bestandteile, die für den zuverlässigen und sicheren Betrieb einer automatisierten Produktionsanlage erforderlich sind.

Anspruchsvolle Mittel erfordern fortgeschrittenes Sicherheits-Wissen, erweitertes Fachwissen, fortgeschrittene Kenntnisse des Zielsystems oder Kombinationen daraus. Ein Angreifer, der nach einem SL 3-System sucht, verwendet wahrscheinlich Angriffsvektoren, die für das spezifische Zielsystem angepasst wurden. Der Angreifer kann Exploits in nicht bekannten Betriebssystemen, Schwachstellen in industriellen Protokollen, spezifische Informationen über ein bestimmtes Ziel, die die Sicherheit des Systems verletzen, oder andere Mittel verwenden, die eine höhere Motivation sowie Fähigkeiten und Kenntnisse erfordern als erforderlich für SL 1 oder 2.

Ein Beispiel für ausgeklügelte Mittel könnten Passwort- oder Schlüsselcracking-Tools sein, die auf Hash-Tabellen basieren. Dieses Tools stehen zum Download zur Verfügung, erfordern jedoch Kenntnisse über das System (z.B. den Hash eines zu knackenden Passworts). Ein weiteres Beispiel wäre ein Angreifer, der über die serielle Leitung Zugriff auf die Functional Safety-SPS (FS-SPS) erhält, nachdem er über eine Sicherheitslücke im Ethernet-Controller Zugriff auf die Steuerungs-SPS erlangt hat. Unter Verwendung von Abbildung 12 wäre ein drittes Beispiel ein Angreifer, der Zugriff auf die Datenhistoriker erhält, indem er einen Angriff mit „roher Gewalt “ (en: brute force attack) über die DMZ-Firewall für Industrie und Unternehmen aus dem drahtlosen Unternehmensnetzwerk ausführt. Die Brute-Force-Methode ist eine Angriffsform, bei der Hacker versuchen, durch „rohe Gewalt “ (en: brute force) also durch mehr oder weniger wahlloses Ausprobieren Passwörter zu knacken oder Daten zu entschlüsseln.

SL4: Schutz vor vorsätzlichen Verstößen durch ausgefeilte Mittel mit erweiterten Ressourcen, IACS-spezifische Fähigkeiten und hohe Motivation

SL3 und SL 4 sind insofern sehr ähnlich, als beide hochentwickelte Mittel beinhalten, um die Sicherheitsanforderungen des Systems zu verletzen. Der Unterschied besteht darin, dass der Angreifer noch motivierter ist und erweiterte Ressourcen zur Verfügung hat. Diese können leistungsfähige Rechenressourcen, eine große Anzahl von Computern oder längere Zeiträume umfassen.

Ein Beispiel für ausgeklügelte Mittel mit erweiterten Ressourcen wäre die Verwendung von Supercomputern oder Computerclustern, um Brute-Force. Passwort-Cracking unter Verwendung großer hash-Tabellen durchzuführen. Ein anderes Beispiel wäre ein Botnetz, das ein System angreift, das mehrere Angriffsvektoren gleichzeitig verwendet. Ein drittes Beispiel wäre eine organisierte kriminelle Organisation, die die Motivation und die Ressourcen hat, Wochen zu verbringen, um ein System zu analysieren und benutzerdefinierte Zero-Day-Exploits (wenn ein Benutzer eine Sicherheitslücke in einem Programm entdeckt, kann er diese dem Softwareunternehmen melden, damit ein entsprechendes Sicherheitspatch entwickelt wird) zu entwickeln.²⁸

²⁸ E DIN IEC 62443-3-3 (VDE 0802-3-3):2015-06, A.2, Seiten 75 bis 79

2.3.4 Resümee

Die durchgeführte Recherche zu aktuellen Normen- und Standardisierungsprojekten zeigt, dass eine Vielzahl an Normen, Richtlinien und Standards im Umfeld der Informationssicherheit Teilbereiche im Kontext „Sichere Digitale Identitäten“ aufgegriffen haben. Verschiedene Normungs- und Standardisierungsorganisationen haben zum Teil auch Festlegungen getroffen, die das Thema von digitalen Identitäten, meist bezogen auf einen konkreten Anwendungsfall, betreffen. Das führte zu Inzellösungen, die nicht kompatibel sind und zu einer erheblichen Fragmentierung von sicheren digitalen Identitäten in der Normung und Standardisierung selbst innerhalb einer Branche. Denn es fehlt oft an einer für ein Unternehmen einheitlichen Vorgehensweise für sichere digitale Identitäten, da es unterschiedliche Normen und Standards für diverse Rollen der einzelnen Bereiche innerhalb eines Unternehmens gibt. Das beginnt mit den digitalen Identitäten der Mitarbeiter eines Unternehmens für den Zugang zu Systemen und Anwendungen und setzt sich fort bei der Kommunikation und dem Datenaustausch mit Kunden und Partnern. Das führt zu unterschiedlichen Lösungen hinsichtlich des Zugriffs auf Systeme und Produkte des Unternehmens, um diese z. B. remote zu warten und zu pflegen. Dadurch werden in nahezu jedem Unternehmen Ressourcen und Kosten verbraucht, um zumindest ein Mindestmaß an interner Koordination zu erreichen. Diese Situation wird insbesondere KMUs behindern, da diese die erhöhte Entwicklungskosten und personellen Ressourcen nicht aufwenden können. Es bleibt auch immer ein Maß an Unsicherheit, sowie eine suboptimale Allokation der Ressourcen. Damit wird Aufwand betrieben, welcher für die Weiterentwicklung der Technologie und Lösungen fehlt.

So wichtig es auch ist, dass sichere digitale Identitäten sich in der Normung und Standardisierung der unterschiedlichsten Branchen und Produkte wiederfinden, so wichtig ist es aber auch ein gemeinsames Verständnis und einen gemeinsamen Rahmen zu haben, und so für Orientierung und Interoperabilität zu sorgen. Daher müssen bestimmte Themen im Interesse aller über alle Normungs- und Standardisierungsorganisationen orchestriert werden. Zu diesen Themen gehören vor allem:

- Terminologie und Typologisierung
- harmonisierte Sicherheitslevel
- Governance Modell und Strukturen

Dann können die Detailregelungen für unterschiedliche Branchen und Produkte entsprechend auf diese übergeordneten Punkte verweisen. Das vermeidet Widersprüche und Missverständnisse und ist die wichtige Grundlage für eine branchenübergreifende Interoperabilität von digitalen Identitäten. Der entsprechende Koordinierungsaufwand, der hier notwendig ist, ist erheblich geringer als die Summe der vielen Einzelaktivitäten, die heute jedes Unternehmen für sich regeln muss. Deutschland als ein führendes Mitglied der europäischen und internationalen Normung bei ISO, IEC, CEN und CENELEC muss hier Initiative ergreifen, um vor allem die mittelstandsgeprägte Wirtschaft zu stärken. Das Beherrschen sicherer digitale Identitäten ist nicht nur bei dem Thema Industrie 4.0 für den Marktzugang wichtig.

Heutzutage werden signifikante Informationstechnologien und Strukturen außerhalb von Deutschland, z.B. USA, China und Korea, entwickelt. Dem kann durch eine einheitliche und unternehmensübergreifende Normung und Standardisierung begegnet werden.

Dies kann durch eine noch einzurichtende, neutrale nationale Koordinierungsstelle, die international agiert, sichergestellt werden. Die Aufgabe der Koordinierungsstelle liegt hierbei in der kontinuierlichen Betrachtung und Analyse der international agierenden Normungs- und Standardisierungs-Organisationen,

wie beispielsweise IETF, IEEE, TCG, FIDO Alliance. Hierbei ist die grundlegende Aufgabe der Koordinierungsstelle der Informationstransfer zu nationalen Gremienstrukturen herzustellen und bei gemeinschaftlichen Normungs- und Standardisierungs-Verfahren als Vermittler oder als Transferpartner zu agieren und die Gremienarbeit zu unterstützen.

2.4 Recherche Recht

2.4.1 Ziele, Aufbau und Vorgehen

SDI unterliegen vielfältigen Anwendungsszenarien, darüber hinaus sind sie nicht selten mit interdisziplinären Themenstellungen und Sachverhalten verknüpft. Bei einer Betrachtung der juristischen Grundlagen von SDI ist es deshalb notwendig, domänenübergreifend sachverhaltsspezifische Rechtsvorschriften zu ermitteln, diese zu systematisieren und zu interpretieren. Indem juristische Vorgaben das Ergebnis eines demokratischen Meinungsbildungsprozesses darstellen, geben sie nicht selten auch die generelle Auffassung von Bevölkerung und Wirtschaft im Hinblick auf bestimmte Maßnahmen – hier: Technologien – wieder. Unter diesen Gesichtspunkten war es eines der vordefinierten Hauptziele der juristischen Recherche von SDI, nicht nur die allgemeinen rechtlichen Rahmenbedingungen zu ermitteln, in denen sich sichere digitale Identitäten bewegen, sondern, gemessen an den regulatorischen Vorgaben, auch zu bestimmen, in welchen Anwendungsfeldern SDI jetzt und in Zukunft verstärkt zur Anwendung gelangen können und werden. Durch den Stakeholder-Dialog wurde darüber hinaus sichergestellt, dass stets eine Rückspiegelung der gefundenen Ergebnisse in die entsprechenden Interessengruppen und Gremien erfolgte, um eventuelle Diskrepanzen zwischen der öffentlichen Wahrnehmung von SDI im rechtlichen Bereich und dem praktischen Handlungsbedarf aus der Wirtschaft zu ermitteln. Die juristische Bearbeitung von SDI konzentrierte sich dementsprechend auf drei Arbeitsschwerpunkte:

1. Rechtsrecherche: Ermittlung der wesentlichen juristischen Grundlagen für SDI in Deutschland sowie in Europa und deren Systematisierung in Europa-, Bundes- und Landesrecht und in gesetzliche sowie untergesetzliche Vorgaben. Darüber hinaus erfolgte die Sichtung und Zusammenstellung von Rechtsprechung und juristischer Fachliteratur für den Bereich der SDI.
2. Auslegung der gefundenen juristischen Vorgaben: Ermittelt wurde, unter welchen Bezugspunkten und mit welcher Granularität die juristischen Vorschriften auf SDI Bezug nehmen: So ist es einerseits möglich, dass sichere digitale Identitäten in rechtlichen Vorgaben explizit benannt werden, sich der Bezug zu ihnen andererseits aber auch erst durch eine extensivierende Auslegung der gefundenen Rechtsvorschrift ergibt.
3. Relevanzbeurteilung: Unter Einbeziehung der an SDI beteiligten Stakeholder ist zu bestimmen, in welchen wirtschaftlichen Themenfeldern, Forschungs- sowie Arbeitsbereichen ausgehend vom Recht ein besonderes Bedürfnis zur Schaffung sicherer digitaler Identitäten besteht und inwieweit das Recht hierbei einen unterstützenden Beitrag leisten kann, so zum Beispiel als Impulsgeber.

Bei der Bearbeitung sämtlicher Arbeitspakete wurde die Prämisse zugrunde gelegt, dass die rechtliche Regulierung von SDI nicht nur, wie zumeist üblich, der Vereinheitlichung von Sachverhalten dient und Transparenz sowie Vorhersehbarkeit staatlichen Handelns im Sinne der Rechtssicherheit gewährleisten soll, sondern durch die damit zugleich beschriebene rechtspolitische Entwicklung, die in einer demokratischen Gesellschaftsordnung die Stimmen der Mehrheit der Bevölkerung wiedergibt, auch die technologische Entwicklung in Deutschland in einem wesentlichen Sinne mitbestimmt. Hieraus lässt sich eine enge Verknüpfung zwischen Rechts- und Normungspolitik herleiten: Indem die juristischen Grundlagen für eine neue Technologie wie SDI geschaffen werden, geben sie zugleich auch der Normung und der Standardisierung wesentliche Leitlinien vor, in welche Richtung die Konstituierung allgemein verbindlicher technischer Vorgaben in diesem Forschungsfeld gehen soll.

2.4.2 Darstellung der gefundenen Ergebnisse

Die juristischen Vorgaben mit einem herleitbaren SDI-Bezug sind umfassend. Als generelle Aussage lässt sich festhalten, dass nahezu sämtliche Rechtsvorschriften mit einem Bezug zur Informationssicherheit die Aufnahme von SDI ermöglichen, wobei unterschiedliche Anwendungsfelder sicherer digitaler Identitäten deutlich zutage treten und zur Systematisierung der gefundenen Rechtsvorschriften verwendet werden können: die Sicherheit in der Kommunikation Mensch – Mensch, die Sicherheit in der Kommunikation Mensch – Maschine sowie die Sicherheit in der Kommunikation Maschine – Maschine. Deutlich wird, dass durch das geltende Recht nicht alle drei Anwendungsfelder gleichermaßen feingranular abgedeckt werden. Regelungslücken bestehen hier insoweit, als dass der Bezug zu SDI in einer Vielzahl von juristischen Vorschriften nur durch eine extensivierende Auslegung hergestellt werden kann. So wird das Thema in verschiedenen Rechtsvorschriften unmittelbar adressiert, wohingegen andere Gesetze nur einen mittelbaren Bezug zur Thematik herstellen, beispielsweise über den Themenkreis der IT- und Cybersicherheit. Hierdurch wird auch deutlich, dass das Zusammenspiel von Recht und Technik in Zukunft noch weiter zu intensivieren ist, indem rechtspolitisch nicht nur mittelbar auf die technische Normung eingewirkt wird, sondern die technische Normung weitergehend als bisher zur Auslegung des Rechts herangezogen werden kann und sollte.

Die Rechtsgrundlagen von SDI sind so vielfältig wie die abgedeckten Anwendungsfelder und auf allen Regulierungsebenen vertreten, so finden sich Vorgaben im Europa-, im Bundes- und im Landesrecht, im gesetzlichen sowie im untergesetzlichen Bereich, thematisch beispielsweise verortet in den Bereichen Industrie 4.0, KRITIS, öffentliche Verwaltung, e-Commerce, Health, Mobilität, Bankwesen, und Smart Cities. Auch die juristische Fachliteratur sowie die Rechtsprechung nehmen auf SDI Bezug. Deutlich wird somit die enorme gesellschafts- und wirtschaftspolitische Relevanz des Themas. Durch die unterschiedliche Granularität der Themenabdeckung offenbart sich aber auch gleichermaßen, dass das Thema der SDI in rechtspolitischer Hinsicht noch nicht überall in gleicher Tiefe angelangt ist und folglich das technische wie wirtschaftliche Potenzial von sicheren digitalen Identitäten noch längst nicht vollständig ausgeschöpft werden konnte.

Beispiele für Rechtsvorschriften im Bereich der SDI sind im Bereich des Europarechts die eIDAS-Verordnung und die E-Commerce-Richtlinie; auf bundesrechtlicher Ebene das Signaturgesetz, (aufgehoben mit Wirkung vom 29.07.2017), das De-Mail-Gesetz, das E-Government-Gesetz, das BSI-Gesetz, das Bundesdatenschutzgesetz, das Telekommunikations- und das Energiewirtschaftsgesetz, das Messstellenbetriebsgesetz, wie auch allgemeine und branchenübergreifende Vorgaben aus dem Aktien- oder aus dem GmbH-Gesetz. Die landesrechtlichen Rechtsvorschriften zu sicheren digitalen Identitäten bewegen sich vornehmlich im Bereich der digitalen Verwaltung und des digitalen Zugangs des Bürgers zu Behördendiensten. Verschiedene Länder haben deshalb inhaltlich ähnliche ausgestaltete Regelungen erlassen, so zum Beispiel Baden-Württemberg mit dem E-Government-Gesetz oder Bayern mit der Verordnung über den elektronischen Rechtsverkehr bei den ordentlichen Gerichten (E-Rechtsverkehrsordnung Justiz – ERVV Ju). Die hohe Aktualität der Thematik spiegelt sich vor allem auch in der Rechtsprechung und der rechtswissenschaftlichen Literatur zu SDI wider: Hier wird vor allem explizit bisher fast ausschließlich nur der Mensch bzw. die menschliche Kommunikation in den Mittelpunkt der Betrachtungen gestellt, wohingegen das Potenzial von SDI, beispielsweise bezogen auf die rein maschinelle Kommunikation unter Gesichtspunkten der IT-Sicherheit, bisher eine nur unzureichende Berücksichtigung findet. Gerade hier sind aber wesentliche Handlungsfelder der zukünftigen Forschung zu sicheren digitalen Identitäten zu verorten.

Soweit SDI nicht explizit angesprochen werden, lässt sich der Zugang zu ihnen im rechtlichen Bereich in vielen Fällen nur über eine Auslegung ermitteln, die über unbestimmte Rechtsbegriffe bzw. über Generalklauseln als Anknüpfungspunkt vorgenommen wird. Oft finden sich in Rechtsquellen bewusst offen formulierte Normen, wie „Stand der Technik“, „Sorgfalt eines ordentlichen Geschäftsmannes“ oder „Zuverlässigkeit“. Die Verwendung derartiger unbestimmter Rechtsbegriffe ist angesichts der raschen wissenschaftlichen und technischen Veränderungen notwendig. Insbesondere wenn die umfassende Regelung eines Sachverhalts unmöglich erscheint, ist eine offene Formulierung sinnvoll, um einen dynamischen Grundrechtsschutz²⁹ zu vermitteln. Als allgemeine und branchenübergreifende Beispiele unbestimmter Rechtsbegriffe können hier der § 91 II AktG und der § 43 I GmbHG herangezogen werden – denn tatsächlich weisen die zwei Vorschriften einen Bezug zu SDI auf, ohne dass dies explizit im Wortlaut dargestellt wird. So verpflichtet § 91 II AktG verpflichtet den Vorstand, „geeignete Maßnahmen“ zu ergreifen, um Bestandsgefährdungen der Gesellschaft zu erkennen. Die „geeigneten Maßnahmen“ sind normativer Anknüpfungspunkt für die Frage, ob die Maßnahmen auch IT-sicherheitspezifisch sein müssen. Ein klares Verständnis davon, was unter „geeignete Maßnahme“ zu verstehen ist, ergibt sich aus der Fassung der Norm selbst nicht. Die Literatur geht überwiegend davon aus, dass Maßnahmen im Sinne der Vorschrift geeignet sind, wenn nach der Erfahrung (eines ordentlichen und sorgfältigen Geschäftsleiters)³⁰ davon ausgegangen werden könne, dass der Vorstand die erforderlichen Informationen zur Bestandsicherung rechtzeitig erhält.³¹ Über die geeigneten Maßnahmen entscheide der Vorstand innerhalb seines Ermessens³² unter Berücksichtigung der Besonderheiten des betroffenen Unternehmens, insbesondere seiner Größe, Struktur, Lage und Branchenzugehörigkeit sowie seinem Kapitalmarktzugang.³³ Umstritten ist, ob die gesetzliche Anordnung, „insbesondere ein Überwachungssystem“ einzurichten, als Konkretisierung der geeigneten Maßnahmen zu verstehen ist. Der Streit betrifft indes nicht unmittelbar die Frage, ob § 91 II AktG auch eine Vorschrift des IT-Sicherheitsrechtes ist. Mit der überwiegenden rechtswissenschaftlichen Literatur ist daher davon auszugehen, dass das Überwachungssystem die Umsetzung und Einhaltung der eingeleiteten Maßnahmen zur Früherkennung bestandsgefährdender Risiken kontrollieren soll.³⁴ Nach allgemeinem Verständnis hat der Vorstand einer Aktiengesellschaft demnach gemäß § 91 II AktG auf einer ersten Stufe ein Risikomanagementsystem einzurichten, welches auf die Früherkennung bestandsgefährdender Risiken abzielt, und dieses auf einer zweiten Stufe durch ein Überwachungssystem zu kontrollieren.

Fraglich ist jedoch, ob hierunter auch Maßnahmen fallen, die den Bereich der sicheren digitalen Identitäten abdecken. Bei den zu treffenden „geeigneten Maßnahmen“ handelt es sich um einen unbestimmten

²⁹ BVerfG, Beschluss vom 8. August 1978 – 2 BvL 8/77 = NJW 1979, 359 (362).

³⁰ *Dauner-Liebin* in Henssler/Strohn, Gesellschaftsrecht, AktG § 91 Rn 8.

³¹ *Fleischer* in Spindler/Stilz, AktG, 3. Aufl., § 91 Rn 33; *Kort* in Hopt/Wiedemann, AktG, 4. Aufl., § 91 Rn 44; *Krieger/Sailer* in Schmidt/Lutter, AktG, 3. Aufl., § 91 Rn 12; *Müller-Michaels* in Hölters, AktG, 2. Aufl., § 91 Rn 6; *Spindler* in Goette/Habersack/Kalss, MüKo-AktG, 4. Aufl., § 91 Rn 23.

³² Vgl. OLG Frankfurt am Main, Urteil vom 12. Dezember 2007 – 17 U 111/07 = AG 2008, 453 (455); *Bürgers/Israel* in Bürgers/Körber, AktG, 4. Aufl., § 91 Rn 10; *Koch* in Hüffer, AktG, 12. Aufl., § 91 Rn 7; *Mertens/Cahn* in Zöllner/Noack, AktG, 3. Aufl., § 91 Rn 25.

³³ *Grigoleit/Tomasic* in Grigoleit, AktG, § 91 Rn 7; *Kort* in Hopt/Wiedemann, AktG, 4. Aufl., § 91 Rn 47; *Spindler* in Goette/Habersack/Kalss, MüKo-AktG, 4. Aufl., § 91 Rn 28 ff.

³⁴ *Grigoleit/Tomasic* in Grigoleit, AktG, § 91 Rn 8; *Koch* in Hüffer, AktG, 12. Aufl., § 91 Rn 8; aA etwa *Spindler* in Goette/Habersack/Kalss, MüKo-AktG, 4. Aufl., § 91 Rn 30.

Rechtsbegriff, dessen Verwendung durch das Bundesverfassungsgericht grundsätzlich als zulässig eingestuft wird.³⁵ Im Hinblick auf das IT-Sicherheitsrecht als Querschnittsmaterie mit Bezügen zur Technik liegt die Herausforderung indes darin, dass in vielen Fällen nicht auf eine bestehende Auslegungserfahrung zurückgegriffen werden kann.³⁶ Angesichts einer fehlenden speziellen Methodik muss die Auslegung unbestimmter Rechtsbegriffe sich daher auch im Kontext von IT-sicherheitsrechtlichen Aspekten an den bewährten Auslegungsmethoden von Wortlaut, Systematik, Gesetzgebungsgeschichte (historische Auslegung) sowie Sinn und Zweck (teleologische Auslegung) orientieren.

Der Wortlaut des § 91 II AktG ist aufgrund seiner offenen Formulierung allein untauglich, um die Frage des Bezuges zur IT-Sicherheit und somit auch von SDI zu beantworten.³⁷ Zumindest aber schließt er gerade wegen seiner unbestimmten Weite nicht aus, als Einfallstor für IT-sicherheitsrechtliche Vorgaben zu fungieren. Weil das Tatbestandsmerkmal „geeignete Maßnahmen“ ein unbestimmter Rechtsbegriff ist, liegt es im Gegenteil nahe, die Norm für IT-sicherheitsrechtliche Einflüsse und somit auch für sichere digitale Identitäten offen zu halten. Bei einer systematischen Betrachtung des § 91 II AktG wird die Vorschrift zur Auslegung ihrer unbestimmten Rechtsbegriffe in das gesamte Rechtsgefüge einbezogen und auch zu anderen, vergleichbaren Vorschriften in Bezug gesetzt. Zentrale Rechtsnormen sind hier insbesondere der § 93 I 1 AktG sowie der § 25a I KWG.

Ausgehend von § 93 I 1 AktG haben die Vorstandsmitglieder bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Die sogenannte „Business Judgement Rule“³⁸ besagt – verkürzt –, dass Vorstände nicht für negative Folgen unternehmerischer Entscheidungen einzustehen haben, wenn die Entscheidung auf Grundlage angemessener Informationen zum Wohl der Gesellschaft gefasst wurde. In der Literatur wird darauf hingewiesen, dass die Pflicht zur Etablierung effektiver IT-Sicherheitsmaßnahmen und damit mittelbar auch von SDI aus § 93 I 1 AktG folge und § 91 II AktG keine wesentlichen Neuerungen enthalte.³⁹ Die Pflicht, für eine angemessene Organisation zu sorgen und gefährdende Entwicklungen zu erkennen, habe schon gemäß §§ 76, 93 AktG bestanden.⁴⁰ Will man § 91 II AktG so auslegen, dass aus ihm die gleichen Pflichten folgen, wie sie ohnehin bislang aus §§ 76, 93 AktG abgeleitet wurden, dann erscheint § 91 II AktG zwar überflüssig. Allerdings ist § 91 II AktG zum einen spezifischer als der allgemeinere § 93 AktG, indem er nur auf die Früherkennung bestandsgefährdender Risiken abstellt. Zum anderen liegt ein wesentlicher Unterschied zwischen § 91 II AktG und § 93 I 1 AktG darin, dass § 91 II AktG nicht die Pflicht umfasst, auf erkannte Risiken zu reagieren. Schließlich ergibt sich aus der Gesetzesbegründung, dass der Gesetzgeber die bestehenden Pflichten mit der Fassung des § 91 II AktG „hervorheben“ wollte.⁴¹ Der Norm kommt daher eine Klarstellungsfunktion zu. Dass sie also eine

³⁵ StRspr BVerfGE 21, 73 (79); 31, 255 (264); 37, 132 (142); BVerfG, Beschluss vom 8. August 1978 – 2 BvL 8/77 = NJW 1979, 359 (361).

³⁶ KipkerDuD 2016, 610.

³⁷ Vgl. von Holleben/Menz CR 2010, 63 f.

³⁸ Zum Begriff *Dauner-Lieb* in Henssler/Strohn, Gesellschaftsrecht, AktG § 93 Rn 17; Spindler NZG 2005, 865 (871).

³⁹ Spindler in Fleischer, Handbuch des Vorstandsrechts, § 19 Rn 6 mwN.

⁴⁰ Conrad in Auer-Reinsdorf/Conrad, Handbuch IT- und Datenschutzrecht, § 33 Rn 36 mit Verweis auf Merkt DB 2014, 2271 (2272).

⁴¹ Begründung RegE KonTraG BT-Drs 13/9712, S. 15.

Pflicht regelt, die ohnehin galt, macht sie nicht überflüssig. Danach sprechen die besseren Gründe dafür, die Auslegung des § 91 II AktG an § 93 AktG zu orientieren, woraus für § 91 II AktG die Pflicht zu IT-Sicherheitsmaßnahmen und damit auch zur Einführung von sicheren digitalen Identitäten folgen kann, obwohl dies im Gesetzeswortlaut nicht ausdrücklich verankert ist. § 25a I 3 Nr. 4 KWG schreibt vor, dass eine ordnungsgemäße Geschäftsorganisation insbesondere ein angemessenes und wirksames Risikomanagement umfassen muss, das auch die personelle sowie die technisch-organisatorische Ausstattung des Kreditinstituts angemessen berücksichtigt. Die Norm nimmt eine allgemeine Schrittmacherrolle⁴² ein, weshalb sie für die Auslegung des § 91 II AktG im Hinblick auf SDI von Bedeutung ist. Gegen eine direkte Beeinflussung der Auslegung von § 91 II AktG spricht jedoch zunächst, dass § 25a KWG nicht unmittelbar auf Aktiengesellschaften anwendbar ist, solange sie nicht Finanzdienstleistungen anbieten. Außerdem ist § 25a KWG der qualitativen Bankenaufsicht zuzuschlagen und verfolgt damit ein anderes Ziel. Zweck des KWG ist, durch vorbeugende Überwachung allgemein das Entstehen von Schäden im Kreditwesen zu verhindern. Das KWG leistet einen Beitrag zur Stabilisierung des nationalen und internationalen Finanzsystems. Adressat und Schutzzweck sind demnach andere als bei § 91 II AktG, der die wirtschaftliche Stabilität von Aktiengesellschaften zum Schutz der Anleger im Blick hat. Dennoch kann trotz der nicht zwingenden Identität von Aktiengesellschaften und Banken- sowie Finanzdienstleistern eine Parallele zwischen den als Adressaten genannten Geschäftsleitern in § 25a I KWG und dem Vorstand des § 91 II AktG gezogen werden. Das Verwaltungsgericht Frankfurt hebt eine gemeinsame gesetzgeberische Intention der beiden Vorschriften hervor.⁴³ Für eine einheitliche Anwendung und Auslegung von § 25a KWG und § 91 II AktG plädiert überwiegend auch die Literatur.⁴⁴ Es stellt sich damit die Frage, ob § 25a I KWG auch IT-spezifische und damit SDI-bezogene Maßnahmen umfasst. Dies spräche dafür, gleiches für § 91 II AktG anzunehmen. Hintergrund von § 25a I 3 Nr. 4 KWG ist die Dominanz von IT-Produkten in allen Geschäftsbereichen der Kredit- und Finanzdienstleistungsinstitute, die zu einer immer stärkeren Abhängigkeit von der Betriebsbereitschaft der IT-Systeme der Institute und der IT-Systeme Dritter führen. Entscheidend bei der Auslegung des § 25a I KWG ist die internationale Übereinkunft „Basel II“ des Basel Committee on Banking Supervision für die Eigenkapitalvorsorge der Kreditinstitute.⁴⁵ Principle 8 der Empfehlungen des Basel Committee verlangt: „an effective internal control system requires that there are reliable information systems in place that cover all significant activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently and supported by adequate contingency arrangements.“⁴⁶ Zur weiteren Konkretisierung wird ausgeführt: „Electronic information systems and the use of information technology have risks that must be effectively controlled by banks in order to avoid disruptions to business and potential losses.“ Basel II verpflichtet somit mittelbar, indem Unternehmen bei nicht ausreichendem Risikomanagement beim Rating der Finanzinstitute schlechter

⁴² *Fleischer* ZIP 2003, 1 ff.

⁴³ VG Frankfurt am Main, Urteil vom 8. Juli 2004 – 1 E 7363/03 (1) = WM 2004, 2157 (2160); *von Holleben/Menz* CR 2010, 63 (65).

⁴⁴ *Bürkle* WM 2005, 1496 (1497); *Preußner* NZG 2004, 303 (305);

Witte/Hrubesch BB 2004, 725 (730); vorsichtiger *Spindler* in *Fleischer*, Handbuch des Vorstandsrechts, § 19 Rn 19.

⁴⁵ Basel II ist über die RL 2006/48/EG und RL 2006/49/EG Maßstab nationalen Rechts geworden (dazu *Schmidl* in *Hauschka/Moosmayer/Lösler*, Corporate Compliance, § 28 Rn 621) und durch das Gesetz zur Umsetzung der neu gefassten Bankenrichtlinie und der neu gefassten Kapitaladäquanzrichtlinie in Verbindung mit der Solvabilitätsverordnung (SolvV) und der überarbeiteten Großkredit- und Millionenkreditverordnung (Gro-MiKV) in deutsches Recht umgesetzt worden.

⁴⁶ www.bis.org/publ/bcbs40.pdf (letzter Abruf 19. September 2017).

abschneiden und schlechtere Kreditkonditionen angeboten bekommen. Weiteren Aufschluss über die Auslegung des § 25a I KWG geben die „Mindestanforderungen an das Risikomanagement (BA)“, die als Verwaltungsanweisungen durch Rundschreiben der Bundesanstalt für die Finanzdienstleistungsaufsicht (BaFin) veröffentlicht wurden und auf der Basis von § 25a KWG einen ganzheitlichen Rahmen für das Management aller wesentlichen Risiken vorgeben. Insbesondere AT 7.2 (technisch-organisatorische Ausstattung) fordert unter Nr. 2, dass die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Hieraus folgt, dass erstens § 25a I KWG IT-sicherheitsrechtliche Maßnahmen mit erfasst, worunter auch SDI fallen. Die Schrittmacherrolle des § 25a KWG spricht in systematischer Auslegung der Vorschrift zweitens dafür, gleiches auch für § 91 II AktG anzunehmen.

Die historische sowie die teleologische Auslegung gelangen wie die zuvor ausgeführte systematische Auslegung zu einer ganz ähnlichen Anwendbarkeit des § 91 II AktG auch für SDI, obwohl diese in der Vorschrift nicht ausdrücklich benannt werden. Im Hinblick auf die historische Auslegung hat der Gesetzgeber § 91 Abs. 2 AktG 1998 mit dem „KonTraG“⁴⁷ eingeführt. Gemäß der Begründung zum Gesetzentwurf hat das Gesetz in erster Linie negative Änderungen der Vermögens-, Ertrags- oder Finanzlage der Gesellschaft im Blick.⁴⁸ Die Gesetzesbegründung sagt zwar nichts konkret darüber aus, welche auslösenden Faktoren für die Verschlechterung der Finanzlage bekämpft werden sollen. Daraus ist aber zu schließen, dass der Gesetzgeber sich nicht auf bestimmte Gefahren festlegen wollte. Vielmehr wollte er Aktiengesellschaften gegen jede Art von Gefahr wappnen, die sich gravierend auf deren wirtschaftliche Stabilität auswirken kann. Zwar mögen damals IT-spezifische Risiken noch keine derart bedeutende Rolle gespielt haben wie heute. Dies schließt aber nicht aus, solche Risiken heute in den Regelungsbereich der Norm einzubeziehen. Der beabsichtigte Schutz von Aktiengesellschaften vor Bestandsgefährdungen bedingt im Gegenteil, alle nur möglichen Gefahrenlagen gleichermaßen zu berücksichtigen, um die in der Gesetzesbegründung ausgedrückten Schutzziele zu erreichen. Neben Gesetzesverstößen im Allgemeinen sah der Gesetzgeber eine besondere Gefahr in Unrichtigkeiten in der Buchführung und Rechnungslegung.⁴⁹ Die Buchführung ist heute aber üblicherweise IT-gestützt. Das wiederum spricht auch dafür, dass § 91 II AktG nach dem Willen des Gesetzgebers ein Früherkennungssystem verlangt, das IT-spezifische Risiken mit in den Blick nimmt. Die Gesetzesbegründung streitet somit ebenfalls dafür, dass § 91 II AktG auch zu IT-Sicherheitsmaßnahmen verpflichtet.

Die teleologische Auslegung berücksichtigend ergibt sich aus den in der Gesetzesbegründung formulierten Zielen eine Brücke zu Sinn und Zweck der Norm. § 91 II AktG will Entwicklungen verhindern, welche die Aktiengesellschaft in ihrem Bestand gefährden. Unter „Entwicklungen“ werden – im Gegensatz zu den nicht gemeinten Risikozuständen – Veränderungen und Prozesse verstanden.⁵⁰ Das Gesetz definiert nicht, welche konkreten Gefahren es erfassen will. Die Vorschrift zielt aber – wie gezeigt – gerade auf solche Veränderungen ab, die sich auf die Vermögens-, Ertrags- oder Finanzlage der

⁴⁷ Gesetz zur Kontrolle und Transparenz im Unternehmensbereich vom 27. April 1998 (BGBl. I S. 786); RegE KonTraG BT-Drs 13/9712.

⁴⁸ Begründung RegE KonTraG BT-Drs 13/9712, S. 15.

⁴⁹ So *Nolte/Becker* BB-Special 5, 2008, 23 mit Verweis auf BT-Drs 13/9712, S. 15.

⁵⁰ *Spindler* in Goette/Habersack/Kalss, MüKo-AktG, 4. Aufl., § 91 Rn 20.

Gesellschaft wesentlich auswirken können. Damit wird insbesondere das Risiko einer Insolvenz erfasst. Denkbar ist auch, dass eine Aktiengesellschaft durch IT-spezifische Risiken bestandsgefährdend⁵¹ bedroht wird. Daher liegt es nahe, solche Gefahren in die Norm des § 91 II AktG mit einzubeziehen. Die „enorme Abhängigkeit moderner Unternehmen von ihrer IT“ macht es gerade erforderlich, IT-Sicherheit in § 91 II AktG zu integrieren. Angesichts der Vielzahl an möglichen Gefahren, die mit der Implementierung moderner Informationstechnologien einhergehen, stellt sich folglich eher die Frage, weshalb § 91 II AktG nicht auch vor IT-Risiken schützen sollte. Insbesondere der Ausfall von IT-gestützten Steuerungs- oder Buchführungssystemen kann bereits innerhalb weniger Tage zu einem größeren Schaden für das Unternehmen führen.⁵² Die Nichtverfügbarkeit der IT kann Produktionsausfälle und Handlungsunfähigkeit eines Unternehmens bedeuten. Auch Verlust und Manipulation von Daten bedingen eine Pflicht zur Sicherung, insbesondere soweit sich unternehmerisches Know-how in dem Datenbestand eines Unternehmens widerspiegelt. Bei Verlust wichtiger betrieblicher Daten drohen irreversible Schäden. Gerade mittlere und größere Unternehmen sind bei der Risikoanalyse bezüglich der Bestandsdaten, ordnungsgemäßen Buchführung und Rechnungslegung auf IT-Sicherheit angewiesen. Eine mittelbare Bedrohung mag auch darin liegen, dass bei IT-sicherheitsbezogenen Mängeln nicht selten automatisch und als Begleitschaden ein Reputationsverlust eintritt. Laut einer Studie des BSI ist die IT-Sicherheit zu einem entscheidenden Faktor in der Wertschöpfungskette geworden, der die Risikoexposition eines Unternehmens, seine Kreditwürdigkeit und seine Haftpflichtversicherungsprämien im Zweifelsfall negativ beeinflussen kann.⁵³ Dies alles spricht dafür, dass die geeigneten Maßnahmen im Sinne von § 91 II AktG zur Abwehr von IT-Risiken dienen und zur Ergreifung entsprechender Maßnahmen, worunter auch SDI fallen können, verpflichtet.

Es stellt sich die Frage, ob das für das Aktienrecht gefundene Ergebnis auch für das Recht der Gesellschaft mit beschränkter Haftung gilt. Der normative Anker ist § 43 I GmbHG, der anordnet, dass „die Geschäftsführer in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden (haben)“. Der überwiegende Teil der Literatur⁵⁴ nimmt eine Übertragung der Pflichten aus § 91 II AktG auf alle dem GmbHG unterfallenden Gesellschaften an. Die Gegenauffassungen sprechen sich dafür aus, § 91 II AktG nicht⁵⁵ oder nur eingeschränkt⁵⁶ für die Pflichtenbestimmung der Geschäftsführer heranzuziehen. Gegen eine Übertragung der aktienrechtlichen Pflichten auf den Geschäftsführer spricht zunächst, dass das GmbHG keine § 91 II AktG entsprechende Norm enthält. Hätte der Gesetzgeber aber dem Vorstand und dem Geschäftsführer die gleichen Pflichten auferlegen wollen, hätte er eine solche Norm schaffen können. Dieses Argument lässt sich aber mit Hinweis auf den Gesetzgeber selbst entkräften. Der Gesetzgeber nimmt eine Ausstrahlungswirkung des § 91 II AktG an und hält die Analogie für

⁵¹ Vgl IDW Prüfungsstandard 340, WPg 1999, 658 und IDW Prüfungsstandard 330, WPg 2002, 1167.

⁵² *Schmidl* in Hauschka/Moosmayer/Lösler, Corporate Compliance, § 28 Rn 48; *Spindler*, Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären, Rn 342.

⁵³ *Spindler*, Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären, Rn 2.

⁵⁴ Zum Meinungsstand *Fleischer* in Fleischer/Goette, MüKo-GmbHG, 2. Aufl., § 43 Rn 61 mwN.

⁵⁵ *Fleischer* in Fleischer/Goette, MüKo-GmbHG, 2. Aufl., § 43 Rn 61; *Merkt* ZIP 2014, 1705 (1713).

⁵⁶ *Drygala/Drygala* ZIP 2000, 297; *Gaycken/Karger* MMR 2011, 3 (8); *Hommelhoff* in Berger/Ebke/Elsing u.a., FS Sandrock, S. 377 ff.

derart klar, dass er auf eine gesonderte Regelung im GmbHG verzichtete.⁵⁷ Gegen eine analoge Anwendung wird auch angeführt, dass § 91 II AktG allein auf die Aktiengesellschaft zugeschnitten sei. Die Aktiengesellschaft unterscheidet sich aber von der Gesellschaft mit beschränkter Haftung durch ihre Organisation mit einem von den Anlegern unabhängigen Vorstand. Dies verbiete eine Übertragung auf das Recht der Gesellschaft mit beschränkter Haftung, bei der die Geschäftsführer den Gesellschaftern untergeordnet seien. Die Gesellschafter seien wegen ihrer Weisungsbefugnis nicht schutzwürdig.⁵⁸ Teils finden sich Hinweise auf eine Überregulierung der kleinen und mittleren Gesellschaften mit beschränkter Haftung. Sie zur Einrichtung eines Risikomanagementsystems zu verpflichten, sei nicht angemessen.⁵⁹ Für eine Analogie spricht neben der Gesetzesbegründung indessen eine einheitliche Auslegung gesellschaftsrechtlicher Pflichten der Unternehmensführungen. Die IT-spezifischen Risiken sind im Allgemeinen für Unternehmen gleich, unabhängig von ihrer gesellschaftsrechtlichen Organisation. Das Pflichtenprogramm für die Unternehmensleitung hinge sonst vom Zufall ab, ob das Unternehmen als Gesellschaft mit beschränkter Haftung oder als Aktiengesellschaft organisiert ist. Dass dabei auf den Einzelfall abzustellen ist und für kleine Gesellschaften mit beschränkter Haftung andere Maßstäbe gelten als für große, versteht sich von selbst. Selbst die Gegner einer generellen Analogie nehmen eine Übertragung von § 91 II AktG auf große Gesellschaften mit beschränkter Haftung an, soweit sie mit der Aktiengesellschaft vergleichbar sind.⁶⁰ Dies entspricht auch der Wertung des Gesetzgebers, der die Ausstrahlungswirkung des § 91 II AktG auf Gesellschaften nach dem GmbHG annimmt, „soweit Größe, Komplexität ihrer Struktur und die Geschäftstätigkeit es erforderten“.⁶¹ Auch das folgende systematische Argument spricht für eine Gleichbehandlung: § 43 I GmbH konkretisiert den Sorgfaltsmaßstab des § 276 II BGB für die Gesellschaft mit beschränkter Haftung. Danach hat der Geschäftsführer die Sorgfalt eines ordentlichen Geschäftsmannes zu beachten. Auch § 93 I AktG normiert, wenngleich sprachlich minimal unterschiedlich, die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters. Da § 91 II AktG wie zuvor festgestellt wiederum eine Klarstellung und Konkretisierung der allgemeinen Vorstandspflichten aus § 93 AktG ist, spricht auch die inhaltliche Übereinstimmung von § 43 I GmbHG und § 93 I 1 AktG dafür, die Pflichten des § 91 II AktG auf die GmbH-Geschäftsführer zu übertragen – womit die SDI auch in das Recht der Gesellschaft mit beschränkter Haftung Einzug halten und damit einen flächendeckenden wie branchenübergreifenden Anwendungsfall eröffnen. Nach alledem ist davon auszugehen, dass § 91 II AktG analog auch für die Pflichten des Geschäftsführers aus § 43 I GmbHG gilt. Der Geschäftsführer hat danach entsprechend § 91 II AktG ein Risikomanagement für IT-Sicherheitsrisiken unter Berücksichtigung von SDI zu implementieren.

⁵⁷ Begründung RegE KonTraG BT-Drs 13/9712, S. 15; dagegen *Hommelhoff* in Berger/Ebke/Elsing u.a., FS Sandrock, S. 377.

⁵⁸ *Hommelhoff* in Berger/Ebke/Elsing u.a., FS Sandrock, S. 376 ff; vgl auch *Drygala/Drygala* ZIP 2000, 297 (301).

⁵⁹ *Drygala/Drygala* ZIP 2000, 297 (300 f).

⁶⁰ Vgl *Drygala/Drygala* ZIP 2000, 297 (302); *Gaycken/Karger* MMR 2011, 3 (8); *Hommelhoff* in Berger/Ebke/Elsing u.a., FS Sandrock, S. 378 ff; der Sache nach auch *Fleischer* in *Fleischer/Goette*, MüKo-GmbHG, 2. Aufl., § 43 Rn 61.

⁶¹ Begründung RegE KonTraG BT-Drs 13/9712, S. 15; *Terlau/Hürten* in Römermann, AnwHdb GmbH-Recht, Teil C § 10 Rn 66.

2.4.3 SDI als Impulsgeber in den Bereichen IT-Sicherheit und Datenschutz: IT-SiG, EU DS-GVO, eIDAS-VO

Soweit SDI durch spezielle Regelungen adressiert werden, dienen sie vornehmlich der Beförderung sowohl der IT-Sicherheit wie auch des Datenschutzes. Seit dem Jahr 2015 wurden in diesen Bereichen umfangreiche neue Regularien geschaffen, im Kern sind hier das IT-Sicherheitsgesetz (IT-SiG), die eIDAS-Verordnung und die EU Datenschutz-Grundverordnung (EU DS-GVO) zu nennen. Letztere entfaltet ihre Wirkkraft zum 25. Mai 2018, weshalb sich zahlreiche Unternehmen, die mit der Verarbeitung von personenbezogenen Daten befasst sind, zurzeit inmitten der Umsetzung des neuen europäischen Datenschutzrahmens befinden. Datenschutz und IT-Sicherheit stehen dabei, soweit es SDI anbelangt, miteinander in Einklang, denn ohne hinreichend abgesicherte IT-Systeme kann es auch keinen Datenschutz geben. Das IT-SiG zum Beispiel trifft Anforderungen vorwiegend für die Betreiber von Kritischen Infrastrukturen (sowie durch die EU NIS-RL festgesetzt auch für die Anbieter von Digitalen Diensten), die unter Qualitäts- und Quantitäts Gesichtspunkten eine herausragende Stellung in der Versorgung der Bevölkerung einnehmen. Kritische Infrastrukturen sind grundsätzlich solche, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen zugehörig sind und darüber hinaus den Schwellenwerten unterfallen, die durch die BSI-KritisV bestimmt werden. Wer als Betreiber einer Kritischen Infrastruktur identifiziert wurde, den trifft nicht nur die Verpflichtung, schwerwiegende IT-Sicherheitsvorfälle zu melden, sondern auch, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit derjenigen IT-Systeme zu treffen, die für das Funktionieren der betriebenen Kritischen Infrastruktur maßgeblich sind. Dabei greift das Gesetz auch hier wieder auf einen unbestimmten Rechtsbegriff, nämlich den „Stand der Technik“, zurück, der von den Betreibern grundsätzlich einzuhalten ist. Dieser Stand der Technik umfasst auch die technische Anforderung der Einrichtung einer hinreichend abgesicherten Kommunikationsstruktur, soweit in diesem Zusammenhang eine reine M2M-Kommunikation stattfindet, wo SDI maßgeblich sind.

Die EU DS-GVO geht an dieser Stelle weiter, indem hier nicht nur die so gesehen abstrakte Aufrechterhaltung der Funktionsfähigkeit von Computern, Anlagen und Maschinen betrachtet wird, sondern die informationelle Selbstbestimmung des Individuums, dessen personenbezogene Daten verarbeitet werden, zu verwirklichen ist. Die EU DS-GVO, die dabei die alte Datenschutzrichtlinie der Europäischen Union aus dem Jahre 1995 ersetzt, soll den Datenschutz insoweit auf das Niveau des 21. Jahrhunderts befördern. Zur Wahrung eines effektiven Datenschutzes gehört jedoch nicht nur die gelebte Selbstbestimmung des Betroffenen, vor allem verkörpert durch die Einwilligungserteilung in eine Datenverarbeitung sowie durch einen Katalog von umfassenden Betroffenenrechten, sondern genauso das Vertrauen darin, dass einmal erhobene und auf IuK-Systemen gespeicherte Daten hinreichend sicher verarbeitet werden. Der Datenschutz umfasst somit zwangsläufig auch das Element der Datensicherheit. Speziell hierfür enthält die neue Grundverordnung eine eigenständige Regelung in Art. 32, die den Betreiber verpflichtet, für die Verarbeitung der personenbezogenen Daten ein angemessenes Schutzniveau zu gewährleisten. Die dabei zu treffenden Maßnahmen sollen unter anderem die Fähigkeit einbeziehen, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der IT-Systeme sicherzustellen. Auch hier werden somit, trotz eines unterschiedlichen Regelungsbereiches, in technischer Hinsicht ähnliche Vorgaben wie auch schon für die IT-Sicherheit der Kritischen Infrastruktur getroffen. Auch hier ist somit ein zukünftiges Einsatzfeld von SDI zu verorten.

Nicht zuletzt wird die Thematik der SDI durch die eIDAS-Verordnung der EU aufgegriffen, wobei hier die elektronische Identifizierung im digitalen Raum im Mittelpunkt steht. Ziel ist dabei, ein ordnungsgemäßes Funktionieren des europäischen Binnenmarktes zu gewährleisten und gleichzeitig ein angemessenes Sicherheitsniveau bei elektronischen Identifizierungsmitteln und Vertrauensdiensten sicherzustellen. Dazu legt die eIDAS-Verordnung die Bedingungen fest, unter denen die EU-Mitgliedstaaten elektronische Identifizierungsmittel für natürliche und juristische Personen anerkennen. Die Verordnung bestimmt darüber hinaus, welche Vorschriften für Vertrauensdienste und insbesondere für elektronische Transaktionen gelten. Nicht zuletzt bildet der europäische Rechtsakt einen umfassenden Rahmen für elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Dokumente, Dienste für die Zustellung von elektronischen Einschreiben und von Zertifizierungsdiensten für die Website-Authentifizierung. All diesen Diensten ist ebenso die Gewährleistung angemessener technischer und organisatorischer Schutzanforderungen immanent, will man eine wert- und nachhaltige Entwicklung der neuen Konzepte gewährleisten. SDI sind somit auch hier unerlässlich. Dies bestimmt die eIDAS-Verordnung, indem auch sie auf den „Stand der Technik“ verweist, der SDI beinhaltet.

2.4.4 Zusammenfassung / Rückschlüsse / Interpretation / Resümee

Im Ergebnis lässt sich im Rahmen einer juristischen Betrachtung von SDI festhalten, dass die Thematik zwar bereits seit Jahren bekannt ist und auch von Seiten der Rechtspolitik sowie von Seiten des Gesetzgebers behandelt wird, gleichwohl aber noch nicht vollumfänglich ausgeschöpft und exploriert wurde. Vor allem auf die Aspekte Security und Industrie 4.0 bezogen ist die rechtliche Befassung noch ausbaufähig – dies insbesondere vor dem Hintergrund einer steigenden Relevanz von Cybersicherheit, innerhalb derer mit dem IT-Sicherheitsgesetz (IT-SiG) von 2015 sowie mit der Netz- und Informationssicherheitsrichtlinie (NIS-RL) der EU aus dem Jahre 2016 und dem entsprechenden nationalen Umsetzungsgesetz von Ende Juni 2017 neue Verpflichtungen für zahlreiche Unternehmen geschaffen wurden, sodass hier auch ein erheblicher wirtschaftlicher Handlungsbedarf besteht (dieser wird unter anderem durch den Entwurf der EU Cybersecurity-Verordnung von 2017 adressiert und weiter aufgegriffen). Soweit mittel- und langfristige keine weiteren eigenständigen, speziell auf die Betriebs- und Anlagensicherheit bezogenen, gegebenenfalls auch kodifizierten rechtlichen Regelungen, geschaffen werden, wird es vornehmlich Aufgabe der technischen Normung und Standardisierung sein, bestehende Regelungslücken zeit- und praxisnah sowie flexibel auszufüllen, um Anwender- und Rechtssicherheit bei der Realisierung neuer Technologien in Deutschland und Europa zu schaffen. Wie auch schon für das IT-Sicherheitsgesetz wird es bei den juristisch-technischen Betrachtungen in einem erheblichen Maße auf die Auslegung von unbestimmten Rechtsbegriffen und Generalklauseln wie dem viel zitierten „Stand der Technik“ ankommen, um die optimale Übertragbarkeit abstrakter gesetzlicher Anforderungen in die technische Anwendungspraxis sicher zu stellen. Dass eine entsprechende Auslegung und somit eine Unterbringung von sicheren digitalen Identitäten auch in gesetzlichen Regelwerken möglich ist, die SDI (noch) nicht explizit adressieren, wurde zuvor im Rahmen der Auslegung von § 91 II AktG sowie von § 43 I GmbHG aufgezeigt.

3 Ergebniszusammenführung zur Sach- und Prozessbeschreibung & Beispiele

Zu Projektbeginn wurde davon ausgegangen, dass

- es bezüglich des Themas Sichere Digitale Identitäten einige Insellösungen gibt,
- es zum Erlangen einer größeren Interoperabilität und eines gesamtgesellschaftlichen Mehrwerts Harmonisierungsmöglichkeiten geben könne,
- damit ggf. zusätzliche politische, rechtliche als auch technologische Herausforderungen verbunden sein würden und
- es für einen abgrenzbaren Sachverhalt normungsrelevante Aspekte zu identifizieren galt.

Im Rahmen dieser Annahmen stand auch gelegentlich die Vermutung oder die Hoffnung, es könne eine zentrale technische (eine annähernde „One-Fits-All“) Lösung geben oder selbige könne entwickelt werden. Der Gesamtsachverhalt und seine Zusammenhänge zeigten jedoch in der vorliegenden tiefergehenden ganzheitlichen Betrachtung, dass es eine One-Fits-All-Lösung nicht gibt.

Der Recherche- und Analyseprozess macht deutlich, dass das Thema Sichere Digitale Identitäten vielschichtiger, komplexer und weitreichender ist, als vermutet. Die Vielfalt an Entitäten, also Dingen, für die Digitale Identitäten erzeugt werden, an individuellen Anwendungsfällen und den jeweiligen Bedürfnissen, Intentionen und Rahmenbedingungen sowie an unterschiedlichen zu berücksichtigenden möglichen Handlungsebenen und Varianten zur Erzeugung von Sicheren Digitalen Identitäten sind immens. Dies wird verstärkt durch unterschiedliche Konstellationen der möglichen Ausprägungen oder Lösungsvarianten in den verschiedenen, aber interdependenten Handlungsfeldern. Darüber hinaus zeigte der Analyseprozess, dass das Verständnis davon, was Sichere Digitale Identitäten sind, in zweierlei Dimensionen neu zu definieren ist.

Das folgende Kapitel führt die erarbeiteten Informationen im Sinne einer Sach- und Prozessbeschreibung des Themas und der diesbezüglich im Analyseprozess herausgearbeiteten Dimensionen zusammen. Die Auffächerung der Betrachtungsebenen und Identifizierung der unterschiedlichen Handlungsebenen dient als Grundlage zum Erfassen des Gesamtsachverhalts und als Voraussetzung für das Entwerfen einer sinnvollen Strategie zur Gestaltung des Themas im Ganzen und diesbezüglicher Handlungsempfehlungen im Speziellen.

Im Zentrum der Themenanalyse steht eine Systematisierung anhand des klassischen Lebenszyklus Digitaler Identitäten (angelehnt an ISO/IEC 29115). Um ihn herum wird in Kapitel 3.2 sukzessive ein Schaubild zum Gesamtsachverhalt aufgebaut. Bevor aber in den Unterkapiteln 3.2.1 bis 3.2.7 die verschiedenen konkreten Schritte des Lebenszyklus genauer betrachtet werden, werden in Kapitel 3.1 die im Analyseprozess herausgearbeiteten typischen Perspektiven und Dimensionen eruiert. Sie stellen die Betrachtung des Sachverhalts und der einzelnen Schritte des Lebenszyklus in einen logischen Kontext, machen sie detaillierter und differenzierter und erweitern sie um begleitende Sachverhalte.

Das in Kapitel 3.2 entstehende Schaubild zum Gesamtsachverhalt bietet im Anschluss einen Überblick, der die Vielschichtigkeit aufzeigt, so zu einem besseren Verständnis der Zusammenhänge zwischen den verschiedenen Handlungsfeldern beiträgt und gleichzeitig Ansatzpunkte für Transfer- und oder

Zusammenarbeit, für Harmonisierung, Regulierungs- oder Forschungsbedarf usw. adressieren lässt. Jegliche bestehende Aktivität, Initiative, Forschungsvorhaben, vorhandene Lösungen, bestehende Normen und Normungsvorhaben oder bspw. auch der Wirkungsfokus von Gesetzen lassen sich auf diesem Schaubild verorten.

3.1 Relevante Dimensionen des Gesamtsachverhalts

Im Analyse- und Rechercheprozess ergaben sich unterschiedliche überlagerte Perspektiven, die Themen bzw. kausale Zusammenhänge oder intentionale Sichtweisen adressieren, welche für das Verständnis des Gesamtsachverhalts bzw. die Entwicklung von Handlungsempfehlungen grundlegend sind. Sie führen dabei zu einer weiteren aber verständlicheren Diversität des Themas, der Herausforderungen, der Identitätslösungen sowie des Handlungsfeldes in dem es gegebenenfalls einer Harmonisierung, Systematisierung, Priorisierung, Bewertung, Adaption etc. bedarf. In dem Schaubild des Gesamtsachverhalts in Kapitel 3.2 und 3.3 werden diese Dimensionen dann mitadressiert und helfen die zu verortenden Aktivitäten und Initiativen etc. zusätzlich zu klassifizieren.

3.1.1 Die zwei Interessenspole – Schutz des Identitätsgebers und Identitätsabfragenden

Die Expertenbefragung hat gezeigt, dass das Thema Sichere Digitale Identitäten grundsätzlich aus zwei Richtungen interpretiert bzw. verstanden und angegangen wird. Den Ansätzen und Umsetzungen in Forschung und im Markt für Identitätslösungen liegt in der Regel auch zunächst eine der beiden Richtungen zu Grunde. Die Bedeutung der Identitätslösungen adressierenden Projekte und der dahinter stehenden Stakeholder Gruppen ist aus Richtung beider Perspektiven vergleichbar.

Die eine Sicht ist die des „Identitätsprüfenden “ bzw. die des „Identitätsabfragenden “, der sich sicher sein möchte, dass das Gegenüber, mit dem er interagiert, auch das ist (oder für das steht und damit verbunden ist), was es vorgibt zu sein. Aus dieser Sicht geht es bei Sicheren Digitalen Identitäten zunächst darum, das Gegenüber sicher identifizieren zu können und im Verlauf der Interaktion, sicher sein zu können, dass das Gegenüber nicht korrumpiert wurde.

Die andere Sicht ist die des „Identitätsinhabers “ bzw. die des „Identitätsgebers “. Er, bzw. der für seine Interessen eintretende Akteur, versteht unter Sicherer Digitale Identität die Sicherheit der digitalen Sammlung von Attributen / Informationen, also der digitalen Identität, der Entität - im Sinne des Schutzes vor unlauterer Verwendung derselben.

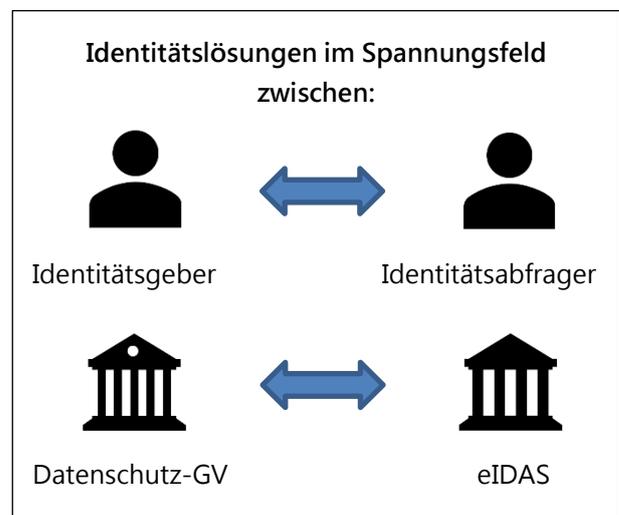


Abbildung 16 – Identitätsgeber und -abfrager

Man könnte fast davon sprechen, dass die Identitätslösungen im Spannungsfeld zwischen diesen beiden Polen stehen. Die beiden Sichtweisen sind sich vom Prinzip her aber eben nicht zwingend gegenüberliegend bzw. konträr. Beide Interpretationen bzw. Sichtweisen sind nicht nur legitim, sondern für eine Gestaltung sowohl einzelner Lösungen, als auch insbesondere bei der strategischen Betrachtung und Entwicklung des Gesamtsystems, zwingend notwendig.

Die Bipolarität zeigt sich auch in den gesetzlichen Herangehensweisen. Die eIDAS-Verordnung adressiert vor allem die sichere Identifikation der Beteiligten und bedient somit primär die Sicht des „Identitätsprüfenden“ bzw. „-abfragenden“. Die Datenschutzgrundverordnung hingegen adressiert vom Prinzip her die Sicht und Belange des „Identitätsgebenden“. (vgl. Kapitel 2.4)

Der Verdacht liegt nahe, dass sich die zweite Perspektive, die des Identitätsgebenden, vornehmlich auf Identitätslösungen zur Entität „Mensch“ beziehen – im Sinne der personenbezogenen Daten – bezieht. Dies trifft aber nicht zu und wurde im Analyseprozess mehrfach bestätigt. Als zentrales Beispiel mag hier auf den Ansatz des groß angelegten Forschungsprojekts Industrial Data Space⁶² verwiesen werden. Des Weiteren sei auf die Problematik verwiesen, dass Identitätsmanagement auch von Organisationen angeboten wird, deren primäres Geschäftsmodell auf dem Sammeln von Daten und daraus generiertem Mehrwert, wie bspw. durch Verkauf von individualisierter Werbung, basiert (vgl. Beispiel in Kap. 3.4.4). Zudem wird die Notwendigkeit beider Sichtweisen verschärft, durch die Möglichkeit i.S.v. BigData aus zusammengeführten Einzeldaten eine deutlich höhere Informationstiefe über Personen, Unternehmen etc. zu generieren. Die Sichtweise des Identitätsgebenden ist also nicht auf die Entität Mensch zu reduzieren, sondern bekommt mit der voranschreitenden Digitalisierung wachsende Bedeutung für Entitäten wie Maschinen, Devices, Software, Systeme etc. Schlussendlich werden beide Perspektiven von dahinter stehenden natürlichen oder juristischen Person adressiert. Auf der einen Seite geht es um personenbezogene Daten, auf der anderen Seite um gegebenenfalls vertrauliche Unternehmensdaten. Der Analyseprozess lässt vermuten, dass das im Hinblick auf die Digitalisierung bereits sehr umfassend behandelte Thema „Umgang mit personenbezogenen Daten“ durchaus veritablen Input für das Thema Identitätslösungen auch im Bezug auf Unternehmensdaten innehat.

„...bei einem unnötigen Datenfluss bei Identitätslösungen von Maschinen ist sowohl das Know-how in Gefahr, aber eben auch das Know-what eine Gefahr. Know-what in dem Sinne, dass Detailinformationen über das Unternehmen, bspw. wie viele Chipsätze eine Maschine bereits produziert hat etc., unnötig oder fahrlässig weitergegeben werden.“

Zitat aus den Fragebögen /
Expertenkonsultationen

Zu Beginn des Projektes wurde folgende Definition von Sicheren Digitalen Identitäten postuliert: *„Sichere digitale Identitäten sind Techniken, die sicherstellen, dass eine Entität auch die ist, die sie vorgibt zu sein.“* Vor dem Hintergrund des gerade geschilderten legitimen und notwendigen bipolaren Verständnisses kann allerdings an dieser Definition nicht festgehalten werden. Sie repräsentiert allein die Sicht des Identitätsabfragenden. Um auf Identitätslösungen und eine diesbezügliche Infrastruktur hinzuarbeiten, die im Sinne der Gesellschaft und Wirtschaft ist, bedarf es der grundsätzlichen Berücksichtigung beider Interessen und einer daraus resultierenden Abwägung im konkreten Anwendungsfall.

- **Es fehlt eine anerkannte harmonisierte Definition dessen, was unter Sicheren Digitalen Identitäten zu verstehen ist.**
- **Es mangelt an einer konzertierten Herangehensweise (bspw. Referenzarchitektur), die vom Grundsatz her beide Perspektiven (des Identitätsgebers und Identitätsabfragers) adressiert.**

⁶² IDS, Industrial Data Space ist ein Projekt der Fraunhofer Gesellschaft; <https://www.fraunhofer.de/de/forschung/fraunhofer-initiativen/industrial-data-space.html>

3.1.2 Lebenszyklus

Beim Einsatz und der Entwicklung von Identitätslösungen ist natürlich der Lebenszyklus einer digitalen Identität der zentrale und zum Verständnis elementare kausale Zusammenhang. In diesem Sinne soll er hier nur in vereinfachter Form kurz vorgestellt werden, denn in Kapitel 3.2 wird er Schritt für Schritt durchlaufen und detaillierter betrachtet. In Kapitel 3.2 und Kapitel 3.3 ist er dann zudem die Basis bzw. strukturgebend für das Schaubild des Gesamtsachverhalts. Unabhängig davon, mit welcher grundsätzlichen Intention oder mit welchem individuellen Anwendungsfall und diesbezüglichen Rahmenbedingungen oder Bedürfnissen man sich der Entwicklung oder der Auswahl einer Identitätslösung nähert, zeigt der Lebenszyklus zeigt mit seinen Schritten die relevanten zu betrachtenden und zu lösenden Sachverhalte.

Angelehnt an ISO/IEC 29115 stellt sich der Lebenszyklus wie folgt dar: Zunächst wird die digitale Identität erzeugt bzw. bereitgestellt. Hierzu werden bestimmte Attribute einer Entität durch eine Instanz festgestellt und bilden als digital abgespeicherter Datensatz die digitale Identität. Entität und digitale Identität werden dann in irgendeiner Weise (beispielsweise mittels einer einmaligen Seriennummer) miteinander verbunden. Für eine Entität könnten auch mehrere digitale Identitäten existieren. Die digitale Identität muss verwaltet, gepflegt und irgendwo abgespeichert werden. Dieser Datensatz wird in unterschiedlicher Weise in der Verbindung mit der Entität zum Steuern, Identifizieren, Zuordnen usw. genutzt. Wird die digitale Identität nicht mehr benötigt, stellt sich die Frage, ob sie gelöscht oder archiviert wird – auch, um sie gegebenenfalls reaktivieren zu können. Dies kann, muss aber nicht mit der Existenz der Entität zusammenhängen.

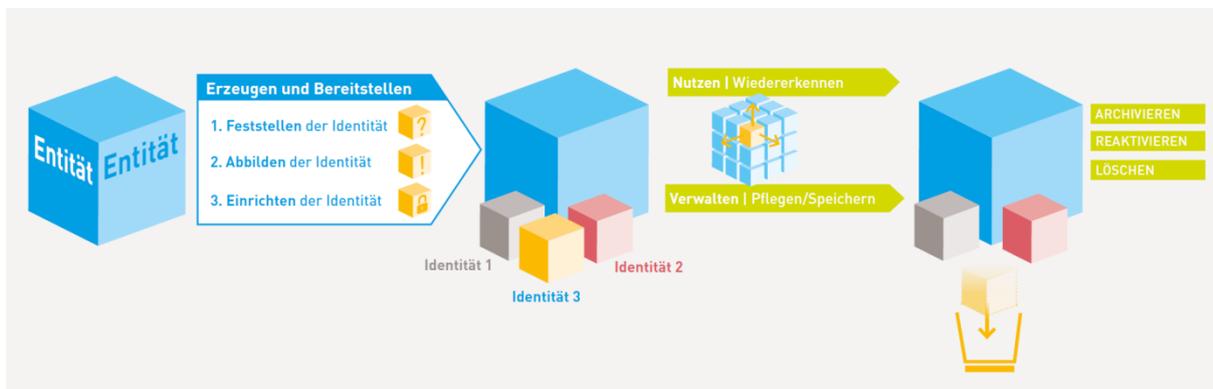


Abbildung 17 – Lebenszyklus von digitalen Identitäten

3.1.3 Einsatz- und Verantwortungsbereich von Identitätslösungen

Um den Gesamtsachverhalt, aber auch einzelne Akteure bzw. Stakeholder zu verstehen, lassen sich drei grundsätzliche Perspektiven beim Einsatz und der Entwicklung von Identitätslösungen festhalten. Auch ohne den konkreten Anwendungsfall oder Anwendungsbedarf für Identitätslösungen zu kennen, können diese Perspektiven Rückschlüsse über die Anforderungen an Identitätslösungen bzw. die Interessen und Überlegungen des jeweiligen Entscheiders zulassen. Zudem lassen sie erkennen, in welchen Bereichen bzw. in welchen generischen Situationen ggf. Harmonisierungs- oder Normungsbedarf vorhanden ist.

Die Frage hinter den drei Perspektiven ist, in welchem Verantwortungsbereich die gesuchte oder zu entwickelnde Identitätslösung eingesetzt werden soll.

3.1.3.1 Eigener Verantwortungsbereich

Insbesondere in der Wirtschaft und Industrie werden in vielen Fällen die Identitätslösungen für den eigenen Verantwortungsbereich entwickelt oder so abgeschlossen eingesetzt, dass Unzulänglichkeiten nicht relevant werden – bspw. innerhalb eines Unternehmens oder einer Abteilung. Die Schritte des Lebenszyklus einer digitalen Identität können also inhouse gestaltet werden. Bspw. ist beim Feststellen der Identität und der späteren Verifikation das komplizierte Einbinden Dritter zur Absicherung (Trust Center o.ä.) nicht notwendig. Das Ergebnis sind proprietäre Lösungen. Zudem zielen die Anforderungen an die Identitätslösung dann eher auf die interne Interoperabilität und eine Sicherheit im eigenen Verantwortungsbereich ab. Die bei vielen sichereren Identitätslösungen notwendige dritte Instanz (Verification Authority) kann kostengünstiger betriebsintern geschaffen werden. Hier wird auch auf Blockchain-Verfahren zurückgegriffen (siehe Kapitel 3.2.6.2).

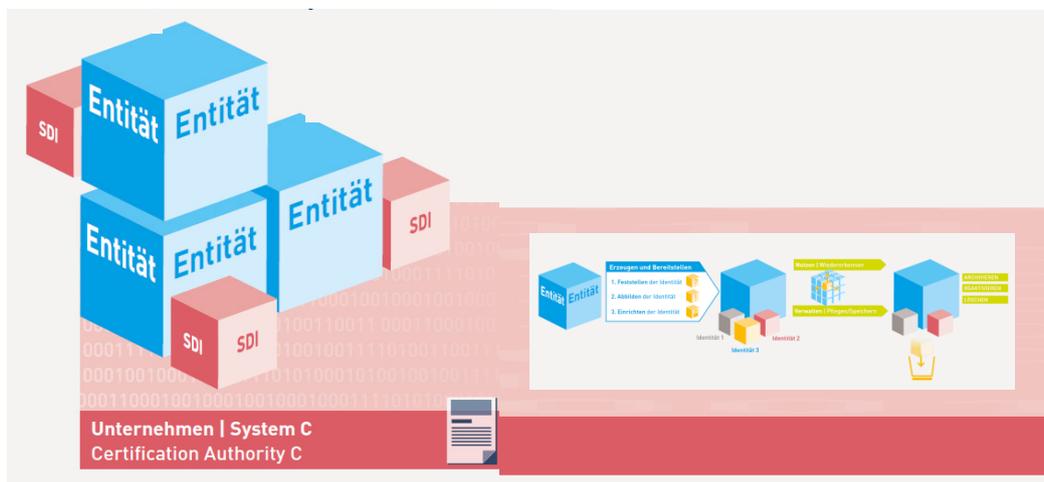


Abbildung 18 – SDI im abgeschlossenen Verantwortungsbereich

3.1.3.2 ein in den eigenen Verantwortungsbereich zu integrierendes Produkt

Eine weitere Perspektive beim Einsatz und bei der Entwicklung von Identitätslösungen und diesbezüglichen Anforderungen betrifft Identitätslösungen, die sich auf für den internen Einsatz zugekaufte Produkte, bspw. Soft- und Hardware, Maschinen, etc., beziehen. Möglich ist auch, dass diese Identitätslösungen als Komponenten innerhalb der eigenen Produkte oder Dienstleistung zum Einsatz kommen. Solche Identitätslösungen werden in den eigenen Verantwortungsbereich übernommen. Das hat zur Folge, dass Anforderungen an Identitätslösungen beim Einkauf zu berücksichtigen sind. Das Erstellen und Entstehen sowie die Art und Weise, in der Identitäten dieser Komponenten gemanagt werden, ist dabei u.U. von der ursprünglichen Produktgestaltung determiniert. Anwender und Integratoren können hier für sie fehlende oder unpassende Eigenschaften ggf. nur bedingt oder gar nicht auffangen.

- **Es bedarf bei der Produktentwicklung eines „by Design“-Ansatzes (vergleichbar „Security by Design“) bezogen auf die Gestaltung (Sicherer) Digitaler Identitäten.**

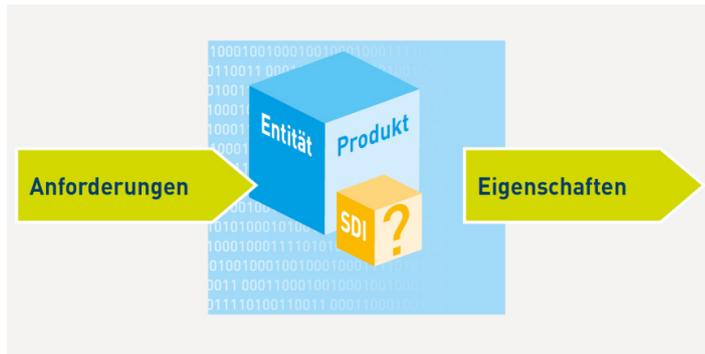


Abbildung 19 – Anforderungen an ein zu integrierendes Produkt

3.1.3.3 Interaktion von Verantwortungsbereichen

Insbesondere bei der Sicherheit von digitalen Identitäten wird zudem das jeweilige Netzwerk – sowohl das jeweilige, in dem sie geschaffen und das, in dem sie genutzt wird – in der Betrachtung eine wesentliche Rolle einnehmen. In verhältnismäßig abgeschlossenen Systemen mag die Vergabe, Sicherung und Management von Identitäten proprietär gestaltet werden können und es mögen zumindest teilweise auch unterschiedliche Standards bzw. Herangehensweisen in den Komponenten ausgeglichen und abgesichert werden können. Dies gilt für Systemkomplexe, die wiederum einzelne Produkte darstellen können, wie aber auch für große Organisationen und Konzerne. Nun ist aber die automatische Interaktion zwischen diesen ein zentrales Element der jetzigen Strömungen der Digitalisierung. Themen wie Internet of Things, Smart Cities, Connected Cars und insbesondere die system- und domänenübergreifende Interaktion der Industrie 4.0 sind davon betroffen. Wenn also die verschiedenen Domänen (Unternehmen, Produkte, Programme, Systemkomplexe, Betriebssysteme aber auch Anbieter und Branchen) die Vergabe, die Sicherung und das Management unterschiedlich gestalten, gewinnen die Identitätslösungen und diesbezügliche Herausforderungen, Lösungen und Handlungsbedarfe hinsichtlich der Schaffung von Interoperabilität, Vertrauen und Sicherheit an Bedeutung.

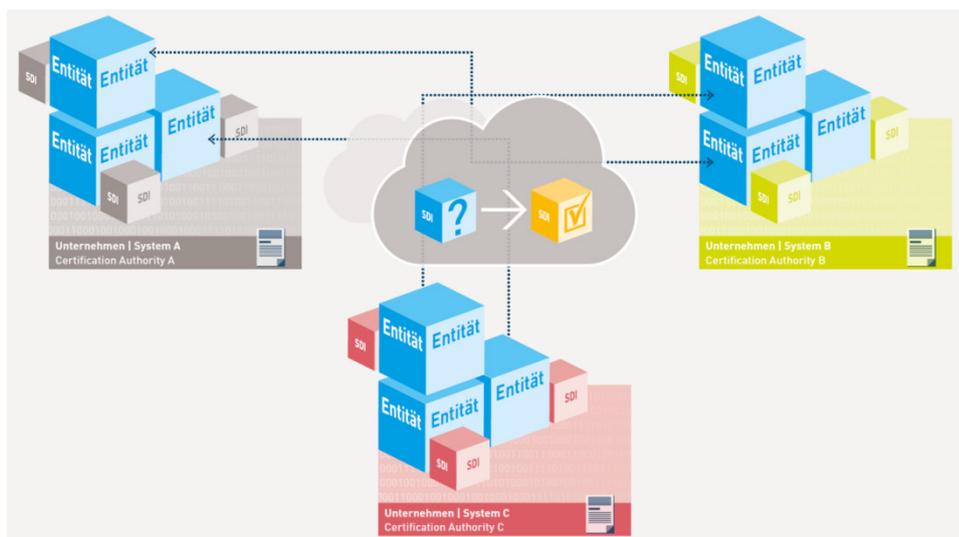


Abbildung 20 – Interaktion von Domänen

In dem Sinne, dass ein Unternehmen bisher aus der Perspektive „Identitätslösungen im eigenen Verantwortungsbereich “ (Kapitel 3.1.3.1) gedacht und gearbeitet hat, aber beispielsweise im Hinblick auf die Verarbeitung von Daten der Kunden oder aber in eine ad hoc Wertschöpfungsnetzwerke bildende Interaktion mit anderen Unternehmen eintritt, wird es für andere Unternehmen interessant zu wissen, wie das Thema digitale Identitäten in dem Unternehmen angegangen wird. Es kann in diesem Sinne dann gar nicht mehr von eigenem Verantwortungsbereich gesprochen werden. Mit dem stärkeren Zusammenwachsen durch die Digitalisierung wird das unabhängige Werk auf der grünen Wiese immer seltener.

3.1.4 Der Anwendungsfall ist maßgebend – Faktoren, die das benötigte Sicherheitslevel determinieren

Bereits aus den in 3.1.1 und 3.1.3 dargelegten Betrachtungswinkeln ergeben sich unterschiedliche Erwartungen und Anforderungen an Identitätslösungen. Im Hinblick auf den jeweilig konkreten Anwendungsfall ist dies aber noch einmal zu differenzieren. So wie Identitätsgeber und Identitätsabfrager von der Art her unterschiedliche Erwartungen und Anforderungen haben, so führt der jeweilige Anwendungsfall zu unterschiedlich starken Ausprägungen dieser Erwartungen und Anforderungen. Zudem entstehen je nach Anwendungsfall u.U. Rahmenbedingungen, die die Identitätslösung in jedem Fall bedienen muss. Bei der Betrachtung des Gesamtsachverhalts und den einzelnen Prozessschritten, ist die determinierende Rolle des Anwendungsfalls und die daher zusätzliche Steigerung der Vielfalt und Komplexität somit entscheidend für das Verständnis und die Entwicklung von Handlungsempfehlungen.

Das Anforderungsprofil an die einzusetzende Identitätslösung im jeweiligen Anwendungsfall wird neben den bereits gegebenen Rahmenbedingungen, wie etwa die Beschaffenheit der Entität, im Wesentlichen bestimmt durch die Faktoren:

- | | |
|------------------------------|--|
| 1) Schnelligkeit / Usability | ...die beim Anwendungsfall benötigt wird |
| 2) Sicherheit / Risiko | ...das mit dem Anwendungsfall zusammenhängt |
| 3) Kosten / Aufwand | ...die mit dem Einsatz der Lösung verbunden sind |

Am Ende der Entscheidungsfindung stellt sich die Frage, welches Sicherheitslevel geschaffen werden kann und muss. Man könnte vermuten, dass das höchste Sicherheitslevel für alle Anwendungsfälle optimal wäre – insbesondere mit dem Gedanken, dass sich in Verbindung mit den oben genannten Perspektiven die Frage stellt, ob zu dem Zeitpunkt, an dem die Identitätslösung bzw. die Grundlagen dafür geschaffen werden (bspw. Produktion einer Entität), die späteren Anwendungsfälle und die daraus resultierenden Anforderungen bekannt sind. Die höchst sichere Lösung ist aber oftmals nicht umsetzbar. Ist die Lösung zu teuer oder zu langsam bzw. zu unpraktisch und führt daher zu entscheidenden Nachteilen im Markt, wird sie (bei freigestellter Umsetzung) wohl eher nicht eingesetzt. Zudem ist die Frage, ob das aus Sicht des Identitätsabfragers höchst sichere Level auch die Sicherheitsbedürfnisse des Identitätsgebers berücksichtigt. Generell wissen wir zudem, dass eine absolute Sicherheit an sich nicht wirklich erreichbar ist bzw. der Gewinn an einem Stück mehr Sicherheit ab einem bestimmten Punkt oft exponentiell auf Kosten der Wirtschaftlichkeit und Praktikabilität geht. In diesem Sinne ist das mit einer Fehlfunktion der Identitätslösung verbundene Risiko (ja vielleicht auch der Möglichkeit selbiges zu versichern) bedeutend.

Geht es um eine Überweisung über 20.000 Euro, sollte vielleicht ein anderer Sicherheitslevel der Identitätsprüfung eingefordert werden, als bei 2 Euro.

Es geht also um die Frage der Verhältnismäßigkeit und es stellt sich daher weniger die Frage, was die sichere digitale Identität ist, sondern vielmehr → welche digitale Identität im jeweiligen Anwendungsfall als sicher einzustufen ist?

Hierbei finden derzeit der Staat oder der Markt die Antworten. Der Staat kann aber nicht für alle Bereiche diese Entscheidung treffen, sondern nur in einem gewissen Rahmen Anforderungen (bspw. KRITIS) stellen. Der Markt hingegen führt oft zu Lösungen, die zu Lasten der Sicherheit des Identitätsgebers oder -abfragers gehen und zwar aus Unwissenheit der Stakeholder oder aus Gründen fehlender Organisation ihrer Interessen.

➤ **Es fehlt eine gemeinsame Artikulation der Anforderungen an Identitätslösungen.**

Sie könnte zu einer entscheidenden Beschleunigung im Hinblick auf allgemein anerkannte Lösungen und Standards beitragen. Aufgrund von mehr Sicherheit bzgl. der Herangehensweisen würde es zudem den Prozess der Digitalisierung auch in Bereichen die noch „hinterherhinken “ vorantreiben (s. Kap. 4).

Welchen Sicherheitslevel es bedarf und dass nicht immer die höchst sichere Lösung notwendig bzw. zielführend ist, wird u.a. auch dadurch beeinflusst, ob im Fall der Fehlfunktion der Identitätslösung andere Mechanismen greifen können, um vor dem Risiko zu schützen. Zum Beispiel könnte der Prozess einfach beendet werden oder das Sicherheitslevel könnte durch weitere Identitätslösungen (Mehr-Faktor-Identifizierung) sukzessive erhöht werden (siehe Kapitel 3.2.6.3). Einfluss hat zudem vor welchen Gefahren die Identifikationslösung denn überhaupt primär schützen soll. Liegt dieser Gefahr z.B. ein krimineller Business Case zugrunde, dann reicht es u.U. auch die Identitätslösung zu wählen, deren Umgehung so viel Aufwand bzw. Kosten verursacht, dass der Business Case für den potentiellen Angreifer unrentabel wird.

Eine weitere dimensionale Unterteilung der Identitätslösungen ist die Frage nach dem Ziel des Anwendungsfalls. Hierbei wäre nämlich bspw. die Unterscheidung zu treffen, ob es im Anwendungsfall der Eindeutigkeit oder Eineindeutigkeit bedarf. Eindeutigkeit bedeutet, dass eine Aussage über die Entität zutrifft und die Entität sicher zu dieser Gruppe gehört (bspw. es handelt sich um einen Menschen). Eineindeutig bedeutet, dass die Entität als die eine identifizierbar wird (bspw. Herr Hans Müller, geboren am 01.01.1991 um 15:20 Uhr im St. Angel Krankenhaus, Niedereinbeck) und es also sicher keine zweite gibt. Beides kann mit unterschiedlicher Sicherheit gesagt werden. Vom Prinzip her findet sich hier auch das Spannungsverhältnis zwischen Identitätsgeber und Identitätsabfragers wieder, denn oftmals wird keine Eineindeutigkeit gebraucht (Entität ist ein Mensch über 18 = volljährig). Akteure, die sich aus Identitätsabfragender Sicht dem Sachverhalt nähern bzw. argumentieren, definieren die „Sichere Digitale Identität “ i.d.R. als eineindeutig. Hierbei stellt sich aber auch sie die Frage, ob Eineindeutigkeit immer notwendig ist oder ob bspw. die Zurechenbarkeit zu dem Haftenden im Schadensfall nicht ausreicht.

„Die Frage, ob man etwas eineindeutig identifiziert und ob es sicher ist, das sind zwei verschiedene Dimensionen.“

Zitat aus den Fragebögen /
Expertenkonsultationen

Weiterhin ist zu berücksichtigen, dass die Maßgeblichkeit des Anwendungsfalls und das hieraus entstehende Konzept unterschiedlicher Sicherheitslevel zwar zunächst von der Phase der Nutzung ausgeht

(siehe Kapitel 3.2.6) aber ebenso für die Anforderungen an die anderen Phasen des Lebenszyklus einer Digitalen Identität gilt (siehe Kapitel 3)

Derzeitige Levelkonzepte in verschiedener Ausprägung und mit verschiedenen Anwendungsbereichen finden sich bspw. in:

- ISO/IEC 29115 - Entity Authentication Assurance Framework
 - LoA 1 - Little or no confidence
 - LoA 2 - Some confidence
 - LoA 3 - High confidence
 - LoA 4 - Very high confidence

- ISO/IEC 15408 - Common Criteria - Evaluation Assurance Level
 - EAL1: Functionally Tested
 - EAL2: Structurally Tested
 - EAL3: Methodically Tested and Checked
 - EAL4: Methodically Designed, Tested and Reviewed
 - EAL5: Semiformally Designed and Tested
 - EAL6: Semiformally Verified Design and Tested
 - EAL7: Formally Verified Design and Tested
 - und weitere Plus-Varianten EAL4+

- Security Level in der IEC 62443
 - SL1: Schutz gegen zufällige Verletzung
 - SL2: Schutz vor vorsätzlichen Verstößen mit einfachen Mitteln mit geringen Ressourcen, generischen Fähigkeiten und geringer Motivation
 - SL3: Schutz vor vorsätzlichen Verstößen mit ausgefeilten Mitteln mit moderaten Ressourcen
 - SL4: Schutz vor vorsätzlichen Verstößen mit ausgefeilten Mitteln mit erweiterten Ressourcen

- IETF - Vectors of Trust
 - P - Identity Proofing
 - 0-3
 - C - Primary Credential Usage
 - 0, a-f
 - M - Primary Credential Management
 - a-c
 - A - Assertion Presentation
 - a-d

- NIST SP 800-63-3 - Digital Identity Guidelines
 - Identity Assurance Level (IAL)
 - 1-3
 - 3 Authenticator Assurance Level (AAL)
 - 1-3

- + 3 Federation Assurance Level (FAL) - refers to the strength of an assertion in a federated environment
 - 1-3

- eIDAS – Level of Assurance
 - LoA - low
 - LoA - substantial
 - LoA - high

➤ Es bedarf einer domänenübergreifenden Harmonisierung der Levelkonzepte zur Sicherheit.

3.2 Schrittweiser Aufbau des Schaubilds des Gesamtsachverhalts an den Schritten des klassischen Lebenszyklus von Digitalen Identitäten

Im Folgenden werden u.a. die verschiedenen Schritte des Lebenszyklus genauer betrachtet. Wenn es darum geht, eine Identitätslösung zu definieren, bieten alle diese Schritte unterschiedliche Lösungsvarianten oder beeinflussen durch ihre a priori gegebene oder gewählte Beschaffenheit die möglichen Lösungsvarianten in den anderen Schritten. Der Lebenszyklus ist somit Basis der hier geschaffenen Systematisierung der relevanten Handlungsfelder, wird aber durch die soeben in Kapitel 3.1 dargestellten Dimensionen differenziert bzw. ergänzt. Mit der Beschreibung der unterschiedlichen Handlungsfelder wird sukzessive das Schaubild zum Gesamtsachverhalt um den Lebenszyklus aufgebaut

Ausgangspunkt einer digitalen Identität ist zunächst eine Entität (Kap. 3.2.1), also eine existierende konkrete oder abstrakte Sache, für die eine digitale Identität geschaffen bzw. erzeugt wird. Dies geschieht dadurch, dass zunächst gewisse Attribute der Entität festgestellt (Kap. 3.2.2) ggf. festgelegt und in einem digitalen Datensatz abgebildet (Kap. 3.2.3) werden. Dann wird die digitale Identität eingerichtet, also die Entität mit der digitalen Identität (dem Datensatz mit der Sammlung von Attributen) verbunden (Kap. 3.2.4). Dies geschieht bspw. durch ein eindeutiges Merkmal, welches die Entität besitzt oder welches auf sie aufgebracht oder integriert wird (Kap. 3.2.4.1). „Eindeutig“ bedeutet dabei, dass ein Attributsatz nur für diese eine Entität existiert – also einmalig ist. Nun wird der digitale Datensatz gespeichert und u.a. beim „Nutzen“ der Entität gepflegt, aktualisiert bzw. verwaltet (Kap. 3.2.5). Wird die Entität in einem Prozess in irgendeiner Weise genutzt, kann durch das eindeutige Merkmal die digitale Identität aufgerufen und bspw. zur Verifikation genutzt werden (Kap. 3.2.6). Dies geschieht so lange bis die Entität bspw. unersetzbar vernichtet wird und ein Aufbewahren der digitalen Identität ggf. nicht mehr notwendig ist. Je nach Anwendungsfall wird die digitale Identität dann gelöscht oder gesperrt und archiviert.

In einem einfachen Beispiel bedeutet dies (vgl. Abbildung 21): Eine Person packt ein Paket und möchte dies verschicken. Das Paket ist die Entität (Kap. 3.2.1) für die in der Postfiliale eine Digitale Identität geschaffen wird. Der Postangestellte stellt fest (Kap. 3.2.2), dass das Paket 20 × 20 cm groß ist, 400 g schwer und erfragt die Empfängerdaten. Er gibt die Daten in sein System ein (schafft also ein Abbild, Kap. 3.2.3) und erstellt eine eindeutige Paketnummer, die per Strichcode-Aufkleber auf das Paket geklebt (eingesetzt, Kap. 3.2.4) wird. Die digitale Identität wird in dem weltweit zugreifbaren System der Post gespeichert (verwaltet, Kap. 3.2.5) und jedes Mal, wenn das Paket bei Zwischenstationen ankommt, wird der Code eingescannt und somit festgestellt, welches Paket es ist und welche Bestimmung es hat (Kap. 3.2.6). Der Ort wird in der Digitalen Identität aktualisiert (Nutzen, Kap. 3.2.6 und Verwalten, Kap. 3.2.5) und wenn das Paket zugestellt wurde, kann diese Digitale Identität auch wieder gelöscht werden (Kap. 3.2.7).

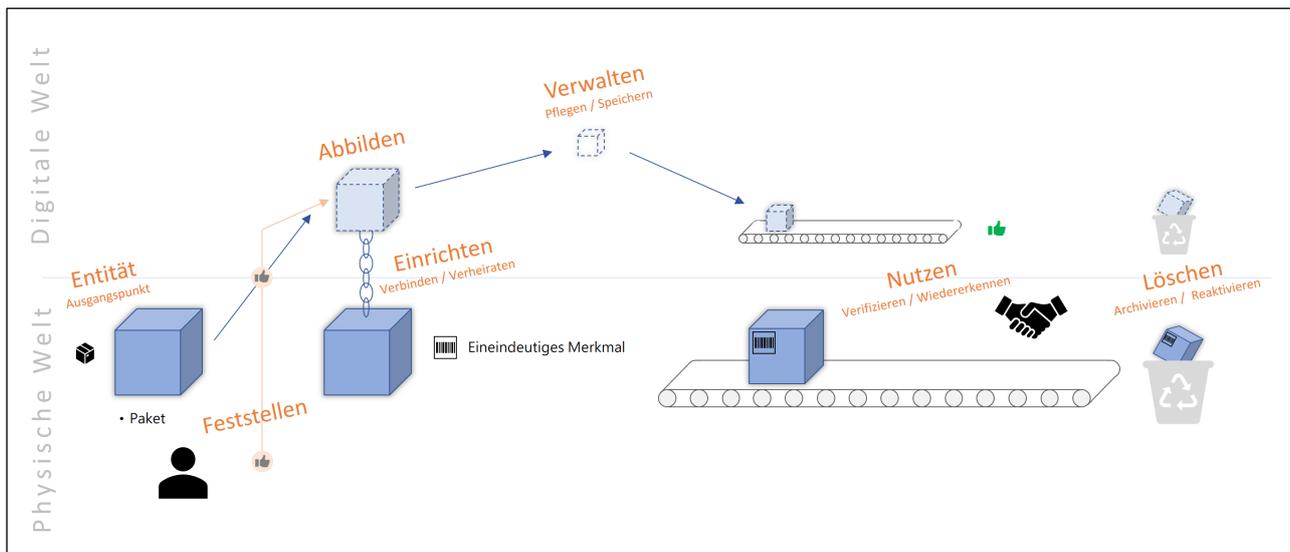


Abbildung 21 – Lebenszyklus der Digitalen Identität eines Postpaketes (einfache Grundstruktur)

Die Digitale Identität des Paketes wäre aus identitätsabfragender Sicht nur als tatsächlich sicher zu bezeichnen, wenn sämtliche Schritte in diesem Prozess und deren Verknüpfungen tatsächlich sicher gestaltet und vollzogen werden.

Aus Identitätsgebender Sicht wäre das Beispiel zum Verständnis vielleicht dahingehend zu erweitern, dass es sich um ein Paket handelt, welches ins Ausland geschickt werden soll und bei dem aufgrund von Zollbestimmungen angegeben werden müsste, was sich in dem Paket befindet. Hierbei wäre dann zur Erreichung einer „Sicheren“ Digitalen Identität aus Sicht des Senders die Frage, wie die abgebildete und verwaltete digitale Identität und die Herausgabe der Informationen über den Inhalt abgesichert wäre.

3.2.1 Entitäten - unbegrenzt mannigfaltiger Ausgangspunkt

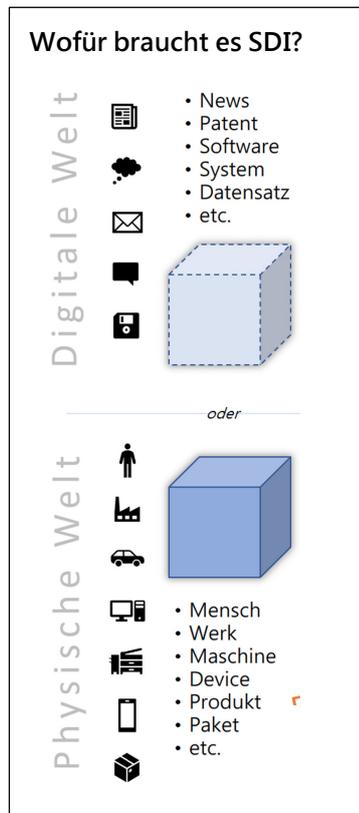


Abbildung 22 – Entitäten

Digitale Identitäten werden dafür geschaffen, dass sie „Entitäten“, bzw. bestimmte Attribute derselben, im digitalen Raum repräsentieren. Der Begriff Entität bezeichnet dabei etwas, das existiert, etwas „Seiendes“. Eine Entität ist ein konkretes oder abstraktes Objekt einschließlich Assoziationen zwischen den Objekten (konkret: bspw. Maschine, Bauteil oder Person / abstrakt: bspw. Patent, Software oder Website). Da es also im Prinzip um jegliche Sache oder Person geht, welche im digitalen Raum Interaktionssubjekt oder -objekt sein soll, erschließt sich, dass es eine unbegrenzte Vielfalt an Entitätstypen gibt.

Die Entität ist Ausgangspunkt aller weiteren Überlegungen im Hinblick auf mögliche Identitätslösungen. Ihr Wesen und ihre Beschaffenheit determinieren einen ganz wesentlichen Teil bei der Erstellung und Nutzung ihrer digitalen Identität. Gerade im Hinblick auf die Frage, wie sicher die Identitätslösung für den Identitätsabfragenden (also dem, der sich sicher sein möchte, dass die Entität auch diejenige ist, die sie vorgibt zu sein) ist, ist es von höchster Relevanz, wie die digitale Identität (als Datensatz) mit der Entität verbunden ist. Bezüglich einer abstrakten Entität handelt es sich nur um die Verbindung eines Datensatzes mit einem anderen. Auch hier gibt es schon diverse unterschiedlich sichere Möglichkeiten. Im Hinblick auf konkrete Entitäten, also physisch existente, wird es jedoch deutlich vielfältiger und komplizierter (siehe Kapitel 3.2.4).

Antwort eines befragten Experten, die nur beispielhaft die Vielfalt an Entitäten darlegt:

Generell relevante Entitätstypen (im weiten Sinne):

| | |
|-----------------------|---|
| # Mensch, Soziales: | Individuum, Familie, Lebenszyklus, Events, Wohnort, ... |
| # Organisation: | public, private; Industrie, Handel, Services - Provider; Verbände |
| # Natur-Ökosysteme: | Stadt, Land, Fauna, Flora, See, Land, Wetter, Klima, ... |
| # Technische Objekte: | in Industrie, Handel, Logistik, Health, Haushalten, Projekten, ... |
| # Geo Dimension: | Inner- bzw. zwischenorganisatorisch, längs der Supply Chain, global – lokal |
| # Netzwerke: | Typ: (Stern, N:m, Ring, Hybrid); Kommunikation, technische vs. ökonomisch |
| # Anwendungen: | Logistik, Handelsabkommen, Absprachen- Kontrakte, ... |

Da die Digitalisierung quasi jegliche Dinge der physischen Welt betreffen wird, erklärt sich die Mannigfaltigkeit der Entitäten mit Identitätslösungsbedarf von selbst. Weniger generalisierend bzw. abstrakt und die Notwendigkeit des Themas somit wesentlich deutlicher adressierend ist der Verweis auf sämtliche Zukunftsprojekte, auf die Wirtschaft und Gesellschaft hinarbeiten - wie Industrie 4.0, Smart Cities, Smart Mobility usw. Denn je fortgeschrittener die Digitalisierung von den Handlungen, Interaktionen, Vernetzungen etc. in einem solchen angestrebten System ist, desto bedeutender wird die Sicherheit von Digitalen Identitäten. Sie sind sogar Voraussetzung dafür, dass diese Projekte funktionieren können bzw. dass in selbige investiert wird, denn Unsicherheit ist der Feind der Investitionen. Die

Zukunftsprojekte adressieren dabei die Steuerung und das Management wesentlicher Systeme unserer Wirtschaft und Gesellschaft. In diesem Sinne lassen sich nicht nur IT-Produkte als Bedarfsinhaber von Identitätslösungen identifizieren, sondern vielmehr alle Entitäten, die durch die digitalen Zukunftsprojekte gesteuert, organisiert bzw. prinzipiell berührt werden.

Im Hinblick auf ein Gesamtsystem bzw. den strukturellen Umgang mit Entitäten mithilfe von SDI ist zudem ein weiterer Aspekt hervorzuheben, den es zu berücksichtigen gilt: eine SDI steht nicht automatisch auch für die Vertrauenswürdigkeit der Entität, die sie repräsentiert.

➤ Eine Sammlung und Kategorisierung von Arten von Entitäten und diesbezüglich möglicher Verfahren für die Schaffung Sicherer Digitaler Identitäten (also auch Einstufung der Sicherheitsniveaus im Sinne von domänenübergreifenden Sicherheitsleveln) fehlt.

3.2.2 Feststellen der Identität – Governance-Strukturen

Das Feststellen der Existenz einer Entität bzw. der die digitale Identität bildenden Attribute ist einer der relevantesten Akte auf dem Weg zu einer Sicherer Digitaler Identität.

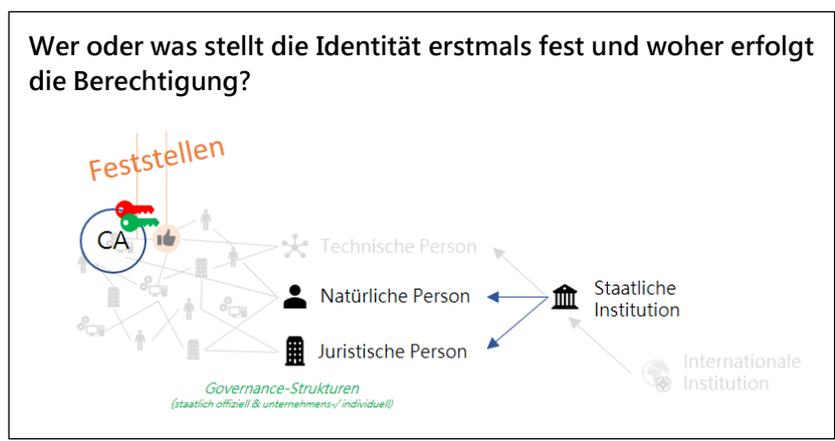


Abbildung 23 – Feststellen einer Identität

Die Instanz, die das „Feststellen“ vornimmt, kann sowohl eine Person, eine Software, ein Roboter oder deren Kombination in einem durch mehrere Instanzen laufenden Prozess sein. Sie bzw. der Prozess muss geeignet sein, die Attribute zu identifizieren und zu verifizieren. Im Hinblick auf die Sicherheit einer digitalen Identität ist weiterhin entscheidend, wie dieser Instanz vertraut werden kann. Nehmen wir an, das

Feststellen findet in einem Unternehmen statt und die Entität sei ein Produkt, welches dann durch das Unternehmen verkauft wird. Dann wird in der Regel die Instanz, die das Feststellen vornimmt, durch das Unternehmen autorisiert worden sein, dies zu tun. Je nach erwünschtem Sicherheitslevel könnte die Anforderung gestellt werden, dass dieser Prozess nach einem bestimmten Verfahren zu gestalten oder zu dokumentieren ist, um sicherzustellen, dass nicht nur der Prozess der Erstellung einer digitalen Identität, sondern auch derjenige, der ihn durchführt (bzw. fähig wäre, ihn zu korrumpieren), vertrauenswürdig ist. Die Autorisationskette geht weiter bis hin zu einer möglichen sicheren Identität des Unternehmens bzw. der juristischen Person. Diese juristische Person, die gegebenenfalls durch eine hochsichere digitale Identität abgebildet werden könnte, könnte oder sollte wiederum beispielsweise durch eine staatliche Instanz erstellt und autorisiert worden sein.

In dem Analyseprozess wurde dies als notwendige zu regelnde Governance-Struktur deklariert, die international nach möglichst vertrauenswürdigen einheitlichen Regeln ablaufen sollte. Im europäischen Raum mag die eIDAS Verordnung in ihrer aktuellsten Anpassung die entsprechenden Ansätze bieten.

Anmerkung: bzgl. immer autarker agierender Systeme, bzw. erster Formen künstlichen Intelligenzen wird u.a. auf europäischer Ebene zudem über eine Erweiterung der Konzepte natürlicher und juristischer Personen um das einer technischen Person diskutiert.

- **Es bedarf der Definition und Sammlung der Vorgehensweisen und Rahmenbedingungen ggf. der Systematisierung und Standardisierung mit Einstufung des Sicherheitsniveaus im Sinne domänenübergreifender Sicherheitslevel.**

3.2.3 Abbilden der Identität

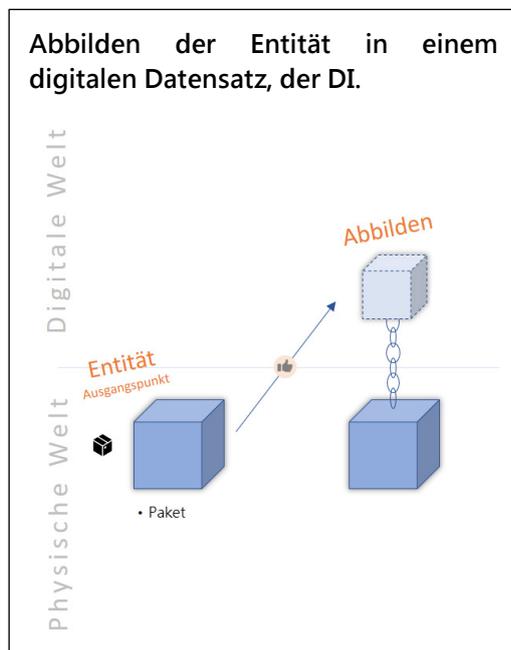


Abbildung 24 – Abbilden einer Identität

Das Abbilden einer Identität kann in unterschiedlichster Art und Weise geschehen. Es stellt sich die Frage, welche Daten wie gespeichert werden. Werden sie verschlüsselt gespeichert (siehe hierzu Kapitel 3.2.6), wo werden sie abgespeichert, in welcher Sprache und Programmiersprache werden sie abgespeichert, wie werden sie klassifiziert (vgl. Projekt eCI@ss) usw. Die Art und Weise des Abbildens ist dabei maßgeblich, ob sie für den späteren Prozess und für die Verwendung über System- und Domänengrenzen hinweg nutzbar, also interoperabel ist. Im Analyseprozess wurde daher von einigen Experten der Software-Aspekt bei Identitätslösungen als der ggü. der Hardwareseite noch dringender zu regelnde bzw. zu standardisierende Sachverhalt adressiert.

Das Abbilden einer digitalen Identität ist einer der Schritte des Lebenszyklus, die im besonderen Interesse des Identitätsgebers stehen. Das Feststellen und Abbilden ist auch nicht als einmaliger Vorgang anzusehen, da Datensammlungen über Entitäten im Laufe der Zeit wachsen. Hier stellt sich bspw. die Frage, ob das Prinzip der Datensparsamkeit gewahrt wird.

- **Es bedarf der Sammlung und Aufstellung sowie der möglichst anwendungsbezogenen Standardisierung der verschiedenen Verfahren mit Einstufung des Sicherheitsniveaus im Sinne domänenübergreifender Sicherheitslevel für Identitätsgeber und -abfrager.**

3.2.4 Einrichten der Identität

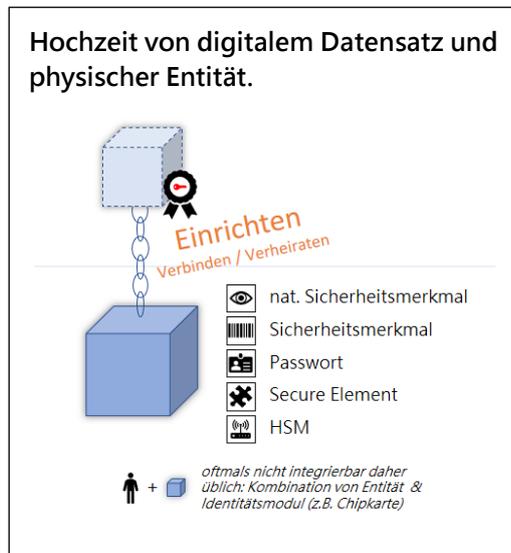


Abbildung 25 – Einrichten einer Identität

Das Einrichten der Identität, also das Verbinden der digitalen Identität, also des Datensatzes, mit der Entität, ist einer der entscheidendsten Sachverhalte im Hinblick auf die Sicherheit einer digitalen Identität und determiniert auch wesentlich die Möglichkeiten der anderen Schritte.

In der Einleitung des Kapitels 3 wurde darauf hingewiesen, dass die Hoffnung bestand, dass es eine One-Fits-All Lösung geben könne. Sowohl diese Überlegungen als auch die Frage vieler, die aus identitätsabfragender Sicht das Thema betrachten: „Welche Arten von Identitätslösungen es denn nun grundsätzlich gäbe?“, reduzieren in der Regel den gesamten Sachverhalt auf diesen Schritt des Lebenszyklus bezogen auf eine physische Entität. Trotz der Wichtigkeit dieses Schrittes, greift dies natürlich viel zu kurz, wie das Kapitel und der Bericht in seiner Gänze deutlich zeigen.

Einrichten abstrakter/digitaler Entitäten

Wir konzentrieren uns in diesem Bericht im Hinblick auf das „Einrichten“ auf physische bzw. konkrete Entitäten, denn das Verbinden einer abstrakten Entität mit seiner digitalen Identität kann zwar ebenso in unterschiedlichster Art und Weise passieren, ist aber prinzipiell andersartig. Die Verbindung zwischen abstrakter oder besser gesagt digital vollständig abbildbarer Entität und ihrer digitalen Identität ist grundsätzlich auch immer untrennbar möglich (indem die digitale Entität mit der DI verschlüsselt wird). Problematisch ist bei digitalen Entitäten vielmehr die Gefahr der unerlaubten Kopie und/oder die Souveränität über selbige, also bspw. Nutzungsrechte wieder entziehen zu können – ein Problem, welches bspw. der Industrial Data Space behandelt.

Einrichten konkreter/physischer Entitäten

Im Hinblick auf die physischen, also konkreten Entitäten erklärt sich von selbst, dass die Beschaffenheit der Entität die Möglichkeiten, die digitale Identität mit der physischen Entität zu verbinden, einschränkt bzw. determiniert. Eine mögliche Klassifizierung könnte wie folgt aussehen:

- (0) Entität ohne künstlich aufgebrachte Sicherheitsmerkmale und ohne eigene Merkmale, die eine Eineindeutigkeit gewährleisten könnten (z.B. Flüssigkeiten, Schüttgut) [Beispiel: Das Verbinden der Entität mit der digitalen Identität ist hier nur mit Hilfsmitteln, z.B. einem Behältnis, wie einer Flasche, oder auch gar nicht möglich. Das Behältnis fällt dann unter die anderen Kategorien. Es gibt aber auch Ansätze für Lösungen bspw. Schüttgut mit Mikropartikeln zur Identifizierbarkeit zu versetzen.]
- (1) Entität ohne künstlich aufgebrachte Sicherheitsmerkmale allerdings mit eigenen Merkmalen, die eine Eineindeutigkeit gewährleisten können (z.B. Biometrie oder, bei Dingen, Vermessung charakteristischer Oberflächeneigenschaften, ebenso das Messung charakteristischen Verhaltens einer Entität) [Beispiel: Mikrorauigkeit eines DINA4 Papiers ist wie ein Fingerabdruck]
- (2) Entität mit aufgebrachtem oder integriertem „künstlichen“ Sicherheitsmerkmal / Identitätskennzeichen (z.B. Strichcode, eindeutige Seriennummer, Rauschmuster)

- (3) Entität mit aufgebracht oder integrierter einfacher IT und Datenträger, der auch die gesamte oder ggf. deutlich mehr Informationen als die eigentliche digitale Identität als Datensatz gespeichert haben kann (z.B. ein RFID-Chip)
- (4) Entität mit aufgebracht oder integriertem Hochsicherheitsmodul HSM (Kleinstrechner mit Zugriff auf Strom und fähig zur Durchführung kryptographischer Prozesse sowie ggf. zur Übernahme von Prozessen, die die Entität erst zu der machen, die sie ist)

Hinsichtlich der Klassen 1-4 wäre die Art der physischen Verbindung noch zwingend zu definieren - also im Prinzip das Level der Trennbarkeit der beiden. Kann beispielsweise das Sicherheitsmerkmal einfach entfernt werden (Abziehen des Strichcode-Aufklebers) oder ist das Hochsicherheitsmodul untrennbar mit der Entität (bspw. mit der Platine) verbunden. Darüber hinaus könnten die Klassen auch kombiniert verstanden werden. So kann bspw. eine Entität natürlich einen RFID-Chip aufgeklebt haben und trotzdem eigene oder aufgebrachte Sicherheitsmerkmale, wie bspw. eine eindeutige Oberflächenstruktur oder den eingefrästen Strichcode.

Einrichten der besonderen physischen Entität - Mensch

Der Mensch ist eine besondere Form der Entität. Durch seine grundsätzlich vorhandenen unterschiedlichen Fähigkeiten ist er ein Sonderfall, auch wenn diese Fähigkeiten durchaus mit den Möglichkeiten bei Dingen vergleichbar sind. Der Mensch hat in jedem Fall eigene Sicherheitsmerkmale im Sinne der Biometrie oder des typischen Verhaltens. Zudem kann er Dinge sicher speichern (Passwort, Gestenmuster, etc.). Er kann Situationen erkennen und analysieren, kann aktiv kommunizieren. Der Mensch kann aber keine höheren kryptographischen Prozesse vornehmen oder größere Datenmengen so speichern, dass sie für die IT unmittelbar verwendbar sind. Er kann aber Träger von Datenspeichern, Secure Elements und Hochsicherheitsmodulen verwahren. In diesem Sinne ist der Mensch prädestiniert für die Kombination mit weiteren Authentifikationsmitteln. Bspw. können RFID-Chip oder Hochsicherheitsmodul in Form einer Chipkarte für die Verifikation der Entität Mensch genutzt werden (z.B. Bankkarten, elektronischer Personalausweis). Wenn die Daten auf der Chipkarte oder die digitale Identität dahinter auch noch Informationen über die Biometrie der Person beinhalten, kann diese zur Verifikation der Verbindung Mensch und Chipkarte dienen. Das meistgenutzte Verfahren hierbei ist, dass der Mensch ein Sicherheitsmerkmal "integriert" mit dem er die Verifikation der Verbindung zwischen Chipkarte und Mensch vornehmen kann: das Passwort.

Bei der Entität Mensch werden bspw. folgende die Authentifizierungsmöglichkeiten unterschieden:

- per Wissen aufgeteilt in Erinnern (Passwort, Unterschrift, Gestenmuster o.ä.) oder Erkennen (Geheimnis auf Bildern erkennen o.ä.),
- per Besitz (Chipkarte)
- per Biometrie

- **Es bedarf der Sammlung und Klassifizierung sowie der möglichst anwendungsbezogenen Standardisierung der verschiedenen Verfahren mit Einstufung ihrer Sicherheitsniveaus im Sinne domänenübergreifender Sicherheitslevel für Identitätsgeber und -abfrager. Gleichzeitig muss diese aufzeigen, welche Grundlagen die Verbindung für den Gesamtprozess schafft.**
- **Ggf. sind Einigungen erzielbar, dass für bestimmte Entitätstypen gewisse Einrichtungsverfahren zum Standard werden bzw. als Voraussetzung für den Einsatz in bestimmten Sicherheitslevelbereichen Voraussetzung werden.**

3.2.4.1 Beispiele: Merkmale und Techniken zum Verbinden einer Entität mit einer Digitalen Identität

Um die Breite der Möglichkeiten darzulegen, werden folgend beispielhaft einige Merkmale und Techniken vorgestellt bzw. aufgelistet, die beim Einrichten der Identität eine Rolle spielen. Allein bei aufbringbaren Sicherheitsmerkmalen für nicht menschliche physische Entitäten beläuft sich dabei die Schätzung von Experten auf 300 bis 400 am Markt verfügbare Technologien. Hinzu kommen die unterschiedlichen Gestaltungsmöglichkeiten der höheren Technik (RFID, HSM, etc.), Techniken, wie die Verhaltensanalyse (die eigentlich eher im Kapitel Nutzen angesiedelt ist) und vor allem die Kombination der Möglichkeiten, die oftmals erst zu einer Eineindeutigkeit führt.

3.2.4.1.1 Beispiele: Biometrie bei Menschen

Zu den sicherheitsrelevanten ggf. eindeutigen Merkmalen im Sinne von Biometrie beim Menschen zählen u.a.:

- (a) Handabdruck (0,2% Fehler)
- (b) Fingerabdruck (0,1% Fehler)
- (c) Stimme (< 1% Fehler)
- (d) Eintastverhalten (< 5% Fehler)
- (e) Iris (0,0001 % Fehler)
- (f) Gesicht (< 1% Fehler)
- (g) Unterschrift nach Form und/oder Schreibdynamik
- (h) Mimik, Motorik
- (i) Ohrgeometrie
- (j) Enzephalogramm
- (k) Kardiogramm
- (l) DNA

Biometrische Verfahren sind dabei nie zu 100% sicher bzw. eindeutig. Es gibt immer „nur“ Wahrscheinlichkeiten, wenn diese auch sehr hoch sein können. Diese spiegeln sich in False Acceptance Rates (Falsche Annahme) und False Rejects Rates (Falsche Ablehnung) wieder. So kann es bspw. vorkommen, dass die Gesichtserkennung bei Krankheit nicht funktioniert.

Grundlegendes Problem der biometrischen Sicherheitsmerkmale ist, dass ein einmal kompromittiertes, also nicht mehr vertrauenswürdige Merkmal, nicht einfach ausgewechselt werden kann. Beispiel: Hat ein Angreifer einen Fingerabdruck gelesen und erfolgreich eine Attrappe davon gebaut, kann der Nutzer diesen Fingerabdruck nicht mehr nutzen – es bleiben nur noch neun.

3.2.4.1.2 Beispiele: Aufbringbare sicherheitsrelevante Merkmale bei Dingen

Zu den aufbringbaren sicherheitsrelevanten Merkmalen zählen, wie folgt aufgelistet, eine Vielzahl an Verfahren. Hierbei sind nicht alle unmittelbar für die Verbindung zwischen digitaler Identität und Entität relevant, insbesondere, da sie in vielen Fällen nicht eindeutig sind. In der Kombination mit anderen Merkmalen können sie aber zur Eineindeutigkeit führen, insbesondere aber stets zur Steigerung der Wahrscheinlichkeit, dass die Verbindung zwischen digitalem Datensatz / digitaler Identität und Entität gegeben ist. So kann in der digitalen Identität angegeben sein, dass die Entität mit einer Spezialfarbe versehen ist. Wenn diese per Kamera wahrnehmbar ist, kann diese auch für die Fernabfrage genutzt werden.

- (a) Biologisch

- a. Antikörper
- b. Desoxyribonukleinsäure (DNA)
 - i. DNA-Sequenz
 - ii. DNA-Strang
- (b) Chemisch
 - a. Nanotech Barcode
- (c) Elektrisch / magnetisch / elektromagnetisch
 - a. Elektromagnetisch detektierbare Farbe
 - b. Akustomagnetisches Etikett
 - c. Elektromagnetisches Etikett
 - d. Elektromagnetische Glasfasern
 - e. Mikrochip mit Kontakt
 - f. Radiofrequenzidentifikation (RFID)
- (d) Haptisch
 - a. Druckverfahren
 - i. Hochdruck
 - ii. Matrixdruck / Nadeldruck
 - iii. Tiefdruck
 - 1. Intagliodruck / Stichtiefdruck
 - 2. Orlof-Technik / Schabloneneinfärbetechnik
 - 3. Rastertiefdruck
 - iv. Siebdruck
 - b. Prägen
 - i. Blindprägung
 - ii. Heißfolienprägung
- (e) Optisch
 - a. Optische Effekte
 - i. Durchsichtsfenster
 - 1. Foliendurchsichtsfenster
 - 2. Moiré Magnifier-Element
 - ii. Durchsichtsregister
 - iii. Hologramme
 - iv. Laserkippbild
 - v. Parallaxe
 - vi. Retroreflektierende Folie
 - vii. Wasserzeichen
 - b. Pre-Press-Druckmerkmale
 - i. Anti-Kopier-Muster
 - ii. Besondere Schriftart
 - iii. Digitale Wasserzeichen
 - iv. Mikrotext
 - v. Rasterbild
 - vi. Scrambled image / codiertes Bild
 - c. Spezialdruck
 - i. Guillochen
 - ii. Irisdruck / Regenbogendruck
 - d. Spezialfarben / Spezialpartikel
 - i. Clustermerkmal
 - ii. Fotochrome Farbe
 - 1. Reversible fotochrome Farbe
 - 2. Irreversible fotochrome Farbe
 - iii. Fluoreszenz
 - 1. Infrarot-Farbe (IR)
 - 2. Röntgenlumineszenz
 - 3. Tagesleuchtfarbe / Neonfarbe als Echtfarbelement

- 4. Ultraviolette Farbe (UV)
 - iv. Interferenz- und Effektfarbe
 - v. Kippfarbe / optisch variable Druckfarbe
 - vi. Magnetisierbare Farbe
 - vii. Metallreagenzfarbe
 - viii. Metamere Farbe
 - ix. Mikrofarbcode
 - x. Mikropunkte
 - xi. Pen-Reactive-Ink / Reagenzfarbe
 - xii. Phosphoreszenz
 - xiii. Sicherheitsfärbemittel
 - xiv. Sonderfarbe
 - xv. Spektralsensible Farbe
 - xvi. thermoreaktive Farbe
 - 1. Thermische Pigmente
 - 2. Thermochrome Pigmente
- e. Sonstige
 - i. Feuchtstempelabdruck
 - ii. Lasergravur
 - iii. Oberflächenauthentifizierung
 - 1. Musteroberfläche
 - 2. Sprengprägen
 - 3. Stochastische Schwankungen im Fertigungsprozess
 - iv. Perforation
 - 1. Laserperforation
 - 2. Nadelperforation
 - v. Rauschmustercodes
 - vi. Sicherheitsanstanzung
 - vii. Sicherheitsfaden
- (f) Sonstige
 - a. Duftstoffe
 - b. Markierung pulvermetallurgisch hergestellter Bauteile
 - c. Nanopartikel

3.2.4.1.3 Beispiele: maschinenlesbare Identitätskennzeichen

Für eine eindeutige Kennzeichnung sorgen unterschiedliche maschinenlesbare Codes. Bei Ihnen bleibt vor allem die Frage nach der Trennbarkeit von der Entität, also ob die Kennzeichnung fest mit der Entität verbunden ist.

- (a) Optische Codierung
 - a. 1D-Code
 - i. Strichcode
 - b. 2D-Code
 - i. Stapelcode
 - ii. Matrixcode
 - 1. QR-Code
 - 2. DataMatrix-Code
 - c. 3D-Code
 - i. Farbcode
 - 1. Color Ultra Code
- (b) Optical Character Recognition (OCR)
- (c) Radiofrequenzidentifikation (RFID)
 - a. Low Frequency (LF)
 - b. High Frequency (HF)
 - c. Ultra High Frequency (UHF)

Hier sind bereits auch RFID-Chips aufgeführt, da sie standardmäßig als Identitätskennzeichen bzw. inzwischen als Ersatz für optische Codes genutzt werden. Aber auch in der einfachsten Variante heben sie sich dadurch ab, dass sie per Funk kommunizieren können und deutlich mehr Daten als ein optischer Code speichern können.

3.2.4.1.4 Beispiel: RFID

RFID beschreibt ein Verfahren zur kontaktlosen Übermittlung von Daten. Diese kontaktlose Übermittlung in einem Kommunikationssystem besteht in den meisten Fällen aus zwei Elementen. Das erste Element besteht aus einem passiven Transponder bzw. einem sogenannten RFID-Tag der Daten vorhält und dementsprechend der zweite Abschnitt aus einem aktiven Lesegerät, der diese Daten auslesen kann.

Somit sind RFIDs nichts Weiteres als eine Technologie für Sender-Empfänger-Systeme zum automatischen und berührungslosen Identifizieren und Lokalisieren von Objekten und Lebewesen mit Radiowellen.

Das vom Lesegerät erzeugte magnetische oder durch hochfrequente Radiowellen erzeugte Feld überträgt nicht nur Daten, sondern versorgt die RFID Chips mit einer gewissen Menge an Energie. Aufgrund der dadurch nicht notwendigen internen Energieversorgung passiver RFID-Chips können sie problemlos günstig in Serie gefertigt werden und lassen sich dadurch vielseitig einsetzen (z.B. im Handel als Ersatz für Barcodes).

3.2.4.1.5 Beispiel: MAC-Adresse

Für die Entitätengruppe „Netzwerkadapter “ oder vielleicht sogar „technische Geräte, die netzwerkfähig sind bzw. einen Netzwerkadapter besitzen “, gibt es eine weltweit einheitliche Hardware Adresse: die Media-Access-Control Adresse (MAC-Adresse). Man spricht auch von einer Physischen Adresse oder Geräteadresse. Bei Apple wird sie auch Ethernet-ID, Airport-ID oder Wi-Fi-Adresse genannt, bei Microsoft Physische Adresse. Ob sie global eineindeutig ist oder lokal administriert wurde und somit nur in einem lokalen Netzwerk eindeutig ist, gibt das 2. Bit der Adresse an. 0 steht hierfür bei für Universally Administered Address und 1 für Locally Administered Address. Die ersten 6 Stellen sind zudem in Teilen (es gibt auch Hersteller unabhängige MAC-Adressen) ein Herstellercode und lassen so auf den Hersteller des Netzwerkadapters schließen.

Herstellercodes von MAC-Adressen (Auswahl)

| | |
|-------------------|--------|
| 00-50-8B-xx-xx-xx | Compaq |
| 00-07-E9-xx-xx-xx | Intel |
| 00-60-2F-xx-xx-xx | Cisco |
| 00-15-F2-xx-xx-xx | Asus |

Prinzipiell könnte die MAC-Adresse als eineindeutiger Identifikator des elektronischen Geräts in einem Rechnernetz gelten, allerdings nur auf einer unteren Sicherheitsstufe. Tatsächlich sind sie auch im Rahmen des OSI-Modells (ein Referenzmodell für Netzwerkprotokolle als Schichtenarchitektur, welches den Zweck die Kommunikation über unterschiedlichste technische Systeme hinweg zu ermöglichen) der Sicherungsschicht (Schicht 2) zugeordnet.

3.2.4.1.6 Beispiel: IMEI

Die International Mobile Station Equipment Identity (IMEI) ist eine eindeutige 15-stellige Seriennummer, mit der jedes GSM-, UMTS- oder LTE-Endgerät weltweit prinzipiell eindeutig identifiziert werden kann. Sie ist bspw. bekannt dadurch, dass ein gestohlenen Mobiltelefon vermeintlich dadurch gesperrt werden kann. In der Theorie ist das Mobiltelefon nach Sperrung auch mit einer anderen SIM-Karte nicht benutzbar. Dazu werden die betroffenen IMEIs in Listen geführt. Die IMEI lässt sich aber mit entsprechender Software neu programmieren. Somit sind wesentliche Sicherheitsmerkmale hinfällig.

3.2.4.1.7 Beispiel: Secure Element

Als Secure Element wird ein spezieller Chip bzw. Mikrocontroller verstanden, der ein sicheres Bereitstellen vertraulicher Daten und Anwendungen ermöglicht. Der Zugriff auf das Secure Element und auf die darin gespeicherten Daten ist durch kryptographische Methoden abgesichert.

Ein Beispiel hierfür sind Chipkarten, welche die sichere Authentifizierung an Bankautomaten (Geldausgabegeräte, etc.) ermöglichen. Die erforderliche Eingabe eines PIN ist ein zentrales Merkmal von Secure Elements, da der Zugriff auf das Secure Element bzw. auf die darin sicher gespeicherten Daten geschützt sein muss.

Die wesentlichen Funktionen eines Secure Elements werden wie folgt zusammengefasst:

- Sicherer Speicher für sicherheitskritische Daten
- Kryptographische Operationen
- Sichere Umgebung zur Ausführung von Programmcode

Generell kann der Lebenszyklus des Secure Elements in die folgenden vier Abschnitte unterteilt werden:

- **Initialisierung:**
 - grundlegende Parameter des Secure Elements werden festgelegt
 - Applikationen können am Secure Element installiert werden
- **Aktivierung:**
 - Platform Manager wird festgelegt
 - Secure Element für eine Verwendung im jeweiligen mobilen Gerät freigegeben.
- **Verwaltungsphase:**
 - umfasst jene Zeitspanne, in der das Secure Element einsatzbereit ist
 - Security Domains werden vom Dienstanbieter angefordert
 - Platform Manager vergibt Security Domains dynamisch
- **Deaktivierung:**
 - Deaktivierung beendet die Verwaltungsphase.

3.2.4.1.8 Beispiel: Trusted Platform Module (TPM)

Das Trusted Platform Module (TPM) ist ein Chip/Prozessor (nach der TCG-Spezifikation), welcher in Systemen eingesetzt werden kann, um Sicherheitsmechanismen aus einem potentiell kompromittierbaren Betriebssystem auszulagern und in einem externen, vertrauenswürdigen Chip durchzuführen. Das TPM fungiert auch als externer, kryptographisch abgesicherter Speicher für Sicherheitsschlüssel. Das TPM ist ein essentielles Element der Trusted Platform Architecture (TPA), ist auch softwaretechnisch nicht manipulierbar und dient u.a. zur sicheren Speicherung und Verarbeitung von systembeschreibenden Referenzwerten der Plattform, in der es sich befindet. Das TPM verhält sich ähnlich einer fest eingebauten Smart Card, mit dem Unterschied, dass es nicht an einen konkreten Benutzer (Benutzer-

Instanz), sondern an den lokalen Computer (Hardware-Instanz) gebunden ist. Es kann zudem nicht nur in PCs sondern auch in PDAs, Mobiltelefonen und Unterhaltungselektronik integriert werden.

Die Funktionen des TPM lassen sich in kryptographische Komponenten und nicht-kryptographische Bestandteile unterscheiden. Zu den kryptographischen Komponenten gehört ein Generator für asymmetrische Schlüssel. Als weitere wesentliche Komponente enthält das TPM einen physikalischen (Pseudo-) Zufallszahlengenerator.

Die drei wesentlichen Schlüsseltypen im TPM:

- Endorsement Key (EK) – eindeutiger Schlüssel der des TPM, dessen privater Teil den TPM niemals verlassen darf (auch ein Backup ist daher nicht möglich)
- Storage Root Key (SRK) – wird benutzt um weitere Schlüssel (z.B. für die Email-Kommunikation eines Benutzers) zu verschlüsseln und wird mit Wechsel des Besitzers des Rechners neu erzeugt
- Attestation Identity Keys (AIK) – fungiert als Pseudonym für den EK zum Schutz des Identitätsgebers zur Beglaubigung der Plattformintegrität und bedarf der Bestätigung durch eine vertrauenswürdige Drittpartei (Trusted Third Party / Privacy-CA) mit einem AIK-Zertifikat oder Direct Anonymous Attestation (DAA)

Sicherheitsfunktionen des TPM:

- Versiegelung – Daten können einzigartig an ein TPM gebunden werden und nur in ein und demselben System wieder entschlüsselt werden
- Auslagerung – Schlüssel, deren Wurzel im TPM verbleibt, können auch auf externen Medien gespeichert werden; somit ist eine unbegrenzte Anzahl an Schlüsseln erstellbar
- Schutz kryptografischer Schlüssel – Schlüssel können innerhalb des TPM erzeugt, benutzt und abgelegt werden und sind so vor Softwaremanipulation geschützt und auch vor Hardwaremanipulation je nach Einbau
- Bescheinigung – die Fähigkeiten und Zustand (Konformität) der Plattform können nach außen hin bestätigt werden; zum Schutz der Privatsphäre mithilfe eines ext. Attestationsverfahren
- Sicherer Zufallsgenerator – die Gewinnung von tatsächlichen Zufallswerten bedarf es für viele Herausforderungen der Informatik

TPM werden für nahezu alle namhaften PCs und Notebooks, die für professionelle Anwendung gestaltet sind, angeboten.

3.2.4.1.9 Beispiel: HSM – Hardware Sicherheitsmodul bzw. Hardware Security Module

Ein Hardware Sicherheitsmodul (HSM) ist ein internes oder externes Peripheriegerät für die effiziente und sichere Ausführung kryptographischer Operationen oder Applikationen. Mittels dieser kryptografischen Applikationen, werden beispielsweise die Vertrauenswürdigkeit und die Integrität von Daten und den damit verbundenen Informationen in geschäftskritischen IT-Systemen sichergestellt.

Dementsprechend ist ein HSM ein Gerät, welches in ein System, Netzwerk oder in ein anderes Gerät eingebunden werden muss. In selbigem hat dann wiederum ein Krypto-Prozessor die Aufgabe, Verschlüsselungs-Keys über den kompletten Lebenszyklus zu schützen. Somit dient das HSM im Sinne einer eigenständigen Einheit als Vertrauensanker.

Die kryptografische Infrastruktur wird durch die Aufbewahrung der kryptografischen Keys in einer hochsicheren, manipulationssicheren Appliance gesichert. Somit können die Schlüssel sicher verwaltet, verarbeitet und gespeichert werden und es wird ein zuverlässiger Schutz für Transaktionen, Identitäten und Anwendungen gewährleistet.

3.2.5 Verwalten der Identität

Das Verwalten der digitalen Identität, also im Prinzip das Pflegen und Speichern des digitalen Datensatzes, welcher u.a. die Attribute zur Entität beinhaltet, kann ebenfalls auf unterschiedlichste Art und Weise geschehen. Der Datensatz kann dabei ganz oder teilweise getrennt von der physischen Entität, z.B. in der Cloud, gespeichert

Von wem, wo und wie werden die Datensätze, die Digitalen Identitäten, gespeichert, verwaltet, gepflegt, zugänglich gemacht?

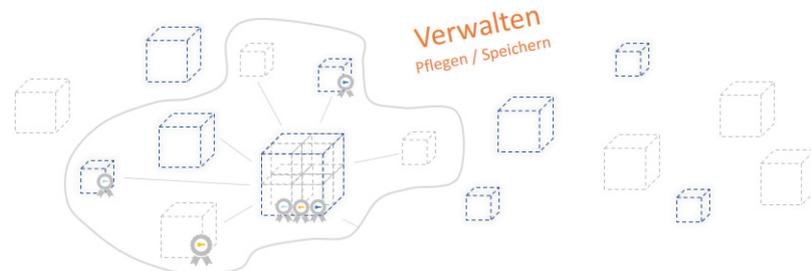


Abbildung 26 – Verwalten einer Identität

werden. Zur Nutzung der Identitätslösung für den Identitätsabfragenden muss dann, sowohl zur Verifizierung der digitalen Identität, als auch zur sicheren Identifizierung der zugehörigen physischen Entität (vgl. Kapitel 3.1.1), der in der Cloud befindliche Datensatz (bzw. mindestens der zur Identifikation notwendige Teil) abgefragt werden und es muss die vorhandene Verbindung zur physischen Entität überprüft werden.

Ist der Datensatz der Identität dabei also in einer Cloud gespeichert, stellt sich aus identitätsgebender Sicht ganz explizit die Frage, von wem er wie verwaltet und gepflegt wird, wer wann und wie darauf Zugriff erhält und ihn verändern kann etc. Bei Varianten, in denen der Datensatz zum großen Teil in einem Datenspeicher in oder auf der Entität gespeichert ist, entstehen die Herausforderungen natürlich an anderer Stelle.

Das Verwalten der Identität ist den natürlich i.d.R. nicht einmaligen Anwendungsfällen (Kapitel 3.2.6 - Nutzen der Identität) sowohl vor- wie nachgelagert. Der Datensatz wird dabei in vielen Fällen durch jede Nutzung inhaltlich wieder aktualisiert. In manchen Fällen kann der Anwendungsfall auch fast schon eine erneute Feststellung darstellen. In diesem Sinne steigt i.d.R. auch das Sicherheitsniveau mit der Aktualität des Datensatzes und der Nähe der letzten vorgenommenen Verifizierung und/oder auch der Konsistenz der Aktualisierungen (vgl. hierzu auch Beispiel 3.4.4).

In dem späteren Schaubild repräsentieren dann die gestrichelten Kästchen (vgl. Abbildung 26) diese unterschiedlichen digitalen Identitäten, die zu einer Entität bestehen können. Hierbei sind auch digitale Identitäten im Sinne von Datensätzen über die Entität transparent dargestellt. Diese repräsentieren digitale Identitäten bzgl. derer die Entität bzw. deren Besitzer, wenn es sich bei der Entität nicht um einen Mensch handelt, unwissend ist. So weiß sie oft nicht, wie sich eine Identität im Prozess der Nutzung weiter entwickelt hat und im Zweifel sogar nicht einmal, dass dieser digitale Datensatz überhaupt existiert.

Sowohl aus Sicht des Identitätsgebers als auch des Identitätsabfragers hängt das Sicherheitslevel einer Identitätslösung also ganz wesentlich davon ab, wer den Datensatz wo und wie speichert, ihn pflegt, zur Verfügung stellt etc. Hierbei stellen sich zudem unterschiedlichste weitergehende Fragen der Integrität und Sicherheit – u.a. auch die Frage, wie sicher die Systeme des Anbieters sind, der diese Aufgaben übernimmt. Darüber hinaus hat zudem noch die Sicherheit der Kommunikation zwischen dem Erzeugen bzw. Abbilden einer Identität und dem Übertrag in die Cloud sowie die Kommunikation zwischen dem

System des Identitätsabfragers und der Cloud – also die Sicherheit der Kommunikationskanäle – Auswirkungen auf das Sicherheitslevel der Identitätslösung.

3.2.6 Nutzen der Identitätslösung

Der Moment der Nutzung der Identifikationslösung, also der konkrete Anwendungsfall, ist der Moment, in dem sich der Identitätsgeber authentisieren möchte oder soll und der Identitätsabfrager die digitale Identität oder die Entität identifizieren bzw. authentifizieren möchte. Hierbei möchte er ggf. sowohl wissen, ob der digitale Datensatz, also die digitale Identität, integer ist und ob sie eindeutig und sicher mit der Entität verbunden ist. Der Moment der Nutzung ist somit der eigentliche Schritt auf den alle vorherigen Schritte hinarbeiten. Auch der nachgelagerte Schritt der Löschung ist auf das Funktionieren dieses Schrittes ausgerichtet. Wie bereits in Kapitel 3.1.4 thematisiert, ist der Schritt der Nutzung (also der Anwendungsfall) auch der maßgebende Schritt für die Gestaltung der anderen Schritte.

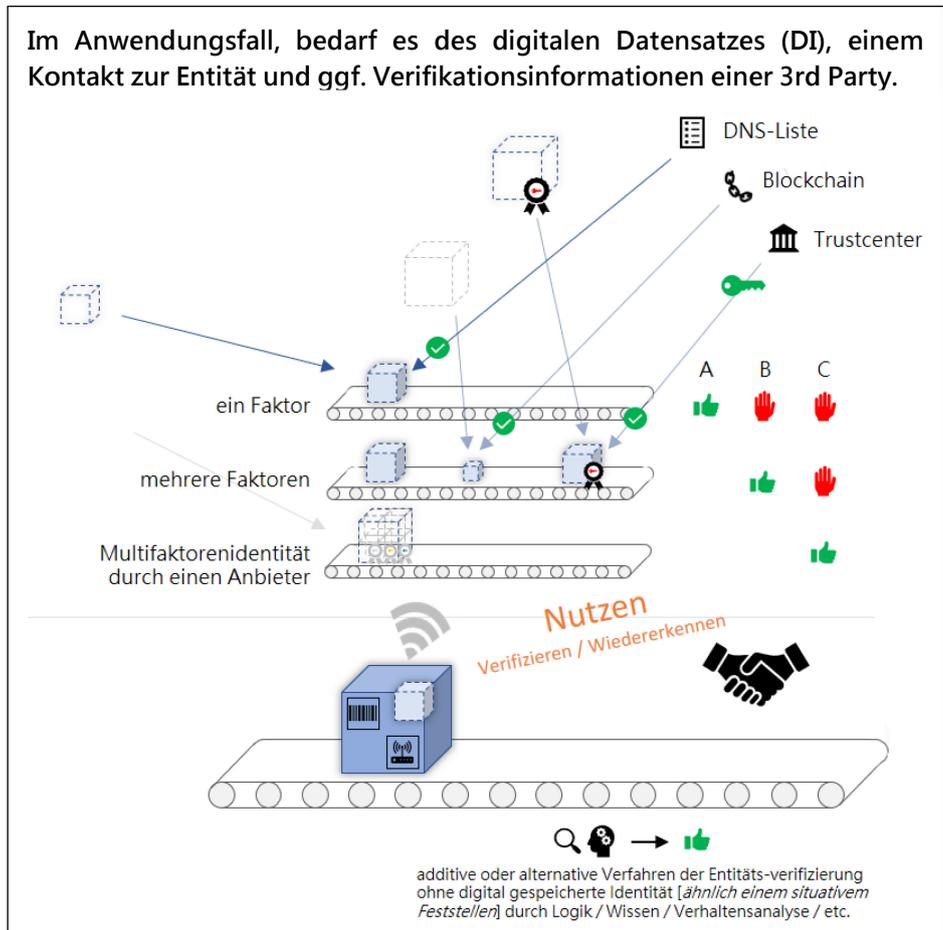


Abbildung 27 – Nutzen / Einsatz der Identitätslösung

Für den Moment des Verifizierens müsste zunächst einmal der digitale Datensatz, also die Identität, greifbar und die Entität kontaktierbar sein, damit das Abfragen des Sicherheitsmerkmals, des Passwortes oder der Zugang zum Secure Element o.ä., also der Technik, die zur Authentisierung notwendig ist, erfolgen kann. Grundsätzlich, aber insbesondere aus Sicht des Kapitels 3.2.4, also der Identitätslösungen im Rahmen der Interaktion von Verantwortungsbereichen bzw. Domänen, ist für das sichere Authentifizieren, zusätzlich der Zugang zu einer dritten Instanz / 3rd Party notwendig. Hierarchische PKI-Systeme und deren Zertifikaterstellung sind hier der Standard.

3.2.6.1 Nutzen einer dritten Instanz / 3rd Party am Beispiel PKI

Unter dem Begriff Public-Key Infrastruktur (PKI) werden die Instanzen zusammengefasst, die für den Einsatz asymmetrischer Kryptographie (insbesondere digitaler Signaturen) in offenen Systemen erforderlich sind. Hierzu gehören:

- Zertifizierungsstelle (Certification Authority, CA): stellt die CA-Zertifikate bereit und übernimmt die Signatur von Zertifizierungsanträgen
- Registrierungsstelle (Registration Authority, RA): hier können Personen, Maschinen oder untergeordnete Zertifizierungsstellen Zertifikate beantragen; nach Prüfung der Richtigkeit der Daten für das gewünschte Zertifikat genehmigt die RA den Zertifizierungsantrag; dieser wird durch die CA signiert
- Validierungsdienst (Validation Authority, VA): ermöglicht die Überprüfung von Zertifikaten in Echtzeit
- Subscriber: Inhaber eines Zertifikates
- Participants: Nutzer der Zertifikate

Zu den wichtigsten Aufgaben einer PKI zählen die Registrierung der Nutzer sowie das Ausstellen, Verwalten und ggf. Prüfen von Zertifikaten, welche die Grundlage für die informationstechnische Fälschungssicherung darstellen.

Die PKI beschreibt die Hierarchie von digitalen Zertifikaten und basiert auf der asymmetrischen Verschlüsselung.

Hierbei wird für jede erforderliche verschlüsselte Kommunikation, ein Schlüsselpaar erstellt, welches aus einem privaten (geheimen) und einem öffentlichen Schlüssel besteht. Das Schlüsselpaar wird so generiert, dass jede Datei, die mit einem öffentlichen Schlüssel des Empfängers verschlüsselt wurde, nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden kann. Außerdem ist es mit demselben privaten Schlüssel möglich, eine Datei digital zu signieren und somit für andere Personen unveränderbar zu machen. Mit Hilfe des öffentlichen Schlüssels des Absenders kann geprüft werden, ob die Datei seit der Signatur unverändert ist.

Ebenfalls können zwei Kommunikationspartner mit dem PKI System einander sicher Nachrichten senden, indem sie ihre Zertifikate austauschen, um Nachrichten so zu verschlüsseln, dass sie nur der jeweils andere entschlüsseln kann. Zusätzlich können sie auch die digitale Signatur des anderen überprüfen. Bei dieser Form der Überprüfung der Identität (der Nachricht) ist es erforderlich, die Identität des Kommunikationspartners zu kennen, auch wenn dieser nicht physisch kennengelernt werden kann. Nur so kann das Zertifikat sicher dem Kommunikationspartner zugeordnet werden.

Die Beweiskraft elektronischer Dokumente hängt entscheidend davon ab, ob Urheber und Inhalt, aber auch der Erstellungszeitpunkt zweifelsfrei und fälschungssicher feststellbar sind. Aus diesem Grund spielen neben digitalen Signaturen auch Zeitstempeldienste eine wichtige Rolle für die vertrauenswürdige elektronische Kommunikation.

3.2.6.2 Blockchain – Alternative zur PKI

Die Integrität von Daten wird vielfach mit Hilfe digitaler Signaturen gewährleistet. Sie stellen nicht nur sicher, dass z. B. eine Person den Inhalt eines Dokuments bestätigt (vergleichbar mit der Unterschrift), sondern auch, dass ein Dokument seit seiner Unterschrift nicht verändert wurde.

Bei Blockchain wird ähnlich wie bei Signaturen ein eindeutiger Fingerabdruck des Datensatzes erstellt, ein sogenannter Hashwert. Er wird über eine mathematische Funktion berechnet und ändert sich, sobald sich der Datensatz auch nur minimal ändert. Der Hashwert ist außerdem unidirektional, das bedeutet, dass man zwar aus dem Originaldatensatz den Hashwert berechnen kann, aber nicht umgekehrt vom Hashwert auf den ursprünglichen Datensatz schließen kann. Wird der Hashwert in einer Blockchain hinterlegt, kann auch dieser nicht mehr geändert werden.

Somit kann für einzelne Daten die Integrität über eine Blockchain überprüft werden. Erste Prototypen für die Abbildung digitaler Identitäten existieren bereits. Dabei werden Hashwerte über eine Menge von Identitätsattributen gebildet und in einer Blockchain abgelegt. Ziel ist es, die Integrität der Identitätsattribute sicherzustellen. Man kann diese Identitätsattribute zusätzlich mit Zugriffsrechten für IT-Systeme verknüpfen. So kann z.B. ein dezentrales Rollen- und Rechtemanagement realisiert werden. In der Blockchain werden dabei zusätzlich zur Identität mit dieser verbundene Zugriffsrechte auf IT-Systeme hinterlegt, die dann von den einzelnen Systemen überprüft werden. Vor allem organisationsübergreifende Zugriffsrechte können über diesen Ansatz realisiert werden. Dazu bedarf es jedoch eines standardisierten Vorgehens.

Da alte Einträge in einer Blockchain nicht gelöscht werden sondern wie ein Journal erhalten bleiben, ist damit eine Historie aller erteilten, geänderten und widerrufenen Zugriffsrechte in einer Blockchain sichtbar.

3.2.6.3 Mehrfaktorabfrage

Die Mehrfaktorabfrage dient der Erhöhung der Sicherheit im Anwendungsfall, durch die Abfrage bzw. Überprüfung weiterer Merkmale oder durch die Hinzuziehung weiterer Identitäten. Einzelne Identitätslösungen nutzen bereits oft zwei Faktoren zur Identifikation. Dies kann auch durch verschiedene Identitätslösungen sukzessiv aufbauend sein. Beispiel: Eine Bestellung bei Amazon kann man in der Regel vornehmen, wenn man sich mit Email und Passwort eingeloggt hat. Möchte man aber beispielsweise ein Buch als Geschenk an einen Freund schicken lassen, also zu einer neuen Adresse, muss man erneut seine Kontodaten eingeben. Letzteres ist der 2. Faktor.]

3.2.6.4 Erkennen ohne wirkliche Identitätslösungen

Mit „Erkennen ohne wirkliche Identitätslösungen“ sind Techniken gemeint, bei denen kein Datensatz für die jeweilige Entität vorhanden ist. Daher geht es auch nicht um das eindeutige Identifizieren, sondern um ein Absichern bzw. Steigern der Sicherheit im Sinne von Kapitel 3.2.6.3 durch das logische Erkennen von Mustern oder Verhalten.

Ein Beispiel hierfür sind die bekannten CAPTCHA Tests (Zahlen / Bilder) auf Webseiten, um festzustellen, dass kein Roboter sondern ein Mensch einen Authentisierungsvorgang durchführt. (CAPTCHA bedeutet „Completely Automated Public Turing test to tell Computers and Humans Apart“) Oftmals werden sie eingesetzt, im Sinne des sukzessiven Schrittes, wenn das Passwort mehrfach falsch eingegeben wurde.

Ebenfalls zum „Erkennen ohne wirkliche Identitätslösung “ also für das Absichern der Interaktion im Netz kann die stetige Überprüfung der Ergebnisse der Interaktion zählen. Sie ist auch die standardmäßige Absicherung digitaler und sonstiger Interaktion. Also einfach zu überprüfen, ob das gemacht wird, was gemacht werden soll. An dieser Stelle interessiert den bzw. hinterfragt der Akteur (eigentlich Identitätsabfrager) nicht, wer dort oder was dort tatsächlich mit ihm interagiert, sondern nur, dass das Ergebnis das ist, was er möchte. Erst in dem Fall, dass nicht das passiert, was erwartet wird, wird nach einer Identifikation gefragt. Passiert das, was gewünscht ist, wird die Identität nicht hinterfragt bzw. gilt als integer.

3.2.7 Löschen, Archivieren, Reaktivieren der Identität

Wann ist eine digitale Identität zu löschen, wann ist sie zu archivieren, wann sollte sie reaktiviert werden können, was ist zu tun, wenn eine Entität die digitale Identität nicht mehr braucht (ggf. die Entität nicht mehr existiert) usw. – diese Fragen spielen eine deutlich größere Rolle bei der Konstruktion von Sicheren Digitalen Identitäten, als man annehmen mag.

Zunächst einmal steigt mit der Dauer der Existenz einer Identität die Wahrscheinlichkeit, dass sie korrumpiert ist. Aus diesem Grund sehen viele Experten digitale Identitäten nur als sicher an, wenn sie ein – nicht in allzu weiter Ferne liegendes – Ablaufdatum besitzen. Dies kann gegebenenfalls durch automatisiertes Verwerfen geregelt werden. Gleichzeitig ist dies aber ein Problem. Z.B. könnte mangels Konnektivität die Identität eines Teils einer Industrieanlage ablaufen und so den gesamten Produktionsprozess gefährden.



Abbildung 28 – Ende des Lebenszyklus von Identitäten

Hoch relevant für die Gesamtkonstruktion einer SDI Struktur ist, dass bei Ausscheiden, Verlust oder Ähnlichem von Entitäten bzw. beim ungültig werden von Identitäten diese Statusänderung an die beteiligten Parteien kommuniziert wird. Dies gilt vor allem dahingehend, dass digitale Identitäten u.a. zur Autorisierung für die Benutzung bestimmter Bereiche gedacht sind. Arbeiten Unternehmen A und Unternehmen B bspw. an einem gemeinsamen Projekt und scheidet ein Mitarbeiter aus Unternehmen A aus, wäre Unternehmen B zwingend zu informieren, wenn hier Bereiche für den ausgeschiedenen Mitarbeiter noch offen stehen.

Funktionen bzw. rollenbasierte Berechtigungen müssen nach Ablauf einer bestimmten Zeit überprüft werden, um festzustellen, ob Identität und Entität noch zusammen passen. Insbesondere bei Personen ist darauf zu achten, dass z.B. durch Wechsel von Aufgaben innerhalb einer Organisation sich auch die Zugriffsrechte zu Anwendungen und Daten ändern.

3.3 Schaubild Gesamtsachverhalt

Dieses Kapitel verweist auf die Darstellung des vollständigen Schaubildes zum Gesamtsachverhalt, welches in den Kapiteln 3.1 und 3.2 eingeleitet wurde. Es stellt den notwendigerweise zu betrachtenden Gesamtsachverhalt, dessen Handlungsebenen sowie Schritte des Lebenszyklus dar, der in Gänze die Sicherheit von Identitätslösungen beeinflusst.

Bei der weiteren Gestaltung der Roadmap kann die Darstellung des Gesamtsachverhalts genutzt werden, um Ausrichtung und Wirkungsbereiche von vorhandenen Initiativen, Lösungen, Normen und Gesetze zu verorten und Handlungsbedarf zu identifizieren.

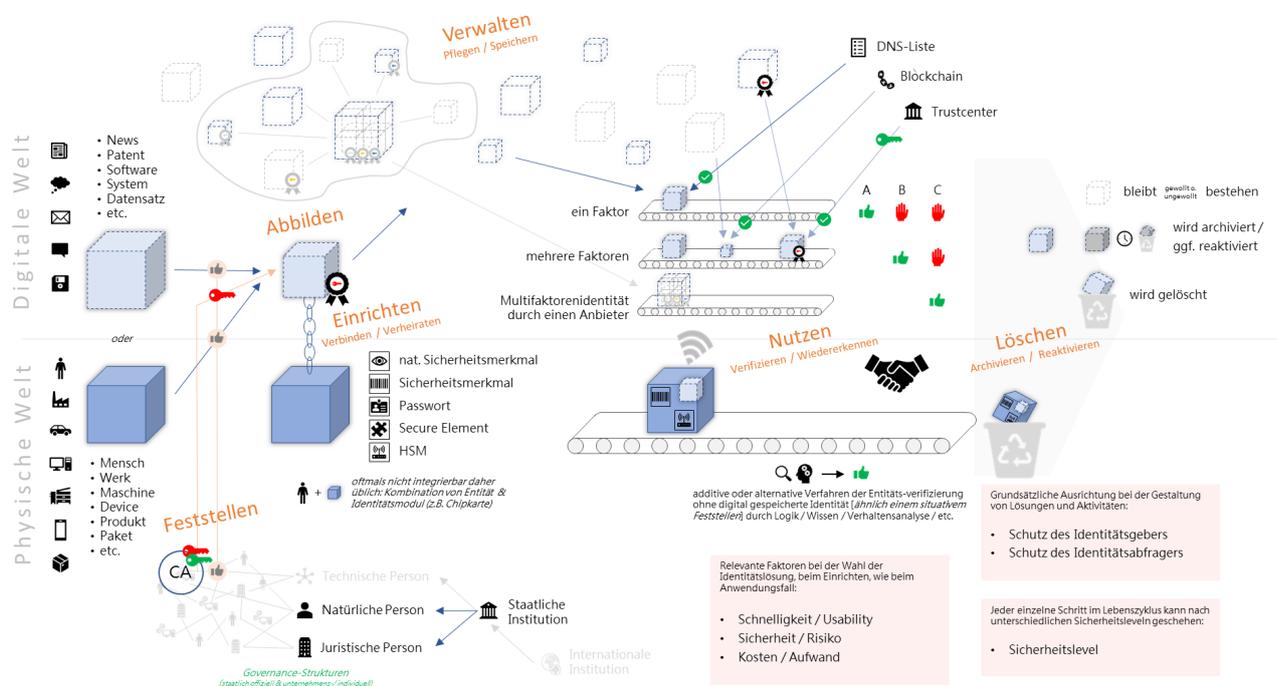


Abbildung 29 – Gesamtsachverhalt SDI mit seinen Handlungsschritten/ebenen (große Version s. Anhang 6.1)

3.4 Strategische Beispiele

3.4.1 Von Markenrechtsverletzungen bis zu unsicheren Bauteilen – Produktfälschungen, durch standardisierte SDI ein Thema von gestern

Grundsätzlich wäre es möglich, annähernd jedes Produkt oder Bauteil einfach per App auf seine Echtheit zu prüfen. Basis wäre das eineindeutige (einmalige) Sicherheitsmerkmal für jede produzierte Einheit und eine einheitliche digitale Abbildung. Die Voraussetzungen für solch neue Services sowie den einfachen Zugang von KMU zu selbigen wären internationale Absprachen bzw. Standards.



Abbildung 30 – SDI machen es möglich, mit dem Smartphone Produkte auf Echtheit prüfen

Neben dem Umsatz, der Unternehmen durch nachgemachte Produkte und Zulieferteile verloren geht, schaden qualitativ minderwertige Kopien dem Ansehen der Originalmarke. Vor allem können sie aber für den Käufer unmittelbar gefährlich sein. Produkte und Bauteile auf ihre Echtheit zu überprüfen, ist im digitalen Zeitalter jedoch einfacher geworden. Beim Bremsenhersteller ATE ist es bspw. per Abscannen des QR-Codes mit dem Smartphone und der ATE-App möglich, exakt das vorliegende Ersatzteil zu verifizieren. Das Prinzip hat hinsichtlich verschreibungspflichtiger Medikamente auch der Gesetzgeber erkannt und reagiert. Am 09.02.2019 tritt daher die Richtlinie 2011/62/EU in

Kraft nach der es Pflicht wird, eine einmalige Seriennummer je Medikamentenpackung zu vergeben, die mit individuellen Produktionsdaten in Form eines Data Matrix Codes verbunden ist. Dieser muss verlässlich generiert, verwaltet und reportet werden und erlaubt so die Prüfung, ob das jeweilige Medikament bzw. eben genau diese eine Packung auch so produziert wurde und in den Verkauf gegangen ist.

Die Kombination aus einem eineindeutigen Sicherheitsmerkmal am einzelnen Produkt und einem digital abfragbaren Verifikationsdatensatz sowie die Verbindung mit einem möglicherweise intelligenten Analysesystem (bspw. Warnung bei zeitnaher Abfrage aus unterschiedlichen Erdteilen) macht je nach Qualität und Marktdurchdringung Produktfälschungen unrentabel und generiert auf diesen Bedarfsfall bezogen „Sichere Digitale Identitäten“. Die Marktdurchdringung, in dem Sinne, dass davon auszugehen ist, dass genügend Akteure das System nutzen und so eine ausreichende Anzahl an Plagiaten erkannt werden, spielt hierbei eine maßgebende Rolle. Erst durch sie zerschlägt sich der Business Case des Fälschens und aus der Digitalen Identität wird eine sichere.

Hersteller-, produktgruppen- und branchenübergreifende Identitätslösungen, die zur breiten Nutzung beitragen könnten, werden grundsätzlich in der Zukunft möglich, ggf. in Form einer App, mit der ein beliebiges Produkt verifiziert werden kann. Die notwendige Eineindeutigkeit bspw. einer Seriennummer über alle Produktgruppen hinweg sowie die Interoperabilität der zugehörigen Datensätze und Verfahren können durch Normen und Standards herbeigeführt werden. Durch sie werden neue Formen der Services möglich und zudem eine Nutzung durch KMU vereinfacht.

3.4.2 SDI - mit Standards potentiellen Sicherheitslücken begegnen

Im Herbst 2017 stellte sich heraus, dass ein für SDI notwendiger und weltweit seit 2012 (sogar für Pässe) eingesetzter Sicherheitschip eine Sicherheitslücke aufweist. Updates können diese Lücke in vielen Fällen schließen. Aber es bleibt ungeklärt, ob alle Hersteller, die den Chip verbauten, mitziehen. Standards können dies explizit einfordern.

Eines der zentralen Elemente einer Sicheren Digitalen Identität ist das Verbindungselement zwischen der Entität und dem Datensatz, der die Digitale Identität darstellt. Häufig werden hierfür spezielle Chips, sogenannte Trusted Plattform Module (TPMs), eingesetzt. Sie enthalten einen eindeutigen kryptografischen Schlüssel, der zur Identifizierung des Gerätes genutzt werden kann.

Im Herbst 2017 stellte sich heraus, dass TPMs von Infineon seit 2012 eine Sicherheitslücke aufwiesen. Hunderttausende bis mehrere Millionen Embedded-Systeme, Notebooks, mobile Endgeräte, Smartcards und USB-Dongles zur hardwarebasierten Identifizierung sowie Personalausweise und Reisepässe sind davon betroffen. Identitätsdiebstahl, das Entschlüsseln sensibler Daten oder das Einschleusen von Schadcode in digital signierte Software wären somit möglich. Infineon gab an, dass es mit den betroffenen Herstellern zusammenarbeitet, um den Update-Prozess voranzutreiben. Wesentliche Teile der betroffenen Hersteller haben hier auch schon gehandelt. Allerdings steht aus, ob dies alle tatsächlich tun.



Abbildung 31 – Sicherheit ist nicht auf Dauer – Standards können den Umgang mit neu entdeckten Sicherheitslücken regeln und so bspw. im Rahmen von Sicherheitsleveln Updateverweigerungen einen Riegel vorschieben

Es ist nicht ungewöhnlich, dass Sicherheitslücken – auch bei der Gestaltung von Sicheren Digitalen Identitäten – auftreten. Manchmal bestanden sie von Anfang an und wurden nur übersehen oder sie entstanden durch neue Technologien und neues Wissen erst nach der Herstellung und dem Einsatz. Im ersten Fall können Standards, Sicherheitslevel und Zertifizierung zumindest vor einem Teil dieser Lücken schützen und dem Käufer dahingehend Sicherheit geben. Der zweite Fall ist dadurch hingegen nicht abdeckbar. Was aber in beiden Fällen idealerweise zu einem breiten Standard für IT-Geräte gehören könnte, wäre die Informationspflicht und die Updatepflicht innerhalb eines gewissen Rahmens. Denn sicherheitsrelevante Systeme müssten im Prinzip ohne weitere Schutzmechanismen nicht aktualisierte oder nicht mehr updatefähige Geräte ausschließen. Wenn es sich zudem um ein solch wesentliches und vielfach verbautes Sicherheitstool wie TPMs handelt (welches ja mit einer angenommenen Relevanz verbaut wird), können Updateverweigerer fatale Konsequenzen verursachen.

3.4.3 Fake News den Boden entziehen mit SDI

SDI für Datensätze und somit prinzipiell auch für Nachrichten sind in unterschiedlicher Weise vorhanden. Spezielle Systeme, die deutlich über ein vermeintliches Logo hinausgehen, um Herkunft und Veränderung erkennbar zu machen, sind in Entwicklung. Ein Schulterschluss von Nachrichten produzierenden Akteuren (Nachrichtenagenturen, Pressestellen und journalistischen Häuser), um sukzessive ein diesbezügliches Standardvorgehen aufzubauen, welches internationalisierbar wäre und Ansätze für unterschiedliche Sozialen Netzwerke und Medien bietet, wäre denkbar.



Abbildung 32 – Fake or Real? - Um diese Frage entscheiden zu können, gibt es bessere Lösungen als ein eingefügtes Logo oder Quellenbezug der vermeintlichen Quelle.

Fake News sind derzeit vielleicht eine der größten gesellschaftlichen Gefahren. Neben direktem wirtschaftlichen Schaden (2016 sackte bspw. der Börsenkurs des Baukonzerns Vinci aufgrund einer gefälschten Pressemitteilung kurzzeitig um 16% ab) vermag vor allem die beeinträchtigte politische Meinungsbildung nachhaltig das Gesellschaftsgefüge ins Wanken zu bringen. Dass es derzeit keinen Standard oder keine allgemeingültige Herangehensweise dafür gibt, wie im Internet die Provenienz – also der Ursprung und damit die Verlässlichkeit – einer Nachricht bestimmt oder festgehalten wird, ist ein Nährboden für Falschmeldungen. Sehr wohl gibt es aber die unterschiedlichsten

technischen Identitätslösungen für Datensätze und somit im Prinzip auch für Nachrichten, die weit über das Einfügen eines Logos bzw. einer nicht unmittelbar nachverfolgbaren Quellenangabe hinausgehen.

Konkret arbeiten die TU Berlin und die Bundesdruckerei derzeit bspw. an einem Lösungsmodell auf Basis von Blockchain-Technologien. Dabei werden im Internet die Informationen eines Autors untrennbar mit einem persönlichen Zertifikat verbunden. Sie erhalten also eine Sichere Digitale Identität. Werden diese Informationen von Dritten weiterbearbeitet, werden deren Zertifikate hinzugefügt. So entsteht eine Zertifikatskette, die stets nachvollziehbar macht, von wem die Information stammt und wer sie wie verändert hat. Sollte ein „Fake-News-Autor“ die Informationen aus dem Kontext reißen oder Bilder manipulieren, würde die Zertifikatskette dies abbilden und der Nutzer die Manipulation erkennen.

Unabhängig davon, ob dieses Modell die Kerntechnik eines Gesamtsystems darstellt, dass es Fake News schwieriger macht, Bedeutung zu erlangen; es sind internationalisierbare Standardvorgehen anzustreben, die interoperabel und auch in den unterschiedlichen Sozialen Netzwerken und Medien nutzbar sind und zudem fähig sind, diese zu überdauern. Adaption in oder aus anderen Domänen, wie der Geschäfts- und internen Unternehmenskommunikation, Wissensmanagement oder Plagiatsschutz sind dabei wahrscheinlich. Ein möglicher Schritt wäre ein Schulterschluss (insb. der Nachrichten produzierenden Einrichtungen, die Presseagenturen, die journalistischen Häuser, wie auch die Pressestellen von Unternehmen, staatlichen Einrichtungen etc.) hinter einem solchen Ansatz, Sichere Digitale Identitäten für Informationen bzw. Nachrichtenmeldungen zu nutzen.

3.4.4 Anbieten von „SDI “ als sekundäres Geschäftsmodell, geht das?

Einige große Anbieter von Identitätslösungen für Personen im Internet (*und auch wahrscheinlich bald zunehmend für andere Entitäten bspw. im Industriebereich*) sind herausragend im sicheren Identifizieren. Die Generierung, Analyse und intelligente Zusammenführung von Daten ist ihre Kernkompetenz. Auf ihr fußen ihre unzähligen Geschäftsmodelle auch für Dritte. Experten und Anwender verstehen unter SDI allerdings nicht nur die sichere Identifikation, sondern auch die Sicherheit der Daten zu einer Entität. Standards können dies explizit adressieren.

Anbieter von diversen Internetservices, sozialen Medien und Suchmaschinen erstellen Nutzerprofile. Dem stimmt die Person, die den Service nutzen möchte, bei ihrer Anmeldung zu. Mithilfe dieser Nutzerprofile sollen dem Nutzer bessere Ergebnisse des Services zur Verfügung gestellt werden, gezielte Zusatzinformationen (Werbung) dargeboten oder andere Services für Dritte angeboten werden. Zunächst findet die Identifikation in der Regel über eine E-Mail und die Vergabe des Passwortes statt. Später kommen ggf. weitere Abfragen hinzu, wie Kontodaten, Telefonnummer und Bestätigungsvorgang per SMS usw. Der Datensatz im Sinne von Informationen über die Entität, also die Digitale Identität, wächst. Da weiterhin der prinzipielle Login über das Passwort und E-Mail erfolgt, wird stetig mit Sekundärdaten überprüft bzw. die Wahrscheinlichkeit bestimmt, ob das Gegenüber auch weiterhin dasjenige ist, das es vorgibt zu sein. Bspw. geschieht dies über das Abgleichen der IP-Adresse oder die Analyse des aktuellen Verhaltens im Vergleich mit dem Nutzerprofil auf der jeweiligen Plattform. Weicht dieses ab, wird auch zur Sicherheit des Nutzers in der Regel eine neue Abfrage von Verifikationsdaten vorgenommen (Bestellen Sie bspw. bei Amazon etwas an eine neue Adresse, müssen Sie die Kontodaten erneut eingeben.).

Zumeist in der Verbindung mit dem praktischen „eingelogg bleiben“, kann mithilfe so genannter Cookies die Informationssammlung zu Nutzerprofilen deutlich über das Verhalten auf der jeweiligen Plattform hinaus erweitert werden. Sogenannte Third-Party Cookies werden hierbei eingesetzt, um auch über Partnerwebsites noch weitere Informationen zum Nutzer sammeln zu können. Je nachdem, welche Cookie-Art benutzt wird, ist man damit eindeutig identifizierbar. So wurden 2013 Googles Tracking Cookies mit einem Eintrag „PREFID“ bekannt, die dies ermöglichen. Prinzipiell wäre es einigen Anbietern sogar nur über die Informationsverknüpfung stets vorhandener system- und browserspezifischer Daten und/oder des Verhaltens und/oder IP-Adressen etc. eine Identifikation ohne Einloggen des Nutzers vorzunehmen.



Abbildung 33 – Viele Informationen über eine Entität zu besitzen, kann das Identifizieren einfacher und sicherer machen. Es ist aber nicht notwendig.

Heute wird Identitätsmanagement ganz explizit von Organisationen angeboten, deren primäres Geschäftsmodell in einem anderen Bereich wie zum Beispiel auf dem Sammeln von Daten und daraus generiertem Mehrwert liegt. Das Angebot dieser Organisationen bringt u.U. viele Vorteile mit sich, da diverse zusätzliche Funktionen hiermit verbunden sein können. Zudem ist eine sichere Identifizierung durch solch eine Multifaktorenprüfung sehr wahrscheinlich. Aber kann man hier auch von Sicheren Digitalen Identitäten sprechen? Ein Großteil der IT-Experten verbindet mit dem Begriff auch die Sicherheit und weitestgehende Souveränität über die Daten einer Entität.

Es braucht daher eine gemeinsame Definition und Standards, die diese Bipolarität berücksichtigen – dies gilt nicht nur für Personen, sondern auch für Unternehmensdaten.

3.4.5 SDI sind der Enabler von Industrie 4.0 und anderen Zukunftsprojekten

Adhoc-Wertschöpfungs-Netzwerke zwischen Unternehmen sind die Kernidee der Industrie 4.0. Potentielle Teilnehmer müssen gewährleisten können, dass sie ihren Verantwortungsbereich sicher und interoperabel gestalten, sonst werden relevante Investitionen in das Thema an sich ausbleiben. SDI sind dabei die Voraussetzung jeglicher Sicherheitskonzepte. Die Industrie 4.0 zeigt in ihrer Mannigfaltigkeit, dass es dabei nicht um die eine Lösung, sondern um die unterschiedlichsten technischen und organisatorischen Sachverhalte geht. Es bedarf eines SDI-Frameworks, der Vorhandenes zusammenbringt und zu Standards führt, die Unternehmen einhalten können.

Industrie 4.0 basiert auf der Idee, dass adhoc-Wertschöpfungs-Netzwerke zwischen Unternehmen sogar auf verschiedenen Kontinenten gebildet werden können. Hierbei sollen auf diversen Ebenen Produktionsnetzwerke autark miteinander zusammenarbeiten. Dieser Prozess auf Arbeitsebene erfordert Vertrauen in den digitalen Austausch zwischen den Systemen und den jeweiligen Teilen. Für unterschiedliche Vorgänge in diesem Prozess, von Austausch von Produktionsdaten, Aushandeln von Preisen und Zeiten, Fernwartung von Maschinen, Lokalisierung von Produkten, Bestimmung von Bauteilen u.v.a.m. bedarf es einer sicheren Kommunikation und der Sicherheit, dass das Gegenüber, das ist, was es vorgibt zu sein.

Allein die Mannigfaltigkeit der Entitäten (Werkssystem, Software, Bauteile, Maschinen, Menschen, etc. pp.), die im Rahmen von Industrie 4.0 identifizierbar sein müssen, determiniert eine Vielzahl an technischen und organisatorischen Identitätslösungen. Darüber hinaus besteht jede Identitätslösung aus einem kompletten Prozess, der bei [a] der Autorisierung der Einheit anfängt, die das Feststellen der Identität vornimmt, [b] den unterschiedlichen Möglichkeiten, die Identität in einem Datensatz abzubilden, weitergeht (wie bspw. der Programmiersprache), [c] das Verbinden des Datensatzes mit der Entität über Sicherheitsmerkmale, vom Barcode bis hin zum eingeschweißten Hochsicherheitsmodul (welches eine kryptographiefähige abgesicherte Rechneinheit darstellt), [d] das Verwalten des Datensatzes und/oder Verifikationsschlüssel, [e] das Nutzen, Aktualisieren und Verifizieren (letzteres über PKI, Blockchain oder DNS-Systeme) dieser Einheit aus Datensatz und Entität und (f) den Umgang bzgl. Löschen, Archivieren oder Reaktivieren beinhaltet.



Abbildung 34 – Industrie 4.0 und die digitalen Zukunftsprojekte bedürfen Identitätslösungen vom Datensatz bis hin zur Werkanlage, vom Mensch bis zur Maschine

Alle diese Schritte können unterschiedlich gestaltet werden und potenzieren die möglichen Identitätslösungen. Das Konzept nochmals erweiternd lassen sich zudem wiederum Identitätslösungen sukzessive miteinander kombinieren. Determiniert wird die Wahl der Lösungen dann, neben den gegebenen Bedingungen durch die Beschaffenheit der Entität, durch die Faktoren: [1] benötigte Schnelligkeit, [2] verursachte Kosten/Aufwand und [3] mit einer fehlerhaften Identifizierung zusammenhängenden Risiko (monetär oder bzgl. der Unversehrtheit von Menschen). Insbesondere das Risiko bestimmt dabei den benötigten Sicherheitslevel im Anwendungsfall.

Es gibt auf jeder dieser Ebenen bereits umgesetzte technische oder organisatorische Lösungen. Mit zentralen Werken, wie bspw. der ISO/IEC 29115, der IEC 62443, der ISO/IEC 24760 oder der ISO 15408 stehen sowohl strukturgebende Normen als auch standardisierte spezifischere Herangehensweisen für wesentliche Teilbereiche zur Verfügung. Es gibt allerdings keinen Standard, der einen Rahmen schafft, der die gesammelten Erfordernisse von Industrie 4.0 und anderen Zukunftsprojekten abbildet. Es fehlen anwendbare Metastandards und Spezifikationen für weite Teilbereiche. Zudem ist das Vorhandene fragmentiert und teilweise nicht kompatibel. So finden sich zum Beispiel bereits in den genannten Werken unterschiedliche Ansätze für Sicherheitslevel. Es fehlt der rote Faden, ein internationales Framework.

Aus diesem Framework kann ein Standard entstehen, der es Unternehmen, von Konzernen bis KMU, im Hinblick auf Industrie 4.0 ermöglicht eine SDI-Struktur aufzubauen, die interoperabel ist und Vertrauen schafft – zunächst vielleicht nur als Selbsterklärung, später ggf. als zertifiziertes Unternehmen. Nur ein solcher Standard vermag die Sicherheit zu schaffen, die zu entscheidenden Investitionen führt und das Zukunftsprojekt Industrie 4.0 real werden lässt.

3.4.6 Vom Smart Meter Gateway lernen - jedem Anwendungsfall seine SDI

Die Frage nach SDI sollte eigentlich die Frage danach sein, in welchem Anwendungsfall welche Identitätslösung als ausreichend sicher angesehen werden kann. Das Smart Meter Gateway (SMGW) gilt hier als eine der Hochsicherheitslösungen, die stets exemplarisch genannt wird, deren Sicherheit aber in diesem oder jenem Szenario in keinem Fall benötigt wird. Entwicklungen um das SMGW zeigen aber gleichzeitig, dass die Sicherheit von digitalen Identitäten immer im System zu betrachten ist und zumindest Knotenpunkte mit einer hochsicheren Identität den Entitäten dahinter generell mehr Vertrauen geben können.

In Zukunft werden Zähler u.a. für Strom, Gas, Wasser, Wärme sowie steuerbare Energieverbraucher bzw. Energieerzeuger in einem intelligenten Messsystem mit einem SMGW verbunden, welches die Messdaten empfängt, speichert und diese für Marktakteure aufbereitet. Alle Kommunikationsflüsse sind verschlüsselt und in Bezug auf

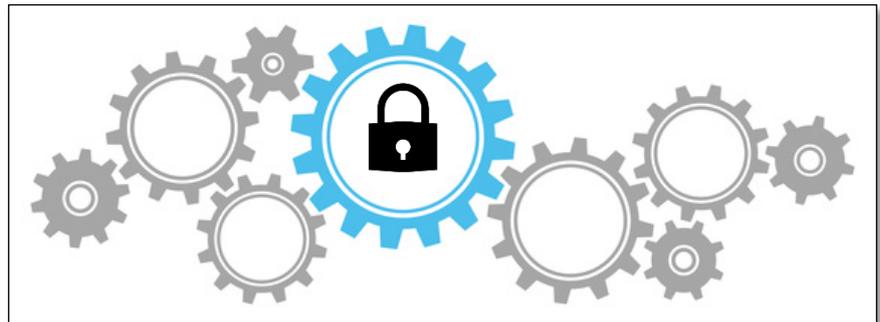


Abbildung 35 – Knoten- und Zusatzpunkt mit hochsicheren Identitäten können zur Steigerung der Sicherheit damit verbundener Entitäten dienen

Integrität, Authentizität und Vertraulichkeit abgesichert. Das SMGW bedient sich hierzu eines sogenannten Sicherheitsmoduls, das zum einen als sicherer Speicher für das zur Verschlüsselung erforderliche kryptographische Schlüsselmaterial dient und zum anderen kryptographische Kernroutinen für Signaturerstellung und -prüfung, Schlüsselgenerierung, Schlüsselaushandlung sowie Zufallszahlengenerierung bereitstellt. Es verfügt in diesem Sinne definitiv über eine Sichere Digitale Identität.

Der Entstehungsprozess und die Gestaltung des Smart Meter Gateways trifft vielerorts aber auf Kritik. Die Sicherheitsbestimmungen werden oftmals als überdimensioniert angesehen und für andere Anwendungsbereiche als nicht beispielhaft. Insbesondere der derzeit bereits über ein Jahr dauernde Zertifizierungsprozess gilt als nicht markttauglich. Da es aber die zentrale Kommunikationseinheit für sensible Daten bildet und es sich um einen regulierten Markt handelt, in dem das Smart Meter Gateway zur Pflicht wird und in dem zusätzliche eichrechtlichen Anforderungen gelten, wurde ein sehr hoher Sicherheitsstandard gewählt.

Die Kritik und der lange Prozess (bis heute hat das Rollout nicht stattgefunden) machen deutlich, dass die höchste Sicherheit von Digitalen Identitäten nicht für alle Anwendungsfälle die richtige ist. Es braucht vielmehr eine Struktur/Heuristik, an welchen Schnittstellen und zu welchen Sachverhalten welches Level an Sicherheit die Identitätslösungen haben sollten. Hierfür gibt es bereits unterschiedliche Ansätze, die es voraussichtlich noch weiter zu differenzieren und möglichst domänenübergreifend zu harmonisieren gilt.

Das Smart Meter Gateway macht aber zudem deutlich, dass die Sicherheit von Digitalen Identitäten auch immer im System zu betrachten ist. Knoten- oder Zugangspunkte mit höchster Sicherheitsstufe können Entitäten „dahinter“, ja sogar ganzen Systemen mehr Sicherheit verleihen. Ein Framework mit anwendungsbezogenen Standards für Unternehmen etc. kann so etwas adressieren. Unabhängig von

seinem energiewirtschaftlichen Hintergrund führte das SMGW in seiner Knotenfunktion als hochsicherer Kommunikationskanal nämlich aktuell dazu, dass Anbieter beabsichtigen, innovative Dienstleistungen wie für Security- oder Smart-Health-Anwendungen darüber zu betreiben. In diesem Sinne kann ein domänenübergreifendes Konsortium Innovationspotentiale aus unterschiedlich bestehenden Lösungen entwickeln. und unter Federführung der Normungsorganisationen domänenübergreifende Plattformen etablieren.

4 Ergebniszusammenführung zu Kernaussagen und Schlussfolgerungen zur Situationsbestimmung und Herleitung der Handlungsbedarfe

Die Informationen aus Expertenkonsultation, Normen- und Rechtsrecherche, sowie die Ableitungen aus der Ergebniszusammenführung zur Sach- und Prozessbeschreibung lassen sich zu einem (auch wertenden) Gesamtbild zusammenfügen aus denen sich die im Folgenden dargestellten Kernaussagen und Schlussfolgerungen ergeben. Wesentliche Teile der Expertenkonsultation gestalteten sich dahingehend als ein gemeinsames Eruiere / Nachdenken darüber, wie dem Sachverhalt SDI begegnet werden kann. In diesem Sinne sind auch die folgenden Ausführungen zur Gestaltung maßgeblich unmittelbar in oder aus der Expertenkonsultation entstanden und Teil der Ergebniszusammenführung.

Feststellungen zur Situation

- 4.1 Relevanz
- 4.2 Hebel für digitale Sicherheit
- 4.3 Handlungsdruck
- 4.4 Keine One-Fits-All-Lösung möglich
- 4.5 Insellösungen am Markt
- 4.6 Insellösungen auch in der Standardisierung
- 4.7 Dreh- und Angelpunkt digitaler Systeme
- 4.8 Jedes Digitalisierungsprojekt braucht SDI
- 4.9 Die Domänen wachsen zusammen
- 4.10 Es geht nur international

Verbindendes Element >Referenzarchitektur< und deren Inhalt / inhaltliche Gestaltung

- 4.11 Ein gemeinsames Ziel (Referenzarchitektur/Framework)
- 4.12 Fokus Anwendungsfall (Sicherheitslevel, u.a.)
- 4.13 Fokus Lebenszyklus (Bestandteile von Identitätslösungen)
- 4.14 Anforderungsprofile nach Einsatz- und Verantwortungsbereich
- 4.15 Anwendbarkeit der Referenzarchitektur
- 4.16 Es wird nicht bei Null angefangen (Grundlagen / Ergebnisse)

Herangehensweise an die Entwicklung und Implementierung einer >Referenzarchitektur<

- 4.17 Ein domänenübergreifendes Netzwerk als Alleinstellungsmerkmal
- 4.18 Die Antwort auf Internationalisierung: Normung
- 4.19 Industrie 4.0 – Potential zum Leitmodell
- 4.20 Auswirkungen – über die digitale Welt hinaus
- 4.21 Auswirkungen – Forschungs- und Infrastrukturbedarf
- 4.22 Auswirkungen – juristischer und gesetzlicher Art
- 4.23 Politisches Engagement notwendig

4.1 Relevanz

Das Thema SDI ist von elementarer Relevanz für Gesellschaft, Wirtschaft und Staat - Wofür SDI stehen, wird dabei allerdings unterschiedlich interpretiert.

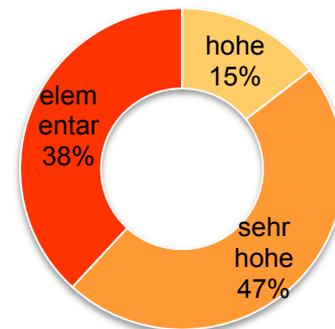
Unabhängig von der aus der Sachverhaltsanalyse abzuleitenden Bedeutung, zeigten die Aussagen der befragten Experten ganz klar eine Richtung: Das Thema „Sichere Digitale Identitäten“ und dessen, was sie damit verbunden sehen, ist von außerordentlicher Relevanz für Gesellschaft, Wirtschaft und Staat. Keine der befragten Personen stufte das Thema als irrelevant ein. Über 85% der Personen, die eine Aussage zur Relevanz tätigten, sahen vielmehr eine sehr hohe bis hin zu elementare Bedeutung für das Gelingen der digitalen Transformation.

Allerdings muss die Aussage über die Relevanz in verschiedener Weise differenziert werden. Insbesondere dahingehend, dass unter dem Begriff SDI zwar zusammengehörende aber verschiedene Sachverhalte assoziiert werden und verschiedene Erwartungen bestehen. Für einen Teil der Befragten bedeuten SDI die Sicherheit der eigenen Daten bzw. des Identitätsgebers, für den anderen Teil steht aber das sichere ggf. uneindeutige Bestimmen einer Entität bzw. eines Identitätsgebers im Fokus; d.h. die Betrachtung von SDI rein aus Sicht des Identitätsabfragenden (vgl. zum Thema Kapitel 3.1.1). Eine dritte Gruppe der Befragten verlangt, dass SDI beide Interessen bedienen bzw. ihre Sicht fokussiert den Anwendungsfall, der jeweilig eine Gewichtung verlangt.

Einzelne Experten haben gefordert, dass Inhalt und Zielsetzung des Konzepts SDI zunächst genauer definiert werden müssten. In diesen Aussagen zeigte sich im Prinzip die einzig wirkliche Relativierung der Relevanz von SDI. Denn für einige Use Cases, die man derzeit mit Identitätskonzepten löst oder zu lösen beabsichtigt, be- oder entstehen Konzepte, die mit Identitätslösungen nicht unmittelbar zusammenhängen - wie etwa logisches Erkennen und direkte Überprüfung der Handlungen. Auch diese Experten waren sich allerdings einig, dass SDI in jedem Fall eine fundamentale Rolle in der Digitalisierung zukommen wird.

SDI werden also als tragende Säulen der Digitalisierung gesehen, die eine Mindestsicherheit im Hinblick auf Referenzierbarkeit, Integrität von Interaktionen und

Generelle Einschätzung der Relevanz von SDI



% der im Sinne des Kap. 2.0 gewerteten Aussagen

„Der Bereich Identitäten ist elementar. Sie sind das Querschnittsthema der Digitalisierung. Wenn die Identitäten nicht sicher sind, worauf will ich dann aufbauen? Dann braucht man gar nicht weiterreden.“

„Die Sicherung physischer und elektronischer Identitäten wird immer mehr zu einem Kernthema unserer Gesellschaft.“

„Ansonsten droht sehr kurzfristig ein massiver gesellschaftlicher Schaden, der über den Zusammenbruch digitaler Kommunikationsmöglichkeiten bis hin zu ganz konkreten Schäden auf nicht digitale Vorgänge reicht (z.B. in der medizinischen Versorgung, der Energieversorgung, des Transports, der Tierzucht).“

„Eine weitergehende Digitalisierung wird [...] ohne SDI nicht möglich werden.“

„Im Zuge der digitalen Transformation werden 30% der Firmen wegen mangelnder digitaler Identitäten Marktanteile verlieren...“

„Im Hinblick auf das Thema ist auch die Schutzfunktion des Staates relevant.“

Zitate aus den Fragebögen /
Expertenkonsultationen

Interaktionspartnern sowie von Datensouveränität erwirken können. Gelingt es nicht eine solche Struktur zu gestalten und zu etablieren, droht massiver wirtschaftlicher und gesellschaftlicher Schaden und eine Gefahr für die Sicherstellung der Aufgaben des Staates (von der Durchsetzung des Rechtssystems im digitalen Raum bis hin zur Zivilen Sicherheit).

4.2 Hebel für digitale Sicherheit

SDI haben das Potential, der Hebel für eine grundlegend sicherere Gestaltung der Digitalisierung zu sein.

Die außerordentliche Relevanz, die dem Thema SDI zugesprochen wird, basiert maßgeblich auf der Annahme, dass mit SDI die digitale Welt grundsätzlich sicherer gestaltet werden kann – eine Herausforderung, die wohl zu den größten unserer Zeit gehört. SDI werden in diesem Sinne als Anker, Pfeiler oder Schlüssel für Verbindlichkeit und Vertrauen verstanden. Die Aussagen, die dies sinngemäß unterstreichen, sind über die Expertenkonsultation hinweg die mit am häufigsten getroffenen.

Zum einen sind SDI die Voraussetzung von IT-Sicherheit. Mit ihnen werden Rollen und Berechtigungen verknüpft und sie sind dadurch Basis sowohl für elementare als auch ausgefeilte Sicherheitskonzepte. Wenn Digitale Identitäten nicht sicher sind und sich z.B. Dritte ihrer bemächtigen können, laufen alle darauf aufbauenden Sicherheitsmaßnahmen ins Leere.

Zum anderen ermöglicht der Einsatz von SDI die Zurechenbarkeit, Verfolgbarkeit, Attributierbarkeit digitaler Vorgänge. Für Schuld- und Haftungsfragen im digitalen Raum bieten SDI somit einen unmittelbaren Ansatzpunkt. Der Aufbau einer Infrastruktur im Bereich Digitaler Identitäten mit einheitlich strukturierten Anforderungsprofilen könnte daher nicht nur mehr Sicherheit per se schaffen, sondern würde auch Sicherheitslücken leichter zurechenbar machen. Die jeweils Verantwortlichen würden identifizierbar. Der Anreiz zur sichereren Gestaltung digitaler Systeme, Produkte, etc. wäre deutlich höher.

Eine solche Struktur steigert darüber hinaus auch die Sicherheit aus Identitätsgebender Sicht. Es wird nachvollziehbar, zu wem die eigenen Daten im Anwendungsfall fließen. Darüber hinaus können aber auch die Interessen des Identitätsgebers in einer konzertierten Herangehensweise an SDI-Strukturen und Lösungen vom Design her Berücksichtigung finden. So ist bspw. nicht in jedem Anwendungsfall eine eindeutige Identifizierung notwendig.

Die häufigsten Aussagen, die das Potential von SDI als möglicher Hebel für mehr Sicherheit stützen

→ **37 mal** wurden direkte Aussagen getätigt, die sinngemäß „**SDI als Schlüssel für Verbindlichkeit und Vertrauen**“ adressierten

→ **44 mal** wurden direkte Aussagen getätigt, die sinngemäß „**SDI als Basis für IT-Sicherheitsmaßnahmen und/oder sichere Kommunikation**“ adressierten

→ **36 mal** wurden direkte Aussagen getätigt, die sinngemäß „**SDI als Basis für Transparenz i.S.v. Zurechenbarkeit, Authentizität und Haftungsfragen**“ adressierten

„Sichere Digitale Identitäten bedeuten Anker für Zurechenbarkeit, Haftbarkeit und somit sind sie Ansatzpunkt für das Rechtssystem. Daher sind sie auch der Ansatzpunkt, dass Akteure ihre Systeme, Prozesse etc. sicherer gestalten.“

„Sichere Identitäten sind der Ausgangspunkt für die Sicherheitskette, welche die Datenerhebung, den -transport und die -verarbeitung auf Hardware-, Software- und Prozessebene absichert.“

„Sichere Identitäten sind die Voraussetzung für viele Schutzmaßnahmen, in der Komponenten oder auch Prozesse eindeutig identifiziert und authentifiziert werden, damit Daten verarbeitet und weitergegeben werden können. Ist es an einer Stelle möglich eine unberechtigte Identität einzuschleusen, sind alle darauf aufbauenden oder folgenden Sicherheitsmaßnahmen hinfällig.“

„Der Kern jeder Interaktion und Kommunikation ist Vertrauen in die richtige digitale Identität, unabhängig, ob von Menschen, Maschinen, Dingen oder Prozessen. Erst wenn diese Voraussetzung erfüllt ist, können neue oder bestehende Abläufe verbessert werden oder Innovationen entstehen.“

Zitate aus den Fragebögen /
Expertenkonsultationen

4.3 Handlungsdruck

Begegnet die deutsche Wirtschaft und Politik dem Thema jetzt nicht mit Nachdruck, besteht die Gefahr, dass eines der wichtigsten Grundlagenthemen der Digitalisierung ohne sie definiert/umgesetzt wird.

„Die Lücken, die es zu füllen gilt, werden gefüllt werden.“ / „Wir müssen uns jetzt mal entscheiden, ob wir überhaupt noch mitgestalten wollen, oder nicht.“ sind zwei Aussagen aus Experteninterviews, welche die vorherrschende Einschätzung der aktuellen Situation widerspiegeln. Die Grundstrukturen der digitalen Welt werden derzeit gestaltet. Die Frage ist, wie dieser Prozess zu einem Ergebnis geführt werden kann, welches im Interesse unserer Gesellschaft, Wirtschaft und Politik liegt. So ist es bspw. möglich, flächendeckend Identitätslösungen zu erhalten, die zwar sicher im Sinne der Abfrager sind, aber in keiner Weise die Interessen der Identitätsgeber berücksichtigen (vgl. Kapitel 3; insb. 3.4.4) Dies gilt dabei für Geräte- und Industrieidentitäten in gleicher Weise wie für Personenidentitäten.

Zum einen werden bereits jetzt Lösungen von außereuropäischen Organisationen in den Markt gebracht, die andere Ziele verfolgen, als es von den Nutzern, sowie gesellschaftlich oder politisch gewünscht ist und die den Anbietern eine außerordentliche Machtstellung verschaffen. Initiativen wie DIPP / VeriMe bestätigen bspw. den Bedarf an dazu alternativen Lösungen. Die Interoperabilität, Einfachheit im Einsatz und Zusatznutzen für Identitätsabfrager, die diese Anbieter allerdings bieten, macht es für Alternativangebote sehr schwer – insbesondere, wenn es keine Vereinheitlichung von Anforderungsprofilen gibt.

Zum anderen treiben außereuropäische Akteure mit Macht das Thema Digitalisierung auf der Standardisierungs- und Strukturierungsebene voran. Wobei sich sich auf der einen Seite die großen digitalen Player aus unmittelbarem wirtschaftlichen Interesse engagieren und auf der anderen Seite das Thema durch staatliche Politik getrieben wird. Es bedarf daher dringend der einheitlichen Positionierung der deutschen und europäischen Wirtschaft und Gesellschaft zur Wahrung ihrer Interessen.

Notwendigkeit des Handelns adressierende Aussagen

→ **12 mal** wurden Aussagen getätigt, die sinngemäß aber ganz konkret einen **„schnellen Handlungsbedarf, den es mit Nachdruck zu verfolgen gilt“** adressierten

„Die Räume werden gefüllt. Notfalls aus dem Markt heraus. Dann gibt es halt den DeFacto-Standard Google und dann ist das halt so.“

„Hinsichtlich eines Produktansatzes werden die großen Portalbetreiber wie Facebook, Apple, Google und Microsoft neben der Authentisierung von Personen auch die Authentisierung von Objekten (bzw. "Dingen" im IoT) vorantreiben und nutzbar machen.“

„Wenn jetzt nicht gemeinsam strategisch und bedacht vorgegangen wird, wird es später teuer.“

„Weil es für alle nur ein Vehikel ist, um andere Geschäftsmodelle zu ermöglichen, stellt sich die Frage wessen Aufgabe es ist, das Identitätsmanagement zur Verfügung zu stellen. Ist es Kernaufgabe des Staates staatlicher Institutionen oder soll man das der Deutschen Bank und Axel Springer überlassen und sind diese vertrauenswürdiger als Google?“

„Da muss viel mehr Momentum dahinter, um da etwas auf die Beine zu stellen.“

„Ein technisch ausgereiftes Konzept einer solchen Identität, das den Bürger in den Mittelpunkt stellt, ... setzt einen Gegenpol zur Parallelwelt digitaler Identitäten, die von sozialen Netzwerken geschaffen wurde (v.a. von Unternehmen wie Google, Amazon, Facebook, Apple).“

„Wir müssen uns jetzt mal entscheiden, ob wir überhaupt noch mitgestalten wollen, oder nicht.“

Zitate aus den Fragebögen /
Expertenkonsultationen

4.4 Keine One-Fits-All-Lösung möglich

Die „eine technische Lösung “ für alle Fälle gibt es nicht – umso mehr braucht es das Nutzen von Harmonisierungs-, Strukturierungs- und Synergiepotentialen.

Da die Digitalisierung bezugnehmen wird auf so ziemlich jegliches Ding der physischen Welt, erklärt sich die Mannigfaltigkeit der Entitäten mit Identitätslösungsbedarf von selbst (vgl. Kap. 3.2.1). Digitale Identitäten sind dabei auch bereits überall vorhanden, denn ohne sie funktioniert keine digitale Interaktion. Die Sicherheit der digitalen Identitäten variiert aber extrem und weil die Bedeutung der Geschäftsabwicklung und der Interaktionen über und in der digitalen Ebene exorbitant zunimmt, wird die Frage nach „der Sichereren Digitalen Identität “ immer lauter. Vor und zu Beginn des Projektes wurde diesbezüglich gelegentlich die Hoffnung oder die Vermutung geäußert, es könne also eine zentrale technische (eine annähernde „One-Fits-All “) Lösung geben oder selbige also „die SDI “ könne entwickelt werden.

→ Die eine technische Lösung für alle Anwendungsfälle gibt es allerdings nicht! – Dies unterstreichen nicht nur die Aussagen der Experten in jeglicher Art (Sollte es nicht unmittelbar genannt worden sein, erschließt es sich i.d.R. aus dem Gesamtbild der Konsultation.), sondern auch die analytische Betrachtung des Gesamtsachverhalts (vgl. Kapitel 3). Eine technische Lösung für einen sehr weiten Anwendungsbereich durchsetzen zu wollen, die zwar eine hohe Sicherheit gewährleistet, aber hinsichtlich anderer Faktoren, wie Schnelligkeit, Usability, Kosten etc. nicht die Marktbedürfnisse erfüllt, kann sogar vielmehr den Digitalisierungsprozess, Innovationen und die Wettbewerbs-fähigkeit gefährden.

Eine Komplexitätsreduktion für die, die Identitätslösungen einsetzen, ist gerade daher aber zwingend. Das Finden von sinnvollen Lösungen für Teilbereiche (bspw. nach Entitäten und Vorbedingungen) gehört hier weiterhin dazu. Dies bezieht sich aber nicht nur auf eine Technik, sondern auf die unterschiedlichen Dimensionen des Themas, das Zusammenspiel der Bestandteile einer Lösung im Lebenszyklus, Einbettung, Sicherheitslevel etc. – wie sowohl im Kapitel 3 detaillierter beschrieben, als auch in den weiteren Schlussfolgerungen noch thematisiert.

→ über 100 mal wurden Aussagen getätigt, die sinngemäß adressierten „es gibt verschiedene Lösungen / die Wahl der richtigen Lösung ist UseCase-abhängig / es gibt nicht die eine Lösung“

„Also, die eierlegende Wollmilchsau ist da auch einfach illusorisch an der Stelle. Das ist halt auch einfach so.“

„Jedes Produkt und auch jeder SDI-UseCase hat nach unserer Auffassung seinen eigenen Fokus. Insofern können wir uns keine Lösung vorstellen, welche allen Ansprüchen gerecht wird.“

„Die Art der technischen Lösung hängt entscheidend vom Integritäts- und Sicherheitslevel sowie dem Kostenaufwand ab, der aus Sicht der Risikobewertung und der Risikobereitschaft des / der Stakeholder angemessen ist.“

„Die Schaffung von DI und SDI fängt bei der Zuteilung einfacher randomisierter Nummern an, die dem Produkt / Dokument zugeordnet werden und manipulations- und fälschungssicher auf dem Produkt angebracht werden und geht hin bis zum Einsatz von Crypto RFID-Chips für Anwendungen mit hohem bis höchsten Sicherheitsniveau.“

„Man wird hier schnell zu dem Ergebnis kommen das man immer risikobasiert vorgehen muss und eine `one size fits all` - Lösung eben nicht anwendbar ist. Hierbei muss stattdessen gefragt werden: Welches Schutzniveau brauche ich? Wie ist der Use Case, den ich absichern will? Dann kann ich darüber nachdenken, welche Technologie zum Einsatz kommen sollte.“

„Die Use Cases sind da zu unterschiedlich für eine Lösung und auch für einen Standard. Aber es wird da gewisse Cluster geben.“

„Die eine SDI gibt es nicht. Es muss differenziert werden.“

Zitate aus den Fragebögen /
Expertenkonsultationen

4.5 Insellösungen am Markt

Die derzeitige Marktsituation ist geprägt von Insellösungen - Keiner profitiert von niemandem.

Aufgrund spezifischer Bedarfe sind verschiedene Branchen, Initiativen, Entwicklungsbereiche und Unternehmen unterschiedlich weit beim Umgang mit Digitalen Identitäten und im Aufbau diesbezüglicher Infrastrukturen und Strukturen bzw. gestalten diese in unterschiedlicher Art und Weise. Es gibt teilweise sogar unternehmensintern für Teilbereiche bereits klare Strukturen und Lösungen, in anderen Bereichen wurde das Thema aber vollständig vernachlässigt.

Die Expertenaussagen haben gezeigt, dass wenig Austausch über Branchengrenzen hinweg zum Thema stattfindet. Dies äußerte sich nicht zuletzt in unterschiedlichen Definitionen und Verständnissen - zum Teil bewusst/beabsichtigt und zum Teil unbewusst/aufgrund mangelnden Wissens. Offenbar bestehen signifikante Knowledgegaps, u.a. → von Projekt zu Projekt, → von Branche zu Branche, → von Wissenschaft zu Anwendung, → wie auch von Normung zu Anwendung.

Dass hier kein größerer Austausch herrscht, liegt an einer mangelnden Vernetzung und Wissen um die Existenz weiterer Projekte, Informationen etc., denn im Gespräch mit den Experten zeigte sich stets großes Interesse an dem Vorgehen, Strukturen, Initiativen und Lösungen anderer (was oftmals auch zur Kontaktherstellung führte, vgl. bspw. Kap. 4.16.1). Die Bereitschaft zur Zusammenarbeit scheint also vorhanden zu sein. Dies mag auch daran liegen, dass die wesentlichen Akteure in Deutschland Identitätslösungen nicht als Geschäftsmodell betrachten, sondern vielmehr als Grundvoraussetzung für ihr Geschäftsfeld und dessen Digitalisierung, so postulierten Experten.

Des Weiteren wurde deutlich, dass Identitätslösungen oftmals individualisiert gestaltet bzw. individuell je Unternehmen oder Projekt entwickelt werden, „da nicht das passende Angebot am Markt vorhanden ist“. Dies resultiert u.a. aus den anderen Anforderungen an Identitätslösungen, wenn diese (erst nur) für den eigenen Verantwortungsbereich benötigt/gestaltet werden (vgl. hierzu Kapitel 3.1.3.1).

Es zeichnet sich zudem ab, dass die be- oder entstehenden Insellösungen aufgrund des mangelnden vorwettbewerblichen Austauschs redundant entwickelt werden und nicht die Gestaltungsqualität (Kosten, Usability, Sicherheit) erreichen, die sie bei Austausch oder Kooperation erreichen könnten.

„Die Erfahrung aus dem Verband zeigt, dass eigentlich in vielen Branchen die Herausforderungen die gleichen sind. Oftmals ist aber das Vokabular ein anderes. Jede Branche glaubt dabei, dass sie etwas Besonderes ist und keine andere Branche die gleichen Probleme hat. Das führt dazu, dass mehrere Branchen parallel fast die gleichen Probleme bearbeiten, anstatt zu gucken, wer da schon sehr weit ist, das Vokabular zu übersetzen und zu schauen, ob und wie man ggf. die vorhandenen Lösungen benutzen kann.“

„Wer immer das geschrieben hat, hat wirklich die Forschung der letzten 10 Jahre großzügig übersehen.“
[Experte zu einem Positionspapier zum Thema aus einer anderen Branche und dem aus seiner Sicht dort eklatanten Wissensmangel]

„Außer für die Nutzung von PKI-Karten sind uns bisher KEINE Produkte und Komponenten bekannt, die in ausreichender Qualität SDI mitbringen (Auch heute im Jahr 2017 nicht!). Daher setzen wir seit langem eigenentwickelte Lösungen ein. Unter anderem zum Schutz des geistigen Eigentums unseres Unternehmens.“

„Die Entwicklung und Weiterentwicklung von Identitäten vollzieht sich aktuell in vielen Anwendungsfeldern der Informatik parallel, teils jedoch in unterschiedlichen Geschwindigkeiten und unterschiedlichen Ausprägungen. Dabei sind die Vorgehensweisen recht unterschiedlich.“

„ID heißt Identifier, nicht Identität.“

„Eine virtuelle Identität ist für mich keine Identität.“

[letztere als Bsp. zur Terminologiediskrepanz]

Zitate aus den Fragebögen /
Expertenkonsultationen

4.6 Insellösungen auch in der Standardisierung

Die im Rahmen der Förderphase vollzogene Normenrecherche (vgl. Kapitel 2.3) zeigt, die Situation in der Standardisierungslandschaft spiegelt das aufgezeigte Bild der Insellösungen unmittelbar wieder. Es gibt zwar diverse aktuelle Normen- und Standardisierungsprojekte, die den Kontext „Sichere Digitale Identitäten“ aufgegriffen haben. Die verschiedenen Normungs- und Standardisierungsorganisationen haben jedoch Festlegungen im Zusammenhang mit der Regelung ihres Kerngeschäfts und meist bezogen auf einen konkreten Anwendungsfall getroffen. Darüber hinaus wurden bestehende Normen, die sich mit grundlegenden Konzepten von Identitäten beschäftigen, teilweise in den Expertenkonsultationen aufgrund abweichenden Verständnisses als nicht passend zurückgewiesen.

Es zeigen sich unterschiedliche Terminologie und Typologisierung, unterschiedliche Herangehensweisen, Sicherheitslevel (vgl. u.a. 3.1.4) etc. Das Resultat sind Insellösungen, die nicht kompatibel sind und eine erhebliche Fragmentierung des Themas in der Normung und Standardisierung nach sich ziehen, selbst innerhalb einer Branche.

„Die Standardisierung ist bisher noch nicht umfassend genug; einige neue Protokolle decken Security und/oder SDI nicht vollständig ab. Beispiel OPCUA; ... Grundvoraussetzung für eine allgemeine Sichere Identität, wäre aus unserer Sicht eine globale Standardisierung der Identifizierungsmerkmale von Entitäten. Eine regional begrenzte Standardisierung ist für uns ein Schritt in die richtige Richtung, aber NICHT ausreichend. - Für Smart City, Smart Home und vernetztes Fahrzeug gibt es bis heute keine Referenzmodelle. Dies gilt auch kritische Infrastrukturen, die unter das IT-Sicherheitsgesetz fallen, wie der Energieversorger in Großstädten etc.“

siehe auch Zitate in folgenden Kapiteln insbesondere 4.11 und 4.16

Zitate aus den Fragebögen /
Expertenkonsultationen

4.7 Dreh- und Angelpunkt digitaler Systeme, Produkte, etc.

Insellösungen? – dabei sind (S)DI Grundbausteine digitaler Systeme und Strukturen – Insellösungen führen unweigerlich zu Interoperabilitätsproblemen bei der Gestaltung neuer Systeme und Produkte.

Digitalen Identitäten und ihre Sicherheit sind Dreh- und Angelpunkt sowie Verbindungselement von unterschiedlichsten Systemen und Vorgängen. Die Auswirkungen von Interoperabilitätsproblemen durch Insellösungen werden mit voranschreitender Digitalisierung massiv zunehmen. Die Notwendigkeit von Interoperabilität und Kompatibilität von Identitätslösungen und ihren Bestandteilen besteht nicht erst bei der Interaktion zwischen Unternehmen und Branchen (Domänen), sondern betrifft bereits die Entwicklung und Gestaltung neuer bzw. eigener Systeme und diesbezüglicher Integration von Software, Geräten, Bauteilen, Programmen, Produkten etc. In diesem Sinne sind Auswirkungen von Interoperabilitätsproblemen bei Digitalen Identitäten potentiell überall möglich. Gibt es keinen Grundstandard, der unterschiedliche Anbieter und Zulieferer zusammenbringt, führt dies zu Problemen und ggf. zu Pfadabhängigkeiten bei der Gestaltung der eigenen Systeme. Insbesondere KMU haben hierbei (mangels Standardverfahren und Infrastruktur) Probleme eigene Lösungen umzusetzen oder sich in Netzwerke zu integrieren. Bei der Wahl der Identitätslösung oder Ausrichtung auf selbige ist die Verbreitung am Markt dann oftmals der maßgebliche Faktor und die Interoperabilität und diesbezügliche Investitionssicherheit obsiegt im Zweifel gegenüber der Sicherheit (insb. der des Identitätsgebers), vgl. Kap. 4.3 und 3.4.4.

„Herstellerspezifische Lösungen sind nicht zielführend.“

„Es ist sehr wichtig, dass SDI sich leicht in bestehende Systeme und Infrastrukturen, wie z.B. SAP, einbetten und nahtlos in die Abläufe integrieren lassen.“

„Da bei SDI entsprechende Unterstützung der gewählten Verfahren (Software und Hardware) sowohl beim Empfänger als auch beim Sender bzw. bei allen beteiligten Entitäten benötigt wird, ist besonders die Frage der Verbreitung am Markt ausschlaggebend für die Nutzbarkeit von SDI.“

„Die Problematik der Prüfung der SDI insbesondere bei Interoperabilitätsanforderungen in verteilten Systemen scheint mir ein in der Praxis schwierig umzusetzendes Problem zu sein, meist finden sich rein proprietäre Systeme.“

„Dabei sollte auch auf die Skalierbarkeit der gewählten Verfahren geachtet werden, da in den beschriebenen Szenarien SDI [...] von Kleinstunternehmen bis hin zu Konzernen ...] im Einsatz sind und entsprechend untereinander kompatibel sein müssen.“

Zitate aus den Fragebögen /
Expertenkonsultationen

4.8 Jedes Digitalisierungsprojekt braucht SDI

Insellösungen? - dabei muss sich jedes Digitalisierungsprojekt mit dem Thema SDI beschäftigen – von groß bis klein.

Die Situation der Insellösungen ist besonders unglücklich, da alle großen Zukunftsprojekte der Digitalisierung (Industrie 4.0, Smart Cities, Connected Cars, etc.) das Thema Digitale Identitäten und diesbezügliche Sicherheitslevel und entsprechende Lösungen angehen müssen (vgl. hierzu u.a. Kapitel 3.2.1). Auch hier zeigt sich der unterschiedliche Entwicklungsstand sowohl in der Umsetzung, der Struktur und der Standardisierung. Die Identitätslösungen werden derzeit - so lassen es die Expertenaussagen vermuten - ohne wirklichen grenzübergreifenden Blick behandelt. Sie sind zudem aus Sicht von Sicherheitsexperten oftmals nicht ausreichend bzw. werden als Bestandteil im System vernachlässigt.

→ Auch geförderte Zukunftsprojekte behandeln somit denselben Sachverhalt redundant. Was angesichts des Einsatzes von Fördergeldern kritisch zu betrachten ist.

Daraus resultiert, dass das Potential für Synergieeffekte, Innovationen und zur Steigerung der Interoperabilität ausgesprochen hoch ist. Vor diesem Hintergrund hat bspw. das FZI (Forschungszentrum Informatik) im 3. Quartal 2017 eine Abfrage an alle laufenden Projekte gestartet, wie das Thema Digitale Identitäten jeweils behandelt und gelöst wird.

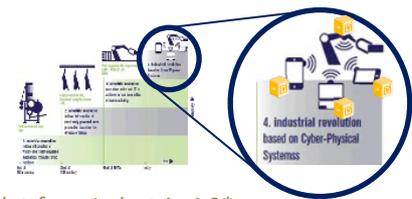
Über die großen Digitalisierungsprojekte hinaus betrifft das Thema aber jeden Bereich der Digitalisierung. Es sind sogar insbesondere die kleineren Digitalisierungsprojekte in jedem Unternehmen, in KMU oder in den Büros der Einzelunternehmer, die angewiesen sind auf standardisierte Identitätslösungen, die Sicherheit bieten. Gerade auch oder insbesondere die, die noch erst den Schritt in die Digitalisierung schaffen müssen (bspw. die konsequente Umsetzung der Idee des papierlosen Büros).

„In Forschungsprojekten - auch den ganzen Smart Data Projekten - spielt im Prinzip überall Identität eine große Rolle aber sie ist eben nicht der zentrale Inhalt des Projektes. Dort werden Plattformen gebaut, Systeme gebaut etc. Identitäten und Identifikation sind ein Thema, das lösen die so nebenbei, jeder für sich.“

Beispiele digitale Großprojekte:



*Nationale Plattform Elektromobilität**



*Plattform Industrie 4.0**

„Die aktuelle Herausforderung besteht im Transfer der Konzepte in die neuen Domänen, für die IT-Sicherheit ein junges Themenfeld darstellt.“

„Der Kern jeder Interaktion und Kommunikation ist Vertrauen in die richtige digitale Identität, unabhängig ob von Menschen, Maschinen, Dingen oder Prozessen. Erst wenn diese Voraussetzung erfüllt ist können neue oder bestehende Abläufe verbessert oder neue Innovationen entstehen.“

„Wer heute in Unternehmen Digitalisierung vorantreibt und Innovationen im digitalen Zeitalter voranbringen will, der kann nicht ohne SDI.“

„Egal welchen Bereich der IT man betrachtet, sind immer Identitäten wichtig.“

**(Grafiknutzung für diesen Bericht mit freundlicher Genehmigung der Plattformen)*

*Zitate aus den Fragebögen /
Expertenkonsultationen*

4.9 Die Domänen wachsen zusammen

Insellösungen? – dabei müssen Identitätslösungen / SDI zunehmend domänenübergreifend funktionieren. Die Digitalisierung lässt die Domänen zusammenwachsen.

Wesentliches Merkmal der Digitalisierung ist, dass unterschiedlichste Domänen interagieren können und Produkte und Dienstleistungen unmittelbar zusammenwachsen. Neue Geschäftsmodelle und Produktivitätsgewinne basieren auf dieser Interaktion. Sind die Schnittstellen für die Identifikationslösungen und die dem Anwendungsfall entsprechend sichere Gestaltung nicht gegeben, vermag dies die Zusammenarbeit erschweren oder sogar verhindern. Fatal wäre, wie es in den Expertenkonsultationen u.a. postuliert wurde, wenn einzelne Domänen hohe Investitionen in die Gestaltung und Implementierung ihrer Identitätslösungen tätigen und eine spätere Interaktion nur unter erneut hohen Kosten stattfinden kann.

Darüber hinaus „durchfließen“ die Produkte der Domänen / Branchen ja teilweise die der anderen bzw. kommen dort zum Einsatz. Auch hierbei werden domänenübergreifende Anforderungen relevant.

„Eine domänenübergreifende Lösung: Heutzutage wachsen die Anwendungsdomänen zunehmend zusammen. Seien es Produktion und Logistik, Logistik und Car2Car, Car2Car und EMobility, EMobility und SmartEnergy, SmartEnergy und Produktion, der Zirkel lässt sich auch noch weiter fassen. All diese Domänen haben ähnliche Probleme und sollen in absehbarer Zeit auch interoperabel sein. Ähnlich wie alle Domänen hin zu ARM, Posix, Ethernet konvergieren, sollte man diese Entwicklung bereits in der Ausgestaltung von SDI vorweg nehmen.“

„Der Automobilssektor macht dies vielfach schon, der Energiesektor jetzt auch. Bei eMobility sieht man hier dann die Überschneidung. Daher ist andererseits eine Interoperabilität zwischen Industriedomänen sehr wichtig. Es bedarf einer gemeinsamen Basis an Technologien und interoperablen Infrastrukturen, aber gezielten Ausprägungen pro Domäne.“

„Die Interaktion über Domänen-Grenzen hinweg bei einer gleichzeitig hohen Qualität der SDI ist der Schlüssel zur Digitalisierung.“

„Es ergibt sich ebenfalls eine Relevanz [von SDI] für Infrastrukturen wie das digitale Stromnetz (Digital Grid), hier insbesondere für den domänenübergreifenden Datenaustausch ...“

„Die Vernetzung von Komponenten, Maschinen und Anlagen nimmt sowohl im industriellen als auch im privaten Bereich immer mehr zu. Dabei entstehen auch Überschneidungen zwischen diesen Bereichen, denn bspw. kann ein Smartphone, das sowohl für den Maschinenzugriff genutzt wird, auch zum privaten Surfen im Internet oder Telefonieren benutzt werden.“

siehe auch Zitate von Kapitel 4.17

Zitate aus den Fragebögen /
Expertenkonsultationen

4.10 Es geht nur international

Insellösungen? – müssen Identitätslösungen / SDI international funktionieren.

Die digitale Welt macht keinen Halt an den nationalen oder kontinentalen Grenzen. Zukunftsprojekte (wie die Industrie 4.0) und sämtliches digitales Handeln, haben zum Teil vielmehr explizit das Ziel, Grenzen zu überwinden. So ist die Internationalisierung auch im besonderen Interesse der exportorientierten und in grenzübergreifenden Wertschöpfungsketten und Netzwerken agierenden deutschen Wirtschaft.

Dass verlangt wird, dass Identitätslösungen international funktionieren und vereinheitlicht werden, hat zudem den Hintergrund, dass die deutsche und europäische Wirtschaft und Gesellschaft im digitalen Bereich der technischen Komponenten, Devices, Programme etc. auf den internationalen Markt angewiesen ist. Die Grundlagen für die Identitätslösungen werden also im Ausland geschaffen. Ein nationales oder europäisches Vorgehen muss international Wirkung erlangen, um überhaupt sinnvoll zu sein.

Es verwundert daher nicht, dass neben den Aussagen zur generellen Relevanz von SDI und der Aussage, dass es keine One-Fits-All-Lösung geben wird, die Aussage, dass ein strategisches Herangehen an das Thema SDI nur sinnvoll ist, wenn es schlussendlich international zu wirken vermag, die wohl am vehementesten vertretene Forderung in den Expertenkonsultationen war.

„DI's müssen technisch, rechtlich und konsistent global einsetz- und validierbar sein.“

„Hinsichtlich einer möglichen strategischen Herangehensweisen an das Thema SDI ist essentiell: 1. die Interoperabilität und Kompatibilität und 2. die Internationalisierung“

„Letztlich muss jede Entwicklung um SDI herum bezahlbar für KMUs sein. Ein VDMA-Mitglied hat im Schnitt 250 MA und keinen CISO. Der Fokus liegt nicht auf internationaler Normung und Standardisierung sondern auf sich selbst und die Lokalregierung. Dennoch werden die Produkte weltweit verkauft. Gerade diese internationale Ausrichtung bedingt die Notwendigkeit einer weltweiten Harmonisierung von Lösungen bevor diese eingebaut werden können. Dies betrifft die Bereiche Recht, Technik und Nachhaltigkeit.“

„Eine Harmonisierung und Standardisierung muss ein internationales Unterfangen sein. Eine allein deutsche Lösung hilft nicht. Eine deutschlandweite Harmonisierung der Hersteller für ID-Semantik wäre aber ein erster Schritt.“

„Der Fokus zur Harmonisierung muss Europäisch oder International sein.“

„Wie soll das denn bitte aussehen, wenn wir bspw. einen Standard machen, der toll ist und die amerikanischen Hersteller und Chinesen sagen, dass ist uns grad mal egal, wir machen/haben da was eigenes.“

„Natürlich muss das Thema international umgesetzt werden. Das verlangt bzw. ist immer eine Frage des Engagements und des Wollens.“

[vgl. auch Kap.4.18]

Zitate aus den Fragebögen /
Expertenkonsultationen

4.11 Ein gemeinsames Ziel (Referenzarchitektur / Framework)

Die Expertengespräche ergaben, es braucht die Vision / das Ziel eines domänenübergreifenden internationalen Frameworks für (Sichere) Digitale Identitäten, also eine Referenzarchitektur, die vom Ansatz her allen Aktivitäten, Entwicklungen und Standardisierungsbestrebungen eine gemeinsame Grundlage und Richtung gibt.

Die eine technische Lösung gibt es zwar nicht, aber es kann einen Lösungsrahmen geben. Eine Referenzarchitektur, die die bestehenden und entstehenden Identitätslösungen zusammenbringt und auf eine Harmonisierung hinarbeiten lässt. Ein Rahmenwerk, was den Entwicklungen und den Bestrebungen im Hinblick auf Interoperabilität und Einsatzmöglichkeit eine gewisse (Zukunfts-) Sicherheit und somit Investitionssicherheit bieten kann. Nur so lässt sich ein Prozess einleiten, der der Bildung von Insellösungen, der Gefahr von Interoperabilitätsproblemen und dem sich Durchsetzen von Lösungen, die nicht im Einklang mit gesellschaftlichen und wirtschaftlichen Interessen sind, entgegensteht.

Etwa 80% der Experten, die die Fragebögen beantworteten, haben unmittelbare Forderung nach weiterer Standardisierung, Normen, einem Framework und/oder Referenzmodellen gestellt. Zum derzeitigen Zeitpunkt fehlt eine strukturierte nachhaltige Herangehensweise. Es fehlt das verbindende Element. Solch ein verbindendes Element könnte ein domänenübergreifendes, ganzheitliches aber Identitätslösungen in den Handlungsebenen betrachtendes Referenzmodell sein, welches Deutschland als Vorreiter positionieren könnte:

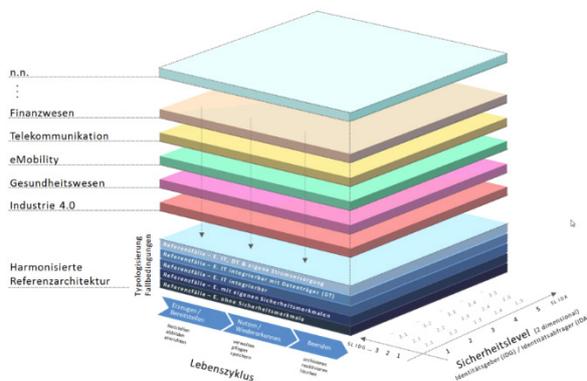
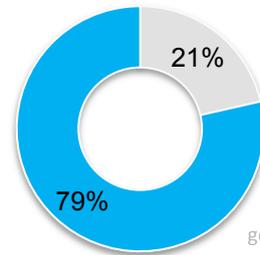


Abbildung 36 – domänenübergreifende Referenzarchitektur SDI (Beispiel) – Details vgl. Kapitel 5



% der im Sinne des Kap. 2.0 gewerteten Aussagen

- keine unmittelbare Aussage
- Forderung nach Standards, Referenzmodellen, Normen

„Es ist auf jeden Fall interessant, am Ende zu einer Infrastruktur zu kommen oder zu einem Rahmenwerk, aus dem ich Handlungsempfehlungen ableiten kann, technisch oder auch organisatorisch.“

„Bisher fehlt jedoch [...] ein übergreifendes, fundiertes Konzept dafür. Um ein solch umfassendes Konzept zu entwickeln, ist es erforderlich, ein Verständnis für die möglichen Entwicklungen und Bedürfnisse im Bereich des Identitätsmanagements in den nächsten 10-15 Jahren zu erlangen.“

„Dabei muss einerseits konzeptionelle Arbeit über die Grenzen von Anwendungsdomänen hinweg gelingen, andererseits eine Adaption von Umsetzungen anhand der spezifischen Anforderungen der jeweiligen Anwendung.“

„Eine Instanz, die die Domänen zusammenbringt und auf Basis der neusten und besten internationalen Technologie gemeinsame Vorgehensweisen entwickelt, würde der Entwicklung von SDI am besten zutragen.“

„Weiterhin müssen auch domänenübergreifende Standards festgelegt werden, da die Systeme der unterschiedlichen Domänen immer mehr verschmelzen.“

„Die Standardisierung ist bisher noch nicht umfassend genug.“

Zitate aus den Fragebögen / Expertenkonsultationen

4.12 Fokus Anwendungsfall (Sicherheitslevel, u.a.)

Zum Inhalt der Referenzarchitektur: Ein zentraler Fokus eines SDI-Frameworks sollte dem Anwendungsfall und dem diesbezüglichen Anforderungsprofil (u.a. Sicherheitsleveln) gelten – das Anforderungsprofil lässt Rückschlüsse auf konkrete Lösungen zu.

Aus den Expertenkonsultationen und der logischen Sachverhaltsanalyse in Kapitel 3 (insb. 3.1.4) lässt sich schließen, dass ein domänenübergreifenden SDI-Framework nicht die SDI-Lösung in den Mittelpunkt der Betrachtung stellt, sondern den Anwendungsfall und das diesbezügliche Anforderungsprofil. Selbiges determiniert schlussendlich die Identitätslösung und somit die technische Lösung. → Es geht also nicht um die universelle Sichere Digitale Identität, sondern um die im jeweiligen Anwendungsfall sichere Identität.

Wesentliche Faktoren sind hierbei:

- (a) Schnelligkeit / Usability
...die beim Anwendungsfall benötigt wird
- (b) Sicherheit / Risiko
...das mit dem Anwendungsfall zusammenhängt
- (c) Kosten / Aufwand
...die mit dem Einsatz der Lösung verbunden sind

Zentrales Element des SDI-Frameworks sind dann die Vereinheitlichung von übergeordneten Sicherheitsleveln und die Beschreibung von Anforderungsprofilen für Kategorien von Anwendungsfällen und dies bezogenen Lösungen. Hierdurch kann determiniert werden, wo, wann, welcher Typ an technischen und/oder organisatorischen Lösungen zum Einsatz kommen sollte.

Identifikations- / Verifikationslösungen können dabei auch an ein und derselben Schnittstelle variabel eingesetzt werden und bei einem veränderten Anwendungsfall und veränderten Anforderungen (zusätzlich) zum Einsatz kommen.

[Wir brauchen...] „Use Case basierend angelegt ein Standardprozessframework“

„Das Sicherheitsniveau wird bestimmt durch Use Case und Business Cases, wobei der Kostenfaktor eine entscheidende Rolle spielt.“

[Wir brauchen...] „Auswahl und Spezifizierung der jeweils für den Anwendungsfall benötigten ID-Typen.“

„Teilweise muss in bestimmten Bereichen den anwendungsspezifischen Anforderungen Rechnung getragen werden ; im Car-2-Car-Kontext müssen Identitätszertifikate und Authentifizierungen besonders klein ausfallen, da potentiell sehr viele Autos gleichzeitig ihre aktuelle Position und Fahr-richtung allen anderen Fahrzeugen mitteilen müssen – hier werden oft Werte von 10 authentifizierten Meldungen pro Sekunde pro Auto genannt.“

„...die Lösung [ist] immer für eine spezielle Klasse von Use Cases erforderlich“

„Eine weitergehende Festlegung von Anforderungen in einer entsprechenden Policy ist vom Anwendungskontext abhängig. Auswahl und Spezifizierung der jeweils für die Anwendungsfälle benötigten ID-Typen“

„Die Faktoren Schnelligkeit/Usability, Sicherheit/Risiko, Kosten/Aufwand sind sehr treffend, zudem mag es je nach Use Case untergeordnete oder Zwischenziele geben.“

vgl. auch Zitate Kapitel 4.4

*Zitate aus den Fragebögen /
Expertenkonsultationen*

4.13 Fokus Lebenszyklus (Bestandteile von Identitätslösungen)

Zum Inhalt der Referenzarchitektur: Ein anderer zentraler Fokus sollte der sowohl ganzheitlichen wie in seine Bestandteile zerlegenden Betrachtung von Identitätslösungen auf Sicherheit und Kompatibilität/Interoperabilität (angelehnt am Lebenszyklus) gelten.

Identitätslösungen bestehen weder nur aus einem technischen Element, welches die Verbindung zwischen Entität und digitalen Datensatz gewährleistet, noch sind sie als Komplettlösung über den gesamten Lebenszyklus zu sehen. Die einzelnen Bestandteile determinieren einander, können aber auch unterschiedlich kombiniert werden. Wie das Kapitel 3 (insb. 3.1.2 und 3.2) darlegt, gehören sämtliche Handlungsebenen im Lebenszyklus zum Thema und nur eine konsistente Gestaltung (gleiche Sicherheitslevel) über den gesamten Prozess ermöglicht Sichere Digitale Identitäten.

Dies bedeutet, dass zum einen eine Harmonisierung im Hinblick auf die Gesamtstruktur und die Erwartungen oder Anforderungen an selbige (ihrem prinzipiellen Aufbau mit dem Ineinandergreifen von technologischen, Hardware- wie Software-Anteilen bis hin zu organisatorischen Elementen) Teil des Frameworks ist. Und bedeutet zum anderen, dass innerhalb des Frameworks selbst die Ausgestaltung der einzelnen Handlungsebenen möglichst kompatibel gestaltet werden muss. Denn dann können die Elemente kombiniert und interoperabel eingesetzt werden und schaffen so neue oder ineinandergreifende Identitätslösungen. Explizit wurde dahingehend in den Expertenconsultationen die Software-Hardware-Schnittstelle mehrfach als notwendig anzugehendes Standardisierungsprojekt adressiert.

Im Kapitel 3 wurde dahingehend ein erster Versuch der Darstellung des Gesamt-sachverhaltes und der relevanten Handlungsfelder bei Identitätslösungen in Anlehnung an den Lebenszyklus einer Digitalen Identität entworfen.

„Angesicht der Sicherheitsbedrohungen muss man mit der Situation in Bezug auf SDI sehr unzufrieden sein. Besonders hoch ist der Handlungsbedarf bei der Gewährleistung eines Sicherheitsniveaus über den gesamten Lebenszyklus.“

„Um Sicherheit und damit auch eine Sichere Identität über den kompletten Lebenszyklus zu bieten, müssen alle Teile geschützt und sicher sein, denn „die Kette ist nur so stark wie ihr schwächstes Glied“.“

„Wie kann der Nutzer sichergehen, dass es eine SDI ist und an den Lebenszyklus gedacht wurde?“

„Der Lebenszyklus einer sicheren Identität muss sich mit dem Erzeugen/Bereitstellen (Feststellen, Abbilden, Einrichten der Identität), der Nutzung (Wiedererkennen), der Verwaltung (Pflege/Speichern) und dem Archivieren/Vernichten (Archivieren, Reaktivieren, Löschen) siehe dazu auch ISO29115, beschäftigen.“

Zitate aus den Fragebögen / Expertenconsultationen

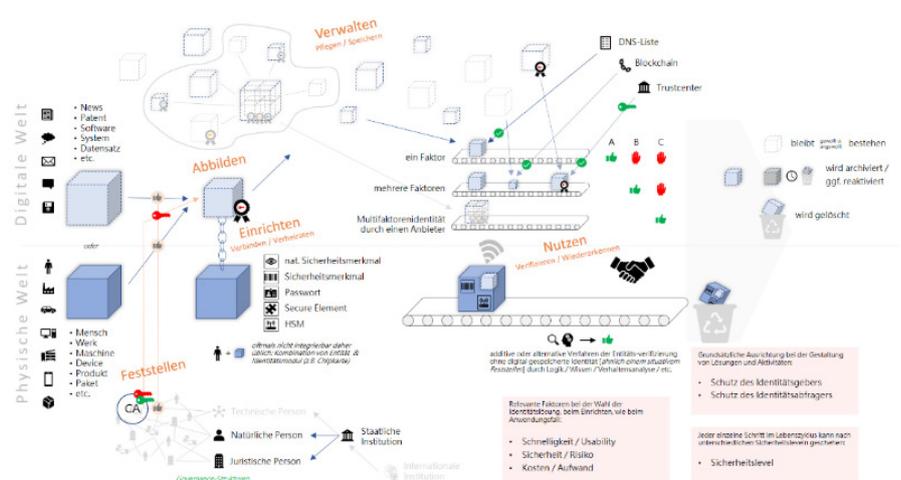


Abbildung 37 – Schaubild Gesamtsachverhalt SDI (s. Anhang 6.1)

4.14 Anforderungsprofile nach Einsatz- und Verantwortungsbereich

Zum Inhalt der Referenzarchitektur: Bei der Gestaltung der Referenzarchitektur sind Einsatz- und Verantwortungsbereich der SDI oftmals maßgebend für das Anforderungsprofil.

Im Sinne des aus den Expertenkonsultationen herausgearbeiteten Kapitels 3.1.3 zeigen sich unterschiedliche grundsätzliche Herangehensweisen und somit Anforderungsprofile an Identitätslösungen je nach Einsatz- und Verantwortungsbereich. Diese gelten für

- die Gestaltung von Identitätslösungen für den „eigenen“ Verantwortungsbereich (bspw. in einzelnen Unternehmen)
- die Anforderungen an die Gestaltung und die Ansatzpunkte für Identitätslösungen in Produkten, die in anderen Verantwortungsbereichen integriert/eingesetzt werden
- die Gestaltung der Interaktion zwischen verschiedenen Verantwortungsbereichen (sowohl Systemen, wie Unternehmen)

Diese Dimensionen gilt es bei der Entwicklung und Gestaltung der unterschiedlichen Bereiche des Frameworks und hiervon abzuleitender Spezifikationen Standards zu berücksichtigen, da aus ihnen unterschiedliche Erwartungen und Implikationen heraus entstehen und zum Teil auch sehr unterschiedliche Sachverhalte zu lösen sind. In diesem Sinne waren die Sichtweisen bei den Interviews oftmals bereits strukturgebend.

„Aus unserer Sicht sollte man Trennen zwischen Anforderungen an DI für internen Prozesse (wie z.B. für Produktion, Verwaltung, Vertrieb, etc) und DI für solche Prozesse, wie sie sich zwischen Kunden und den Produkten abspielen.“

„Generell besteht noch Bedarf an einer allgemeinverständlichen Definition von SDI und den dafür relevanten "Vertrauensräumen".“

„Wie schaffen wir es denn, dass wir auf einmal eine security policy vertrauen die von einem anderen Unternehmen kommt, wie kann man da eine Interoperabilität herstellen?“

„Bei hinzugekaufter Software muss diese den Lebenszyklus unterstützen...“

„Durch die Interaktion mit Entitys außerhalb des eigenen Kontrollbereichs sind zahlreiche neuartige Informationsverbindungen erforderlich.“

„Zukünftig werden jedoch zugekaufte Komponenten bedeutender, da die Vernetzung der neuen Anlagen-generation neue/andere Komponenten erfordert, die nicht selbst hergestellt werden können (z. B. Router, ...).“

Zitate aus den Fragebögen /
Expertenkonsultationen

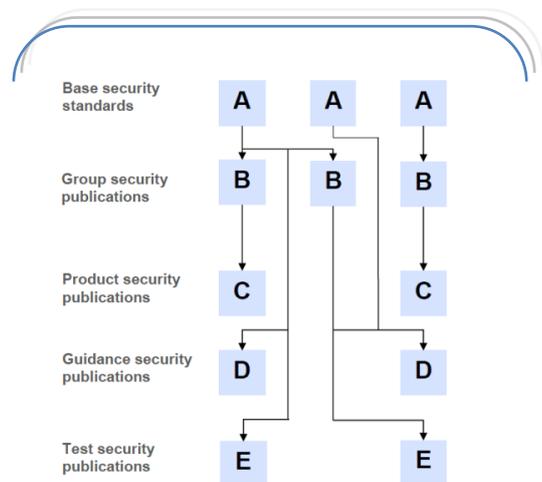
4.15 Anwendbarkeit der Referenzarchitektur

Zum Inhalt der Referenzarchitektur: Das SDI-Framework muss das Ziel haben, anwendbar zu sein und angewendet zu werden.

Die befragten Experten adressierten mehrfach, dass es anwendbare Standards und Referenzmodelle geben müsse – insbesondere auch mit Blick auf die Einbindung von KMU.

Die Referenzarchitektur sollte daher sukzessive das gesamte Spektrum an Spezifikationen adressieren. Also von Basisstandards (A) mit grundlegenden Konzepten über domänenspezifische (B), produktspezifische (C) und Guidelines zur Umsetzung (D) (vgl. Kapitel 2.3 und Kapitel 5.1.2). Insbesondere die letzteren steigern die unmittelbare Anwendbarkeit, leiten sich aber auch aus ersteren ab. Auch die Kategorie E, die die Prüfung von Anforderungen aus A-D definiert, wird Relevanz haben. Sie wurde von einzelnen Experten auch konkret als für das Thema unbedingt notwendige Ebene adressiert.

Ein weiteres Hinwirken auf die Anwendung und die Anwendbarkeit adressiert auch das Kapitel 4.20 „Auswirkungen – über die digitale Welt hinaus“. DI werden überall gebraucht und in vielen Standards und Normen, die nicht unmittelbar der IT zugehören, werden die Grundlagen für die Erstellung und Nutzung von DI geschaffen. Hierfür ist es unmittelbar notwendig bei DIN, die Ergebnisse in die anderen Normungsgremien hineinzutragen und auch hier auf Anwendung und Anwendbarkeit der Referenzarchitektur und ihrer Implikationen hinzuwirken.



Typen von Spezifikationen - vgl. Kapitel 2.3 und Kapitel 5.1.2

„Eine Struktur zu Digitalen Identitäten und Sicheren digitale Identitäten in einer gewissen Abstufung, die u.a. bspw. über die Verbände den Mitgliedsunternehmen empfohlen wird, kann ein Hebel für eine grundlegend sichere Gestaltung der Digitalisierung sein.“

„Um einen Anwender die Anwendung von SDI für die Vielzahl an Herstellern sinnvoll nutzbar zu machen, sind weitere Standardisierungsprojekte in diesem Bereich notwendig.“

„National sollte es vor allem Vereinigungen geben, die Anwendungsempfehlungen und Umsetzungshinweise geben; Nutzergruppen für den Austausch.“

„Referenzmodelle fehlen“

„Der fehlende Aspekt sind AnwenderForen, in denen die Umsetzung von SDI für einzelne Branchen basierend auf der Standard-Technologie dargestellt und unterstützt wird.“

„Es ist auf jeden Fall interessant, am Ende zu einer Infrastruktur zu kommen oder zu einem Rahmenwerk, aus dem ich Handlungsempfehlungen ableiten kann, technisch oder auch organisatorisch.“

„Der Framework muss auch dafür geeignet sein Verifizierbarkeit und Überprüfbarkeit von Sicherheitslösungen zu schaffen!“

Zitate aus den Fragebögen /
Expertenkonsultationen

4.16 Es wird nicht bei Null angefangen (Grundlagen / Ergebnisse)

Zum Inhalt der Referenzarchitektur: Es wird nicht bei Null angefangen! – Unterschiedlichste Techniken, Modelle und Infrastrukturen, Normen und Standards, Gesetze etc. sind vorhanden – Das Richtige zu orchestrieren und auf dessen Etablierung hinzuarbeiten muss nun im Fokus stehen.

Das Thema „Sichere Digitale Identitäten “ ist eines der aktuell wichtigsten Grundlagenthemen der Digitalisierung. Auch daher ist es kein neues Thema, denn Digitale Identitäten waren schon immer notwendig für die digitale Welt.

Neben den unzähligen (auch wenn oftmals spezifischen Insel-) Lösungen und Teillösungen, Infrastrukturen und Standards, die sich am Markt entwickelt haben, wurden insb. durch das IT-Sicherheitsgesetz (KRITIS), die eIDAS Verordnung sowie die Datenschutzgrundverordnung neue gesetzliche Rahmenlinien geschaffen. Auch in der Hightechstrategie, die sie sich ab dem Jahr 2010 insbesondere auf den gesellschaftlichen Bedarf an zukunftsfähigen Lösungen und deren Realisierung fokussierte, wurde das Thema Sichere Identitäten als zentral adressiert und durch Forschung Grundlagen geschaffen.

Einen Überblick über vorhandenen Grundlagen bieten die Kapitel 2.3 Recherche Normung (sowohl von Kategorie A-D bereits in Teilen vorhanden), Kapitel 2.4 Recherche Recht, die allgemeine Recherche und die Sachverhaltsanalyse in Kapitel 3, welche gleichzeitig die Strukturierung der Handlungsfelder vornimmt. Die Expertenkonsultation war Grundlage dieser zusammengetragenen Informationen.

Auf diesen Bausteinen kann und muss die Gestaltung und der Prozess hin zu einem SDI-Framework aufbauen. Der Fokus muss nun von der Forschung darauf gerichtet werden, die sich schrittweise manifestierenden Grundstrukturen der Digitalisierung mit zu gestalten bzw. aus den existenten technischen und organisatorische Lösungen und Herangehensweisen und Spezifikationen, diejenigen in einem Gesamtgebilde als Standard zu etablieren, die im Sinne des Gesamtinteresses von Wirtschaft und Gesellschaft liegen. Die Grundstrukturen der bisherigen Welt sind über Jahrtausende gewachsen. Die der digitalen Welt haben nicht weniger Impact auf die Menschen und Organisationen, entwickeln sich aber gerade innerhalb einiger Jahre und verfestigen sich schon morgen.

„Es mangelt weniger an Lösungen, sondern eher an einer Strukturierung und Anwendung.“

„Es gibt bereits Standards für die Herausforderungen rund um SDIs. Als nächster Schritt müssen die Standardisierungsgremien domänenübergreifend zusammenarbeiten und übergreifende Standards festlegen.“

„Im Prinzip liegen wesentliche Elemente auf dem Tisch, man muss sie nun aber mal sinnvoll zusammenfügen.“

Zitate aus den Fragebögen /
Expertenkonsultationen

4.16.1 Teil-Ergebnisse der Konzeptionsphase

Im Rahmen der Konzeptionsphase wurden durch den Analyseprozess und die Expertenkonsultation auch neue Ansatzpunkte und Grundlaiden geschaffen, die es ermöglichen, eine konzertierte Herangehensweise einzuleiten. Hierzu zählen u.a.:

- Überblick und Strukturierung zum Sachverhalt und Situation und derzeitigen Aktivitäten, Lösungen, Stakeholdern
 - siehe Kapitel 2 und 3
- Sensibilisierung zentraler Entscheider hinsichtlich des Themas
 - Kommunikation über Websites, Vorstellungen, Vorträge, Fragebögen, etc.
 - Kontakt zu über 300 Entscheidern
- Generierung von Bereitschaft zur Mitarbeit durch Key-Stake-Holder
 - siehe Kapitel 2
- Einleitung von Knowhowtransfer sowie Vernetzung nationaler Player, bspw:
 - Vernetzung *BMW, IUNO, BSI, Bundesdruckerei, Fraunhofer SIT / IDS, Plattform Industrie 4.0, Siemens, FU Berlin, Infineon*
 - Vernetzung Bundesdruckerei mit DIPP / Verimi
 - Vernetzung ISÆN Projekt über CEN Workshop Agreement - Anfrage durch AFNOR zur Zusammenarbeit beim Thema SDI
 - Gewinnung des Bitkom CPS Workshop für das Thema SDI

4.17 Ein domänenübergreifendes Netzwerk als Alleinstellungsmerkmal

Zur Herangehensweise an die Entwicklung einer Referenzarchitektur:
Ein domänenübergreifendes Netzwerk auf Basis bestehender Gremien ist die logische Konsequenz für die Entwicklung einer Referenzarchitektur und wäre ein internationales Alleinstellungsmerkmal beim Thema SDI.

Wie beschrieben, ist es eines der wesentlichen Merkmale der Digitalisierung, dass unterschiedliche Domänen ineinander wachsen - durch neue Schnittstellen und darauf aufbauende neuartige Geschäftsmodelle. Um die diesbezügliche Innovationskraft zu ermöglichen oder zu steigern, ist auf die Sicherheit und Interoperabilität der Digitalen Identitäten über die Domänengrenzen hinweg hinzuarbeiten, so die Experten.

Hierbei ist, wenn möglich, auf bestehende/etablierte themennahe Gremien zurückzugreifen, nicht nur weil diese bereits existieren, sondern weil sie zum einen ihre Domäne gut repräsentieren, vernetzen und das KnowHow ihrer Branche abbilden und weil das Gründen eines themenindividuellen Gremiums bei einem Thema, welches „nur“ als Supporttechnologie für das eigene Geschäftsfeld gesehen wird, schwierig wäre. Hierzu könnten ggf. auch Subgremien eingesetzt werden, wie es bspw. die AG3 der Plattform Industrie 4.0 beabsichtigt. Der wesentliche Nutzen wäre der Austausch und Wissenstransfer über die Domänengrenzen hinweg, das Darstellen der eigenen Initiativen zum Thema, das Starten möglicher kooperativer Projekte, sowie das Überprüfen bestehender oder entstehender Standards, Projekte etc. auf die Anwendbarkeit in der eigenen Branche / Domäne oder Sinnhaftigkeit aus Sicht der eigenen Branche usw.

Synergiepotentiale und Innovationspotentiale könnten besser ausgeschöpft werden, der Digitalisierung ggü. noch zögerliche Domänen angeregt werden und insbesondere Interessen im Themenfeld höheres Gewicht auch auf internationaler Ebene verliehen werden. Ein solches Aktionsnetzwerk, welches die Fähigkeit hat Identitätslösungen und diesbezügliche Standardisierungen unmittelbar domänenübergreifend zu bewerten, wäre laut der Expertenkonsultation weltweit einmalig.

„Eine Instanz, die die Domänen zusammenbringt und auf Basis der neusten und besten internationalen Technologie gemeinsame Vorgehensweisen entwickelt, würde der Entwicklung von SDI am besten zutragen.“

[Es braucht einen...] „Vorschlag von branchenübergreifenden Verbänden an die Politik“

„Es würde uns helfen, wenn eine nicht kommerzielle, nicht gewinnorientierte und nicht staatlich koordinierte Stelle existiert, die diese Fragen umfänglich klärt und weltweite die Verwendung koordiniert.“

„Die aktuelle Herausforderung besteht im Transfer der Konzepte in die neuen Domänen, für dich IT-Sicherheit ein junges Themenfeld darstellt.“

siehe auch Zitate von Kapitel 4.9

Zitate aus den Fragebögen /
Expertenkonsultationen

4.18 Die Antwort auf Internationalisierung: Normung

Zur Herangehensweise an die Entwicklung einer Referenzarchitektur:
Zur Internationalisierung des SDI-Framework mit seiner Referenzarchitektur muss dessen Gestaltung auf die internationale Normung ausgerichtet sein.

Sozusagen eine Vorgabe der Experten war, dass jegliche Bestrebungen hinsichtlich der Gestaltung des Themas international ausgerichtet sein sollten. Einzelne Experten erwähnten, dass ein europäischer Ansatz das Minimum wäre, aber an einer Internationalisierung an sich doch nichts vorbeiführe.

Natürlich besteht die Möglichkeit für bestimmte Bereiche national oder europäisch gesetzgeberisch aktiv zu werden. Dies sollte auch nicht ausgeschlossen werden, so wie der Gesetzgeber bspw. beim IT-Sicherheitsgesetz zum Thema KRITIS und der eIDAS-Verordnung gestalterisch tätig wurde. Zudem sind u.U. wie bei Ausweisen Governance-Strukturen aufzubauen oder mit anderen Ländern bzw. international Abkommen zu erwirken, die eine vertrauenswürdige Basis-Infrastruktur hinsichtlich SDI gewährleisten. Hierfür müssen im Prozess der ganzheitlichen domänenübergreifenden und ggf. dann auch internationalen Betrachtung / Auseinandersetzung Antworten gefunden werden. Die notwendige detaillierte Gestaltung ist gesetzgeberisch aber nicht möglich und gesetzliches Einschreiten wäre nicht zuletzt auch immer unter Gesichtspunkten der möglichen Einschränkung der Innovations- und Wettbewerbsfähigkeit zu betrachten.

Auch dem Bundesamt für Sicherheit in der Informationstechnik wird bei höchsten Sicherheitsleveln eine wichtige Rolle in der Gestaltung von Teilen des Gesamtansatzes eines SDI-Frameworks zukommen. Das umfassende Expertenwissen im Bereich IT-Security und später das Wissen um mögliche Bedrohungslagen etc., wird Grundlage für konzeptionelle Ansätze sein. Technische Richtlinien des BSI sollten ggf. auch in die Normung einfließen.

Das Thema SDI strategisch anzugehen und die Aufgabe wahrzunehmen, an der Grundlagengestaltung der Digitalisierung mitzuarbeiten, bedeutet die Prozesse und Ergebnisse in die internationale Normung zu bringen bzw. stets mit der internationalen Normung zu verbinden. Dies ist inzwischen mit der Globalisierung auch der vorherrschende

[vgl. auch Kap. 4.10]

„Natürlich ist der Anspruch dabei, wenn wir in Deutschland sowas erstellen würden, dass das natürlich in einen internationalen Standard mündet wo wir eine Liste von Anforderungen haben, wo dann jedes Unternehmen sagen kann: ich erfülle genau diese Anforderungen“

„...Domänen-übergreifenden und internationalen Standards, so dass sich Synergien bilden können, und sich die Investition in Technologien für Zulieferer lohnt und die Preise für SDI-Hardware und -Infrastruktur sinken.“

„Eine Standardisierung in diesem Bereich muss international erfolgen.“

„Grundvoraussetzung für eine allgemeine Sichere Identität, wäre aus unserer Sicht eine globale Standardisierung der Identifizierungsmerkmale von Entitäten. Eine regional begrenzte Standardisierung ist für uns ein Schritt in die richtige Richtung, aber NICHT ausreichend.“

„Gleichzeit ist es notwendig die entsprechenden Standards, Anforderungen und Rahmenbedingungen auf internationaler Ebene, zumindest auf Europäischer zu etablieren, um unterschiedliche Lösungen zu verhindern, die die Entwicklung von SDI nachhaltig bremsen können.“

„Heutige Zertifizierungs-Schemen wie z.B. Common Criteria sind viel zu langwierig um mit dem immer schnelleren Lebenszyklus moderner IT schritthalten zu können. Wenn ein Zertifizierungsverfahren 1-1.5 Jahre dauert, ist die betreffende Software bereits veraltet, wenn das Verfahren abgeschlossen ist.“

„Eine Verpflichtung zum Einsatz von HW-basierter Sicherheit „überall“ wird jedoch als „knock-out“ gesehen.“

Zitate aus den Fragebögen /
Expertenkonsultationen

Ansatz in den meisten Normungsbereichen. So sind heute über 80% der Normungsaktivitäten bei DIN international. Bei der Vernetzung der Projekte, Aktivitäten und der domänenübergreifenden gemeinschaftlichen Analyse des Sachverhalts in Deutschland sollte stets die Sicht auf mögliche Normungsaktivitäten im Auge behalten werden. Denn (abgesehen von einer aufgrund marktbeherrschender Stellung akzeptierte Lösung) haben die entwickelten Strukturen nur die Möglichkeit tatsächlich nachhaltig die digitale Welt zu gestalten, wenn sie in der internationalen Normung bestehen und Gültigkeit erlangen. DIN SPECS ermöglichen hier einen äußerst schnellen ersten Schritt, der per FastTrack in die internationale Normung führen kann.

4.19 Industrie 4.0 - Potential zum Leitmodell

Zur Herangehensweise an die Entwicklung einer Referenzarchitektur:
Industrie 4.0 hat das Potential zum Leitmodell - auf dem Weg zu einem domänenübergreifenden Framework.

Wie zuvor mehrfach thematisiert, sind die Branchen oder Entwicklungsbereiche unterschiedlich weit beim Thema. Für einzelne Bereiche wurden bereits umfangreiche aber spezifische Lösungen zu SDI und diesbezüglichen Infrastrukturen geschaffen. Für das Projekt Industrie 4.0 genügt keine spezialisierte Branchenlösung und es hat daher noch keinen einheitlichen Ansatz zu einer SDI-Struktur. Es hat dabei aber einen der höchsten Handlungsbedarfe, denn ohne die sichere Kommunikation und das sichere unternehmens- und grenzübergreifende adhoc-Wertschöpfungsnetzwerkebildende Interagieren ist Industrie 4.0 nicht umsetzbar.

Die Anforderungen an eine SDI-Struktur für Industrie 4.0 verlangen einen sehr breiten und gut strukturierten Ansatz von Lösungen. Denn das Zukunftsprojekt hat sehr viele unterschiedliche, teils sehr anspruchsvolle und in der Gesamtbetrachtung sehr bedeutende Anwendungsfälle. Eine vereinheitlichte Umsetzung einer SDI-Infrastruktur würde im Bereich Industrie 4.0 schnell grenzübergreifend. Zudem ist die Industrie 4.0 mit diversen anderen Branchen unmittelbar verbunden.

→ In einem orchestrierten Prozess kann Industrie 4.0 daher von den bereits weiterentwickelten anderen Branchen und deren Teillösungen lernend und gleichzeitig in weitere Bereiche zurückspielend elementar zu der Entwicklung des notwendigen domänenübergreifenden Ansatzes beitragen bzw. sogar selbigen als Grundlage dienen. In einem solch offenen Prozess würde Industrie 4.0 zum Leitmodell und ein Mehrwert für alle geschaffen.

Der erste Schritt wurde bereits gemacht. Und mit der jetzigen Projektphase eingeleitet indem die unterschiedlichsten Akteure und Projekte (IDS, BSI, IUNO, PI4.0, BDR etc.) zusammengebracht wurden und ein erster Fahrplan verfasst und gestartet wurde (vgl. Kapitel 2.1.5).

„Industrie 4.0 hat dahingehend bspw. sehr viele unterschiedliche Use-Cases.“

„Die große Herausforderung für Industrie 4.0 im Sinne von Infrastruktur ist die Ausgestaltung des Konzept von Identitätsdomänen. Das Ziel ist es dabei, global Identitäten ausgeben, verifizieren und revozieren zu können.“

„Weil ein sicherer Informationsaustausch entlang des gesamten Wertschöpfungsprozesses für Industrie 4.0 essentiell ist. Dies erfordert die eindeutige Identifikation und Authentifizierung von Menschen, Maschinen und Prozessen sowie den Nachweis best. Eigenschaften inkl. der Möglichkeiten zur Abstufung der Sicherheit.“

„Bei der Industrie 4.0 hat der Enduser - repräsentiert durch seine SDI - großen Einfluss auf Produktions-Prozesse, z.B. bei Bestellungen oder der Steuerung von Fertigungsabläufen.“

„Aber auch außerhalb der Bankenwelt steigt der Bedarf nach sicheren Identitäten, hier vor allem im Rahmen der Digitalisierung und Industrie 4.0. Da mehr und mehr Geschäftsprozesse die Firmengrenzen überschreiten, gerät das Paradigma des "abgesicherten Firmen-Netzwerks" mehr und mehr in den Hintergrund. Stattdessen sind Lösungen gefragt, die über Firmengrenzen hinweg Kunden, Mitarbeiter, Partner und externe Workforce zusammenbringen und verbindlich und vertraulich miteinander kommunizieren lassen können müssen.“

„Im industriellen Umfeld können SDI auf Produktebene bis hinunter zum Einzelstück dazu beitragen Transparenz über die gesamte Supply Chain zu erhalten. Damit lassen sich wirksame Strategien gegen Produktpiraterie oder illegitimen Handel entwickeln.“

„Für den multilateralen Austausch von Industriedaten stellen sichere Identitäten eine inhärente Security Eigenschaft dar.“

Zitate aus den Fragebögen /
Expertenkonsultationen

4.20 Auswirkungen – über die digitale Welt hinaus

Zur Herangehensweise an die Entwicklung und Implementierung einer Referenzarchitektur: Die Marktdurchdringung der Nutzung von SDI auf Basis oder verbunden durch einer Referenzarchitektur wird auf die unterschiedlichsten bestehenden Verfahren, Prozesse, Strukturen etc. auswirken – auch über die digitale Welt hinaus. Erst hier wird sie tatsächlich zur Anwendung kommen.

Da Digitale Identitäten fast überall notwendig und relevant sein werden, wird ein sicheres Erstellen und Nutzen derselben sich auf unterschiedlichste Vorgänge und Sachverhalte in der physischen Welt beziehen - nicht zuletzt weil die Implementierung von SDI in vielen Anwendungsfällen die Verbindung von digitaler und physischer Welt bedeutet.

→ Es geht hierbei um die Integration der SDI in der breiten Anwendungslandschaft, welches im Bereich der Normung bedeutet, das Thema und die durch den Framework entstehende konsistente Herangehensweise in unterschiedlichste Normungsaktivitäten, wie der Produktion, der Arbeitsorganisation, des Management, der Dokumentation, der Inventarisierung, der Verpackungsgestaltung etc. p.p. einzubringen.

Hier findet sich in der Normung der Hebel, schnell in viele weitere Bereiche zu wirken. Das Thema käme so zudem auch auf die Agenden von Digitalisierungsnachzüglern und Deutschland könnte ggf. führend in der Anwendung von SDI werden.

„Wie weitreichend die Auswirkungen des Themas sind, zeigt sich bspw. daran, dass alles was safety-relevant ist dadurch, dass ja überall das Internet „drangeklatscht“ wird, nun auch security-relevant wird. Der Impact ist nochmal größer und trifft auch diese bisher analogen Bereiche und sämtliche diesbezügliche Prozess, Regeln etc.“

"Aber grundsätzlich ist es tatsächlich die Frage, was sind da auch für Auswirkungen auf das gesellschaftliche Gebilde"

„Auch die kreuzweise Nutzung ist zu berücksichtigen, wie Person im Office-Bereich kommuniziert mit der Maschine in der Produktion.“

„In diesem Sinne betrifft SDI ganze Themenbereiche, wie Anlagensicherheit, Produktzulassung, Betriebssicherheit etc.“

„Manche Kennzeichnungslösungen etablieren, wenn sie auf das Produkt oder ein Dokument (untrennbar) aufgebracht werden, dessen SDI. Deshalb muss im Beauftragungs-, Herstell-, Verteilungs- und Zuordnungsprozess dieser Produkte eine lückenlose Verfolgbarkeit dargestellt werden. Der Austausch dieser Daten geht über mehrere Domänen hinweg.“

„Eine Fokussierung auf Produkte deckt nur Teilaspekte ab. Echte SID sind nur möglich, wenn diese in Vertrauensinfrastrukturen eingebettet sind, die erkennen lassen, welche Güte der Identifizierung zugrunde liegt, welche Anwendungen damit verbunden sind und wie die SID zu prüfen und zu ggf zu sperren ist.“

[Notwendig ist auch...] „Kontrolle der Einhaltung von Compliance Regeln längs der Logistikkette.“

Zitate aus den Fragebögen /
Expertenkonsultationen

4.21 Auswirkungen – Forschungs- und Infrastrukturbedarf

Zur Herangehensweise an die Entwicklung und Implementierung einer Referenzarchitektur: Die Entwicklung und Anwendung einer Referenzarchitektur wird auch Lücken aufzeigen und neue Forschungsvorhaben identifizieren oder Infrastrukturbedarf adressieren.

Die Zusammenführung der verschiedenen bestehenden Identitätslösungen in einem Referenz- und Interaktionsmodell wird aufzeigen, wo und bzgl. welcher Anwendungsfälle es noch Herausforderungen gibt, dem keine aktuellen Lösungen (auch nicht in anderen Branchen) gegenüberstehen. Selbiges gilt für Infrastrukturen bspw. für die Interaktion von Unternehmen und Domänen. Diese konkret identifizieren zu können wird ein Ergebnis des konzertierten Vorgehens sein. In diesem Sinne werden sich ggf. weiterer Forschungs- oder Infrastrukturbedarf sehr spezifisch adressieren lassen. Von einzelnen Experten wurde hinsichtlich Infrastrukturen (Trust Center) auch derzeit ein Marktversagen vermutet, dem es zu begegnen gilt.

„Vielleicht braucht es auch, das zur Verfügung stellen von Plattformen oder Infrastrukturen.“

„Es kann kein rein staatliche getriebenes Vorgehen sein, bei dem Regulierungen und Vorgaben gemacht werden. Jedoch könnte es eine öffentliche Finanzierungsaufgabe sein, die notwendige Basisinfrastruktur zur Verfügung zu stellen, sodass es hier ein gemeinsames Vorgehen gibt.“

„Was fehlt und ob die Definitionen reichen lässt sich aufgrund der Komplexität und des unklaren Scopes derzeit nicht beantworten. Hilfreich wäre jedoch eine Art Landkarte mit den diversen Systemen und den generell relevanten Aspekten und unterschiedlichen disziplinären " Brillen".“

„Es „fehlen“ neutrale Anbieter, die als Cloud zwischen den einzelnen Unternehmensdomänen liegen und die Kommunikation herstellerübergreifend vereinfachen/bündeln“

Zitate aus den Fragebögen /
Expertenkonsultationen

4.22 Auswirkungen – juristischer und gesetzlicher Art

Zur Herangehensweise an die Entwicklung und Implementierung einer Referenzarchitektur: Die Implementierung eines SDI-Frameworks wird auch juristische und gesetzliche Auswirkungen haben.

Mit der eIDAS und Datenschutzgrundverordnung haben wir zwei maßgebliche Rechtsvorschriften, die u.a. einen Rahmen geben in dem die Normen und Standards entwickelt werden müssen.

Sowohl einzelne Experten, wie auch die Rechtsrecherche zeigten auf, dass von einer konsequenten Implementierung einer SDI-Struktur juristische und gesetzliche Sachverhalte betroffen sein werden.

Zum einen sind dies Auswirkungen auf die Anwendung und Durchsetzung von Gesetzen in der digitalen Welt - bspw. dadurch, dass sich Haftungsfragen besser klären lassen.

Zum anderen werden sich Sachverhalte ergeben, die im Rahmen einer gelebten SDI-Struktur Anpassungsbedarf hinsichtlich Gesetzestexten sinnvoll machen. Dies zeichnet sich bspw. bereits hinsichtlich des Themas Anlagensicherheit bezogen auf die M2M-Kommunikation ab.

„Die Kernaufgabe der Politik ist letztlich die rechtlichen Standards zu setzen, dazu muss aber ein Verständnis da sein, was überhaupt passiert!“

„Die größte Herausforderung [...] in der rechtzeitigen Anpassung der Gesetzeslage. Eine zu restriktive Gesetzeslage ist marktverhindernd und stoppt die Technik. Eine fehlende Anpassung kann dazu führen, dass neue Produkte nicht aufgegriffen werden. So wurde durch die eIDAS-Verordnung der EU ein qualifiziertes Siegel geschaffen. Dies wurde jedoch kaum in nationale Gesetze übernommen, so dass viele Prozesse in den Behörden nicht oder nur sehr umständlich digitalisiert werden können. Hier wäre etwa das qualifizierte Siegel in der Telematik Infrastruktur ein sehr gutes Mittel, jedoch fehlt hier wiederum die Anpassung des Sozialgesetzbuches, um es als elektronisches Mittel einsetzen zu können.“

„In Zukunft gibt es grundsätzlich eine gigantische Regelungslücke in dem ganzen Umfeld, z.B. zu Haftungsfragen. Die Legislative hinkt den technologischen Möglichkeiten um Generationen hinterher.“

„Es braucht von der Anlage her die Option einer Steuerbarkeit, risikobasiert im jeweiligen Use-Case, aber es braucht bitte keine Vorgaben, wie gesteuert werden soll.“

„Hier wäre etwa das qualifizierte Siegel in der Telematik Infrastruktur ein sehr gutes Mittel, jedoch fehlt hier wiederum die Anpassung des Sozialgesetzbuches, um es als elektronisches Mittel einsetzen zu können.“

Zitate aus den Fragebögen /
Expertenkonsultationen

4.23 Politisches Engagement notwendig

Zur Herangehensweise an die Entwicklung und Implementierung einer Referenzarchitektur: Die Digitalisierung fordert jedes Unternehmen, jede Organisation, jeden Akteur auf den unterschiedlichsten Ebenen. Ein konzertiertes Vorgehen zum Grundlagenthema SDI wird daher nur erreichbar, wenn ein politisches Engagement dem Vorhaben nachhaltig Gewicht verleiht und so die breite Mitarbeit der Akteure rechtfertigt.

Fast überall wo digitale Identitätslösungen Relevanz haben oder bekommen, sind die Akteure zunächst einmal konzentriert auf den Fokus ihres Projektes, ihres Unternehmens, ihres Netzwerkes oder Branche. Es gilt selbigen fit für die digitale Transformation zu machen oder diesbezüglich neue digitale Business Cases zu entwickeln. Allein das bindet umfassende finanzielle aber insbesondere humane Ressourcen. Die hierbei notwendigen Identitätslösungen werden daher oftmals nur individuell mitgelöst oder Engagement auf konkrete Branchenlösungen konzentriert (vgl. Kap. 4.5 und 4.6). Die notwendige domänenübergreifende Herangehensweise wird insbesondere aus gesamtwirtschaftlicher und –gesellschaftlicher Perspektive zwar gesehen, aber einer diesbezüglichen Initiative würde sich nur zugewendet, wenn von ihr ein entsprechender Impact für den eigenen Bereich und spätere Interaktionspartner erwartet werden kann. Die Grundlage hierfür zu schaffen, wird von vielen Experten als Aufgabe des Staates angesehen und es wurden die Forderungen nach einem konzertierten Vorgehen, Standards, Referenzmodellen etc. mit der konkreten Forderung an die Politik verbunden, selbiges zu fördern bzw. ein Zeichen zu setzen, damit alle Akteure sehen, hier soll die Arbeit konzentriert werden.

Im Sinne des Kap. 4.20 ist für die breite Implementierung neben und mit dem politischen Engagement auch das verbandspolitische Involvement anzustreben, damit das Erreichte umfassend Wirkung entfaltet.

„Gefahr und beliebtes Spiel ist, dass sich bei der Finanzierung die Bälle hin und her gespielt werden. Das gilt es zu vermeiden. Die einzelnen Unternehmen sagen, sie bringen sich da ja mit Manpower, Expertise und KnowHow ein und da profitiert dann die ganze Industrie von. Und hier eben nicht nur die Industrie, sondern auch der Staat.“

„Hierzu sollten Förderprogramme den Standardisierungsprozess unterstützen.“

„Da muss viel mehr Momentum dahinter, um da etwas auf die Beine zu stellen. Da braucht man wirklich Kontinuität und auch Geld dafür und auch Leute, die bezahlt dafür arbeiten. - Das geht nicht nebenher. Man kann sich nicht ein großes Ziel setzen, die Big Five [Big Five meint: Google, Apple, Microsoft, Amazon, Facebook] zu kontern und dann darauf hoffen, dass eine Unterarbeitsgruppe, die sich vielleicht alle 2 Monate trifft, das stemmt. Das geht so nicht, da muss mehr her.“

„Der Prozess muss generell gefördert werden, die Politik darf sich hier aber nicht zu viel anziehen oder regulieren.“

„Es braucht da eine noch fruchtbarere Zusammenarbeit zwischen Industrie und Staat.“

„Man muss da auch Anreize schaffen, damit die Industrie sich da überhaupt mit einbringt. Das [bezogen darauf, dass sich die Industrie hier einbringt] passiert im Moment viel zu wenig [...] und man damit das Feld den anderen überlässt.“

„Das BMWi muss anerkennen, dass die Hütte von oben und unten lichterloh brennt. Und da kann man sich nicht zurücklehnen und sagen, das haben wir im Griff.“

„Es kann kein rein staatliche getriebenes Vorgehen sein, bei dem Regulierungen und Vorgaben gemacht werden. Jedoch könnte es eine öffentliche Finanzierungsaufgabe sein, die notwendige Basisinfrastruktur zur Verfügung zu stellen, sodass es hier ein gemeinsames Vorgehen gibt.“

Zitate aus den Fragebögen /
Expertenkonsultationen

5 Master- und Strukturplan für Sichere Digitale Identitäten

Der vorliegende Bericht zeigt auf, dass das Thema SDI ein Grundlagenthema für die gesamte Digitalisierung und digitale Vernetzung darstellt. Daher sollte auch hier der Staat seine Schutzfunktion erfüllen, indem er auf das Entstehen einer Infrastruktur hinarbeitet, die SDI für den einzelnen Bürger, die Gesellschaft und die Wirtschaft über Branchen- und Sektorengrenzen hinweg garantiert und so zu einem digitalen Ökosystem führt, welches für mehr Sicherheit für alle Beteiligten sorgt und rechtsfreie Räume verhindert.

Es wurde aufgezeigt, dass es nicht eine technische Lösung für alle Anwendungsfälle gibt. Vielmehr handelt es sich um eine Vielzahl an technischen und organisatorischen Lösungen und Teillösungen. Diesbezüglich sind bereits viele Insellösungen entstanden und trotz der zunehmenden Notwendigkeit der Interoperabilität wird individuell weiterentwickelt. Die Lösungen entstanden und entstehen teils für einzelne Projekte, für Unternehmen oder für Branchen. **Insbesondere den größeren Wirtschafts- oder Forschungsinitiativen beziehungsweise Zukunftsprojekten, wie z.B.:**

- Industrie 4.0
- eMobility
- Smart Cities
- Smart Home / AAL
- Industrial Data Space
- eHealth
- Mittelstand 4.0

reichen dabei Insellösungen allerdings nicht aus, sondern es bedarf einer domänen- und entitätenübergreifenden Interoperabilität.

Der Anwendungsscope der bisherigen Lösungen ist zwar mal kleiner mal größer, eine generische zusammenführende Betrachtung, Bearbeitung und Entwicklung erfolgt allerdings auch bei den domänenübergreifenden Initiativen bisher nicht. Sie würde aber zeigen, dass die Gesamtheit der Lösungen bereits deutlich mehr abdeckt, als es die Inselbetrachtungen annehmen (vgl. sinngemäß Abbildung 38). Insbesondere für die genannten Zukunftsprojekte ist dies relevant (hier exemplarisch in der Abbildung als rote Domäne 5 mit einem Bedarf an Identitätslösungen dargestellt). Es zeigen sich also umfassende Synergie- und Innovationspotentiale. Um diese aber nutzen zu können, besteht die Notwendigkeit, Interoperabilität und domänenübergreifende Sicherheitsniveaus bei den Insellösungen herzustellen.

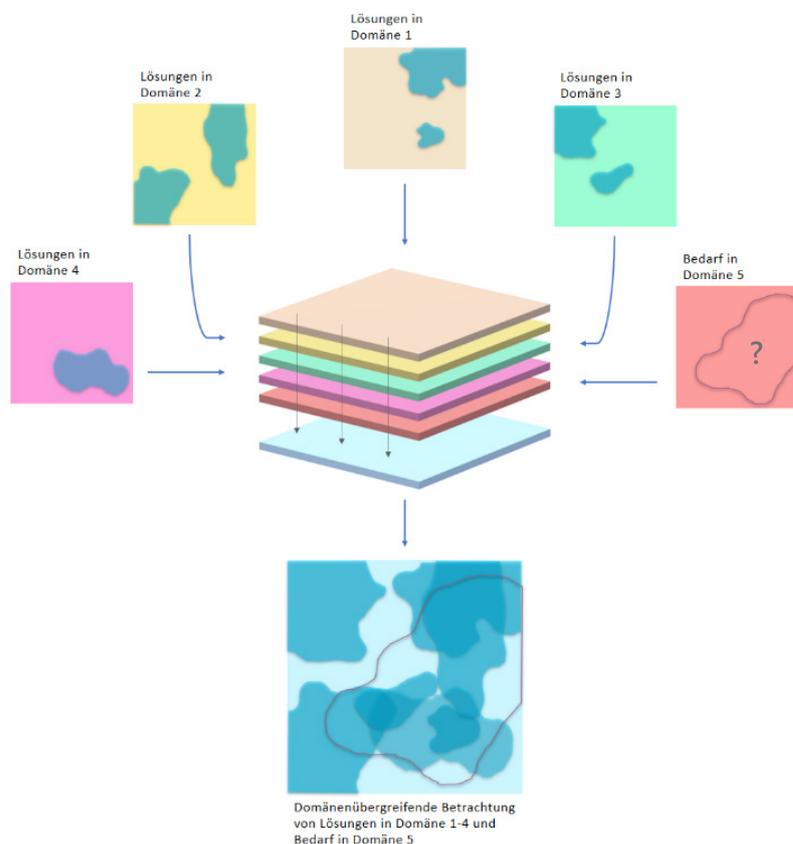


Abbildung 38 – domänenübergreifende Betrachtung von Identitätslösungen (Redundanzen, Synergie- und Innovationspotentiale)

Wenn nun durch die weitere Konvergenz von Technologien und Systemen die Inseln zusammenwachsen sollen⁶³, dann kann das nur geschehen, wenn die Lösungen auf gleichen Prinzipien und Verfahren beruhen. Um dies zu erreichen wird folgend eine Lösungsmethodik vorgeschlagen. Diese Lösungsmethodik berücksichtigt die bereits bestehenden Lösungen und Projekte und sorgt für einen gemeinsamen und branchenübergreifenden Rahmen als Garant für Interoperabilität.

Im Sinne des Ansatzes gilt daher, die vorhandenen Strukturen, Standards und Lösungen zu sammeln, zu beschreiben und in Beziehung zueinander zu setzen und aus ihnen eine gemeinsame Referenzarchitektur abzuleiten (vgl. bereits auch Abbildung 40). Hierbei ist eine Zusammenarbeit mit und zwischen den unterschiedlichsten bestehenden Gremien und Stakeholdern zu organisieren und zu koordinieren:

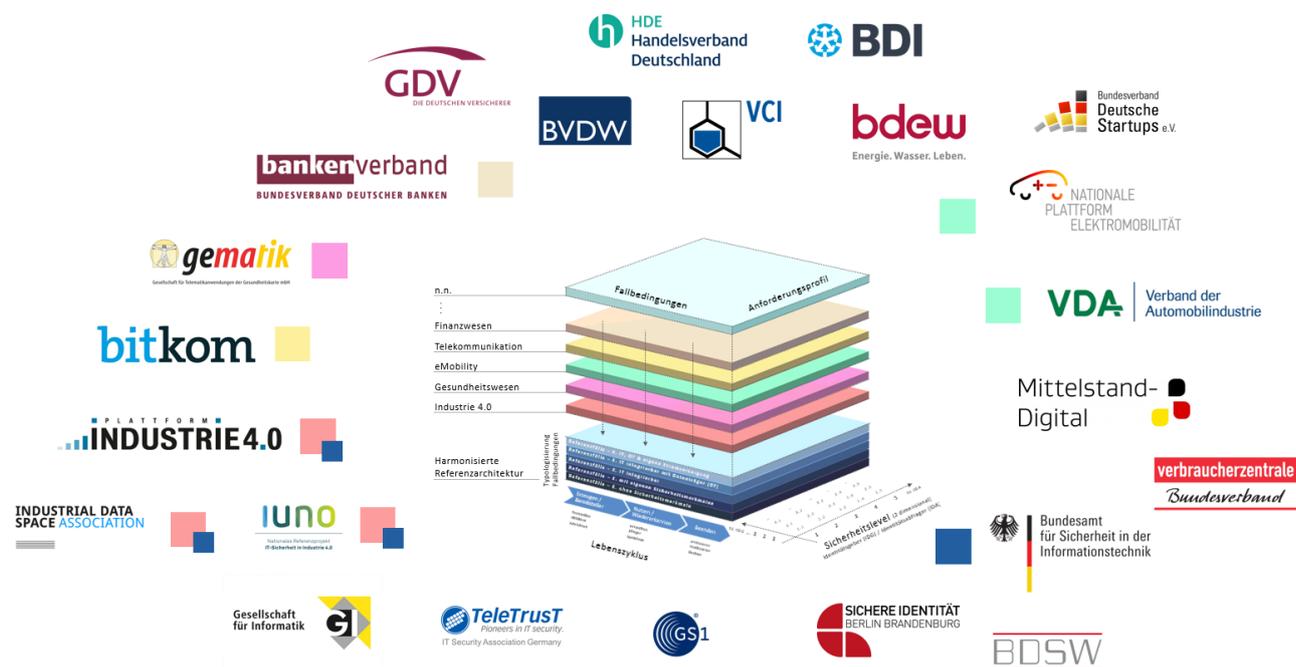


Abbildung 39 – exemplarische Auflistung von Stakeholdern mit bestehenden oder zu aktivierenden Gremien oder ansprechbaren Stellen, die im Sinne eines Aktionsnetzwerkes zum Thema eingebunden werden sollen

Die Referenzarchitektur kann für die Weiterentwicklung aller bestehenden sowie den zu entwickelnden Lösungen und Strukturen Orientierung geben. Das Inbeziehungsetzen der bestehenden Lösungen und Strukturen kann hierbei in eine Art Schnittstellenmatrix fließen, die es einfacher erlaubt, die bestehenden Systeme der Domänen miteinander zu vernetzen oder sich selbigen anzuschließen. Solch komplexe und branchenübergreifende Themen können nur dann gelöst werden, wenn es einen Akteur gibt, der eine neutrale und koordinierende Funktion mit einer von allen Beteiligten anerkannten Governance ausübt.

⁶³ Als Beispiele hierfür können angeführt werden:

- (a) Blockchain - ursprünglich für das Management der Kryptowährung Bitcoin eingesetzt, gibt es heute Ansätze für den Einsatz von Blockchains in verschiedenen Branchen (Versicherungen, Industrie, etc.). Wenn nun z.B. industrielle, technische Anwendungen mit finanztechnischen Prozessen kombiniert werden sollen, bedarf es einem gemeinsamen Verständnis und gemeinsamen Grundlagen.
- (b) die Digitalisierung von Unterhaltungselektronik und Fahrzeugelektronik ist in der Vergangenheit von den jeweiligen Branchen gemanagt worden. Durch den zunehmenden Einzug von Multi-Media Technologien in Fahrzeuge sind jedoch Sicherheitslücken entstanden - und es werden Weitere entstehen -, die nur durch eine übergreifende Koordination aller beteiligter Parteien gelöst werden können.

Die im Rahmen des Projekts befragten Unternehmen, Initiativen und Organisationen halten eine solche neutrale Koordination und Kommunikation für erforderlich. Sie sorgt dafür, dass die einzelnen Lösungen zu einem interoperablen System führen:

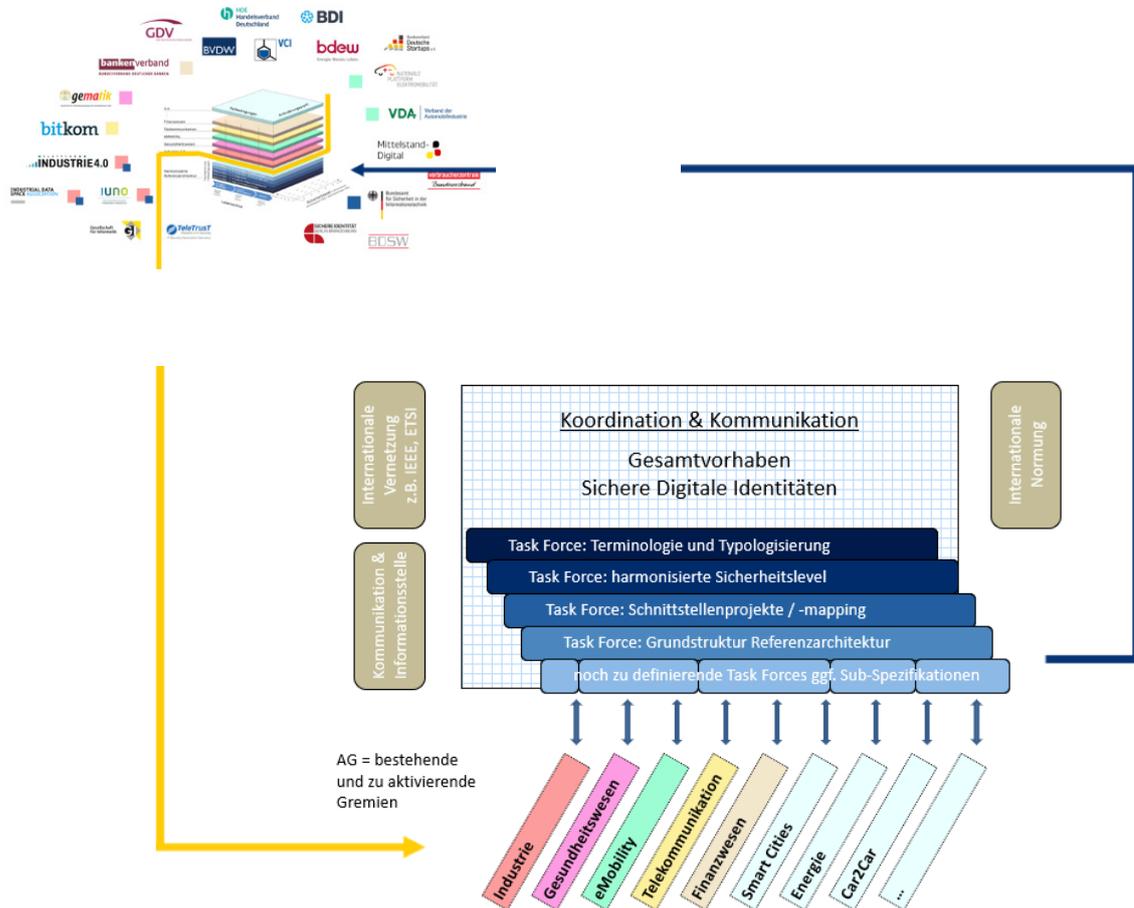


Abbildung 40 – kooperative Entwicklung einer Referenzarchitektur durch neutralen Akteur

Die Interoperabilität muss aber nicht nur national und europäisch, sondern international erreicht werden. Damit wird klar, dass nicht nationale Regulierungen notwendig sind, sondern ein internationaler Konsens, der sich in Form von Normen und Standards niederschlägt. Deutschland hat zurzeit noch die Möglichkeit ein bestehendes Vakuum an internationalen Normen zu nutzen, um maßgeblich die notwendigen Normen mitzugestalten. Mit einem domänenübergreifenden Netzwerk und ganzheitlichem Ansatz wird sich Deutschland von bestehenden Aktivitäten abheben und kann bei der internationalen Gestaltung und Anwendung Sicherer Digitaler Identitäten eine Führungsrolle einnehmen.

Abgeleitet aus den vorliegenden Erkenntnissen werden im Folgenden inhaltliche Koordinierungsaktivitäten und der diesbezüglich notwendige Aufbau eines domänenübergreifenden Aktionsnetzwerkes vorgeschlagen. Damit werden Akteure, Interessen, KnowHow und Entwicklungen der verschiedenen Branchen und Sektoren zusammengebracht und effizient orchestriert. So wird eine anwendbare Referenzarchitektur kooperativ entwickelt, dient neuen Vorhaben als Grundlage und unterstützt die sukzessive Zusammenführung bestehender Insellösungen.

5.1 Inhaltliche Koordinierungsaktivitäten

Die Befragungen und Analysen im vorliegenden Projekt haben den Bedarf für das **branchenübergreifende Identifizieren, Initiieren und Führen von Themen** bei der Schaffung und Nutzung von Sicheren Digitalen Identitäten ergeben. Die dabei identifizierten Themenbereiche sind:

- (1) **Terminologie und Typologisierung**
- (2) **a) Grundstruktur Referenzarchitektur u. systematische Aufgliederung in Spezifikationsvorhaben
b) an Referenzarchitektur orientierte Bereichs-Spezifikationen (Group- & Product-Publications)**
- (3) **harmonisierte Sicherheitslevel**
- (4) **Schnittstellenprojekte / -mapping für kurzfristige Interoperabilität bestehender Systeme**

Mit der hier genannten Struktur beginnend soll eine Normungs-Roadmap gestaltet, umgesetzt und stetig fortgeschrieben werden. Die **SDI-Roadmap** Sicherer Digitale Identitäten ist die wichtigste Grundlage für einen Austausch mit Industrie, Verbänden, Forschungseinrichtungen, Ministerien und Normungs- / Standardisierungsgremien. Sie wird der Wegweiser für Akteure aus verschiedenen technologischen Branchen und unterstützt damit bereits entwicklungsbegleitend die Marktrelevanz der Technologien und Verfahren. Ziel der Roadmap ist es, den Akteuren eine Übersicht über relevante Lösungen und Ihre Normen und Standards zu geben und das aktuelle Umfeld aufzuzeigen. Die Roadmap enthält Handlungsempfehlungen und skizziert Normungsbedarfe im Themenbereich SDI.

Im Ergebnis der Koordinierungsaktivitäten sollen notwendige **Szenarien, Empfehlungen, Leitfäden, und Spezifikationen entwickelt werden**. Sie basieren weitgehend auf branchenspezifischen Erfahrungen und können von anderen Branchen und Organisationen adaptiert werden. Sie sollen ein harmonisiertes und kohärentes Rahmenwerk für Sichere Digitale Identitäten schaffen. Sie bieten ganz konkrete Hilfestellungen bezogen auf konkrete Branchen, Lebenszyklen, Anforderungsprofile, Dimensionen von Entitäten und ermöglichen es dem Leser somit, für sein Anwendungsproblem schnell eine Lösung zu finden. Sie fördern den Wissens- und Technologietransfer, insbesondere dann, wenn sie via DIN SPEC o.ä. in die internationale Normung Einzug halten.

5.1.1 Koordinierungsthema (1) – Terminologie und Typologisierung

In den unterschiedlichen Branchen werden oft Worte und Begrifflichkeiten mit unterschiedlicher Bedeutung und in unterschiedlichem Kontext benutzt. Auch der Begriff der „Sicheren Digitalen Identität“ an sich wird, wie in Kapitel 3.1.1 adressiert, noch nicht einheitlich behandelt. Ein Schlüsselement, um überhaupt zwischen Vertretern unterschiedlicher Branchen eine einheitliche Sprachregelung zu erreichen, ist die gemeinsame Definition der benutzten Begriffe und ihre Einordnung bzw. Klassifizierung. Die wird in der Koordinierungsaufgabe „Terminologie und Typologisierung“ erreicht.

Es wird dabei ein Dokument erzeugt, das alle Begriffe des Themas „Digitale Identitäten“ aufführt und gleichzeitig eine gemeinsam getragene Definition und Einordnung aller beteiligten Kreise einführt.

Das Dokument sollte idealerweise als DIN SPEC entstehen, so dass der Entstehungsprozess nach einem anerkannten Verfahren abläuft und auch die weiteren möglichen Schritte der Verbreitung und Internationalisierung gegeben sind, z.B. über das Einbringen der DIN SPEC in den internationalen Standardisierungsprozess auf europäischer oder ISO-Ebene.

Aus dem domänenübergreifenden Aktionsnetzwerk sollten für die Teilnahme an dieser Aufgabe einerseits Vertreter aus möglichst unterschiedlichen Branchen / Zukunftsprojekten / Domänen (Vertreter aus einschlägigen Verbänden) gewonnen werden, wie auch Firmen und Institutionen, die eine besondere Expertise auf dem Gebiet der Digitalen Identitäten haben, z.B. die Bundesdruckerei oder das Bundesamt für die Sicherheit in der Informationstechnik (BSI). Das Aktionsnetzwerk dient zudem zur zeitnahen Kommentierung und Einschätzung der Ergebnisse.

Als zeitlicher Rahmen bis zur Veröffentlichung ist eine Dauer von 6 Monaten ab Kick-Off-Termin vorgesehen.

5.1.2 Koordinierungsthema (2a) – Grundstruktur Referenzarchitektur und systematische Aufgliederung in Spezifikationsvorhaben

Das Kernelement der Referenzarchitektur, die allen bestehenden und entstehenden Vorhaben als harmonisierende Grundlage dienen soll, ist gewissermaßen eine strukturierende Karte des Gesamtsachverhalts, in der alle Aktivitäten, Normen und Standards verortet werden können (vgl. Kap. 3). In diesem Sinne dienen auch bestehende Werke als Grundlage ihrer Gestaltung, aber eben aufbereitet, als Gerüst, mit dem be- und entstehende Standardisierungen verankert werden. Sie wird somit strukturgebender Grundbaustein der SDI-Roadmap.

„Es ist auf jeden Fall interessant, am Ende zu einer Infrastruktur zu kommen oder zu einem Rahmenwerk, aus dem ich Handlungsempfehlungen ableiten kann, technisch oder auch organisatorisch.“

Zitat aus den Fragebögen / Expertenkonsultationen

Wie das Projekt gezeigt hat, sind die Teilsachverhalte von einer solchen Vielfalt und Komplexität, dass sie nicht in einem Dokument sinnvoll behandelt werden könnten. Die wesentliche Koordinierungsaufgabe liegt daher bei der „Grundstruktur“ darin, mit allen Beteiligten Unterbereiche zu definieren, die in eigenen Spezifizierungsvorhaben behandelt werden. Die Aufgliederung des Gesamtsachverhalts könnte z.B. zum einen in generische Auseinandersetzungen mit den einzelnen Schritten des Lebenszyklusprozesses (Feststellen, Abbilden, Einrichten, Verwalten, etc.) erfolgen und zum anderen wäre eine Aufgliederung nach Entitätsgruppen denkbar.

Die Grundstruktur der Referenzarchitektur ist somit [A] Base Standards (grundlegendes Konzept, Prinzipien und Anforderungen) und Ausgangspunkt für weitere Base Standards sowie [B] Group Publications (Anforderungen in einer Domäne oder

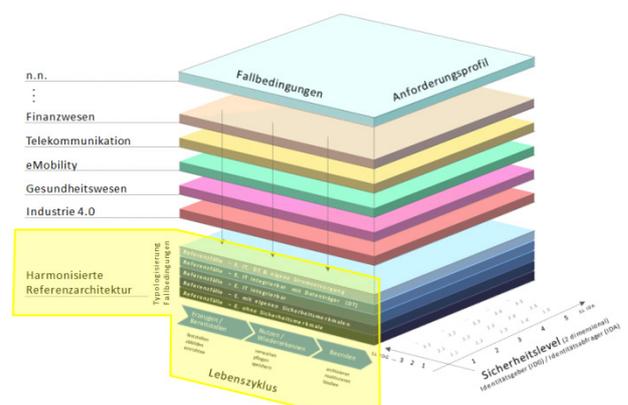


Abbildung 41 – Koordinierungsaufgabe Grundstruktur Referenzarchitektur

Produkt- oder Systemfamilien), [C] Product Publications (Anwendungsdefinition von [A] und [B] auf einen Produkttyp) bis hin zu [D] Guidance (Leitlinien, Beschreibung von der konkreten Umsetzung [A],[B] und [C]) oder [D] Test Publications (Möglichkeiten des Tests der Einhaltung der Anforderungen aus [A],[B] und [C]) - vgl. Kapitel 2.3.3 erster Teil. In diesem Sinne entsteht durch Referenzarchitektur und Roadmap ein „Spezifikationsbaum“, der bis hin zu unmittelbaren Guidelines (nutzbar auch für KMU) Orientierung und konkrete Handlungsempfehlungen bietet.

In diesem Sinne wird ein Dokument erzeugt, das eine gemeinsam getragene generische Beschreibung des Gesamtsachverhalts beinhaltet und die Verortung aller bestehenden und entstehenden Aktivitäten erlaubt. Dies beinhaltet eine systematische Aufgliederung, die detailliertere bis anwendungsbezogene Spezifikationsvorhaben für Teilbereiche einleitet.

Das Dokument und seine Unterdokumente sollten idealerweise als DIN SPEC entstehen, so dass der Entstehungsprozess nach einem anerkannten Verfahren abläuft und auch die weiteren möglichen Schritte der Verbreitung und Internationalisierung gegeben sind, z.B. über das Einbringen der DIN SPEC in den internationalen Standardisierungsprozess auf europäischer oder ISO-Ebene.

Aus dem domänenübergreifenden Aktionsnetzwerk sollten für die Teilnahme an dieser Aufgabe einerseits Vertreter aus möglichst unterschiedlichen Branchen / Zukunftsprojekten / Domänen (Vertreter aus einschlägigen Verbänden) gewonnen werden, wie auch Firmen und Institutionen, die eine besondere Expertise auf dem Gebiet der Digitalen Identitäten haben, z.B. die Bundesdruckerei oder das Bundesamt für die Sicherheit in der Informationstechnik (BSI). Das Aktionsnetzwerk dient zudem zur zeitnahen Kommentierung und Einschätzung der Ergebnisse.

Als zeitlicher Rahmen bis zur Veröffentlichung ist eine Dauer von 6 Monaten ab Kick-Off-Termin vorgesehen. Das Einleiten von weiteren Spezifikationsvorhaben muss allerdings in Teilen unmittelbar und interdependent erfolgen (siehe folgendes Unterkapitel).

Das bearbeitende Gremium der Referenzarchitektur kann möglicherweise in eine Art. „Standing Task Force Referenzarchitektur / Roadmap SDI“ umgewandelt werden, die das Gremium darstellt, dass alle Task Forces / Arbeitsausschüsse übergeordnet, gesamthaft koordiniert und daraus die operativen Elemente der Roadmap ableitet und regelmäßig updatet.

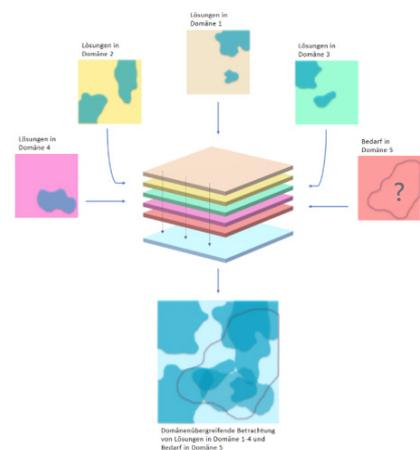
5.1.3 Koordinierungsthema (2b) – parallele Bearbeitung an Referenzarchitektur orientierter Bereichs-Spezifikationen (Group- & Product-Publications)

Die außerordentliche Geschwindigkeit mit der die Digitalisierung voranschreitet und Zukunftsprojekte sich jetzt akut mit dem Thema beschäftigen müssen, erfordert ein paralleles Vorgehen auf mehreren Ebenen. In diesem Sinne ist es notwendig neben der generischen Bearbeitung, bestehende Spezifikationsvorhaben einzubinden sowie auch für bestimmte konkrete Anwendungsfälle und Entitäten neue Spezifikationsvorhaben unmittelbar einzuleiten. Hierbei ist explizit das Vorhaben zu nennen, welches im Rahmen dieses Projektes mit der Plattform Industrie 4.0 und weiteren zentralen Akteuren angegangen und konkretisiert wurde (vgl. Kapitel 2.1.5 und Anhang sowie 4.16.1), wo bereits auf Protokollebene konkrete Spezifikationen für bestimmte Anwendungsfälle und Entitäten erwogen werden. Bei der Umsetzungs-

planung des Gesamtvorhabens ist zu berücksichtigen, dass der Koordinierungsaufwand dadurch maßgeblich steigt.

Es soll dahingehend eine parallele aber zwingend interdependente Erarbeitung der generischen Referenzarchitektur und solcher unmittelbar konkreter anwendungsbezogener Spezifikationen (Group oder Product Publications) stattfinden. Letztere können und sollten wesentlich durch die vorhandenen Branchen- oder Projektgremien (letzteres i.S.v. Zukunftsprojekten, siehe 5.1) geprägt werden und sichern so die Anwendungsbezogenheit der Spezifikationen und Standards. Erstere sichert die domänen- und entitätenübergreifende Gestaltung derselben für eine zukunftsfähige Gesamtstruktur.

Es ist zu unterstreichen, dass nur die interdependente Herangehensweise sinnführend ist. Ansonsten würden die Bereichsspezifikationen nur zu weiteren Insellösungen und ein späteres Zusammenwachsen zu hohen Kosten führen. Zudem profitieren die Akteursgruppen direkt voneinander (vgl. Abbildung 38, Die rote Domäne 5 steht hier exemplarisch für Industrie 4.0 und deren Bedarf an Lösungen.), können Synergie- und Innovationspotentiale nutzen und es ergibt sich die Möglichkeit, dass sich einzelnen Vorhaben weitere Akteure auch domänenübergreifend anschließen. Dies ist bei der vorgezogenen Einleitung beim Bereich Industrie 4.0 bereits in mehrfacher Hinsicht der Fall gewesen.



vgl. Abbildung 38, Einleitung Kapitel 5

In diesem Sinne werden mehrere Dokumente gleichzeitig entstehen. Alle Dokumente sind daher zunächst als „lebende “ Dokumente zu verstehen, die für Anpassungen offen sind. Auch daher sollten die Dokumente zunächst als DIN SPEC umgesetzt werden. Im Anschluss können diese in die internationale Normung einfließen.

Mit dem Kick Off sollte es daher möglichst eine erste Strukturierung im Sinne einer Grundstruktur der Referenzarchitektur geben, der dieser Bericht und bestehende Dokumente bereits als Grundlage dienen können. Parallel und interdependent werden dann in weiteren Task Forces / Arbeitsausschüssen Bereichsspezifikationen angegangen. Ob und wie das zeitgleich oder zeitnah geschieht, hängt auch vom Engagement der bestehenden externen Gremien ab (z.B. zum Thema Industrie 4.0 wurde dies unmittelbar avisiert, Akteure aus dem Finanzsektor gehen zunächst von einer internen Konstituierungsphase aus). Der Zeithorizont für die Erarbeitung von Bereichs-Spezifikationen ist mit deren individueller Gründung zu bestimmen.

(Die Transformation von bestehenden Dokumenten, um sie in die Gesamtarchitektur einzupassen, ist u.U. erst nach Abschluss der Spezifikation der Grundstruktur anzugehen.)

5.1.4 Koordinierungsthema (3) – harmonisierte Sicherheitslevel

Es wurde im Bericht aufgezeigt, dass das Konzept / der Begriff „Sicherheit “ bei Digitalen Identitäten noch genauer zu definieren ist. Zum einen geht es um die Sicherheit der Daten des Identitätsgebers, zum anderen um das Interesse des Identitätsabfragers bspw. eineindeutig die Entität identifizieren zu können. Es zeigte sich, dass die verschiedenen Branchen und Anbieter von Sicheren Lösungen verschiedene Sicherheitsmerkmale benutzen und auch eine eigene Systematik und Klassifizierung der Sicherheitslevel u. ä. eingeführt haben, in Kap. 3 wurden die ISO/IEC 29115: „Entity Authentication Assurance Framework “ , ISO/IEC 15408: „Common Criteria - Evaluation Assurance “ , Security Level in der IEC 62443 , IETF - Vectors of Trust , NIST SP 800-63-3: “Digital Identity Guidelines ” und eIDAS - Level of Assurance angeführt.

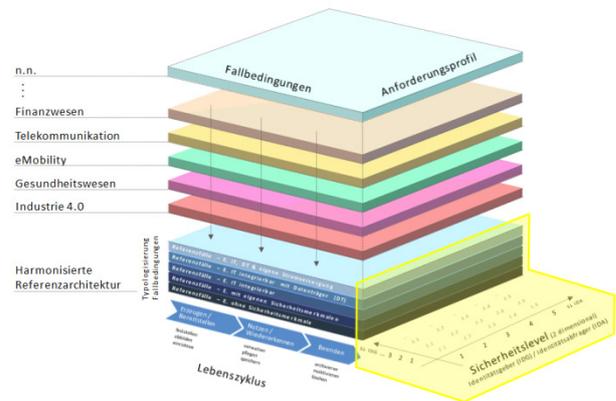


Abbildung 42 – Koordinierungsaufgabe harmonisierte Sicherheitslevel

Level

Da die vorhandenen Sicherheitslevel nicht domänenübergreifend angewendet werden und werden können, sollte erarbeitet werden, wie die bestmögliche Lösung aussehen kann, um am sinnvollsten harmonisierte Sicherheitslevel zu definieren. Dies kann auch eine Matrix sein, die bspw. das Sicherheitsbedürfnis der unterschiedlichen Stakeholder Identitätsgeber und Identitätsabfrager zusammenbringt. Ein harmonisierter Ansatz zu Sicherheitsleveln ist dabei wesentlich für die Gestaltung und Aussagekraft der Referenzarchitektur und ihrer Spezifikationen.

Um einen harmonisierten Ansatz zu erreichen, müssen die Interessensvertreter der einzelnen Branchen bereit sein ihre Anforderungen mit anderen zu diskutieren und ihr jeweiliges Lösungsmodell auf den Prüfstand zu stellen. Wenn die Anforderungen und Lösungen sowie die technischen, wirtschaftlichen und sonstigen Beweggründe diskutiert werden können, wird eine Harmonisierung möglich.

Für diese Koordinierungsaufgabe sind die betroffenen und interessierten Kreise erforderlich, die gemeinsam eine neue oder adaptierte Systematik an Sicherheitsleveln erarbeiten möchten. Hintergrund kann dazu sein, dass entweder durch die Konvergenz von Themenfeldern, auf denen unterschiedliche Lösungen existieren, oder in der Erschließung neuer Branchen, für die die bekannten Sicherheitslevel nicht (effizient) funktionieren, ein Handlungsdruck vorhanden ist.

Das zeitliche Ziel sollte sein, dass innerhalb von 6 Monaten ein Actionplan ausgearbeitet ist, der Handlungsbedarfe, Akteure und Ressourcen benennt.

5.1.5 Koordinierungsthema (4) – Schnittstellenprojekte / -mapping für kurzfristige Interoperabilität bestehender Systeme

Das Thema Digitale Identitäten bzw. dessen Teilbereiche haben Projekte, Unternehmen, Branchen vielfach bereits für sich umgesetzt, teilweise auch in seit Jahrzehnten bestehenden Infrastrukturen. Die Referenzarchitektur zielt auf eine generelle Harmonisierung der Herangehensweise ab und eine Interoperabilität auf möglichst allen Ebenen (bzw. Lebenszyklusritte) von Identitätslösungen - dies ist für die Zukunftsfähigkeit unabdingbar und sollte für alle entstehenden Systeme und Lösungen maßgebend sein. Viele jetzt angegangenen Wirtschaftsprojekte, Entwicklungen und Innovationen bedürfen aber einer unmittelbar erreichbaren Interoperabilität zu/von aktuell bestehenden Gesamtsystemen (Infrastrukturen etc.) zu Identitätslösungen. Im Hinblick auf diese bestehenden Systeme sollte das Projekt also möglichst mit Beschreibung derselben eine Sammlung der Schnittstellen organisieren. Auch Schnittstellenprojekte i.S.v. Spezifikationen werden gegebenenfalls notwendig (vgl. DIN SPEC 92222 in Entstehung). Deren Koordination und Ausrichtung auf bzw. Nutzbarkeit für eine Referenzarchitektur ist zur Effektivität und Synergienutzung zwingend geboten.

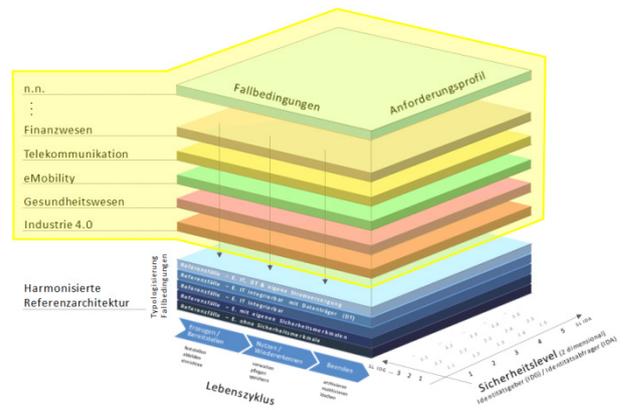


Abbildung 43 – Koordinierungsaufgabe Schnittstellenprojekte / -matrix

In diesem Sinne gilt es ein Schnittstellenmapping vorzunehmen und gegebenenfalls Grundregeln der diesbezüglichen Herangehensweise zu bestimmen o.ä. Wie ein solches Dokument genau auszusehen hat, wäre durch eine Task Force / Arbeitsausschuss noch näher zu definieren.

5.2 Umsetzungsplan - Gesamtvorhaben Sichere Digitale Identitäten

Es wurde aufgezeigt, dass es in Deutschland in verschiedenen Projekte, Unternehmen, Branchen unterschiedliche Lösungen bzw. Lösungsansätze gibt, die heute untereinander nicht oder nur teilweise kompatibel sind. Die Vielfalt der Lösungen/Lösungsansätze wurde beispielhaft in Kap. 3 illustriert. Es gibt aber mindestens zwei wesentliche Faktoren, die Motivation für Deutschland sein sollten, um zukünftig das Thema der Sicheren Digitalen Identitäten gesamthaft anzugehen:

1. Damit Sichere Digitale Identitäten zum Standard und somit Grundlage eines digitalen Ökosystems werden, welches für mehr Sicherheit für alle Beteiligten sorgt und rechtsfreie Räume verhindert, müssen Identitätslösungen im Hinblick auf die weiterschreitende Technikkonvergenz kompatibel werden bzw. bleiben. Die oben genannten Koordinierungsthemen (s. Kap. 5.1) bedürfen hierfür einer aufgabenübergreifende Gesamtkoordination.
2. Um die Position der deutschen Wirtschaft auf dem Weltmarkt langfristig zu halten, wird es erforderlich werden, dass deutsche Anforderungen und Interessen auch nachhaltig vertreten werden. Dies ist insbesondere im Bereich IT- und IT-Sicherheitstechnologie erforderlich, wo eher Länder wie USA, China oder Korea mittlerweile Weltmarktführer sind. Die Berücksichtigung deutscher Anforderungen für IT- & Software-Basislösungen ist somit auch für das Thema Sichere Digitale Identitäten essentiell. Hierfür ist es notwendig mit einer Stimme zu sprechen.

Die Umsetzung der beiden Faktoren erfordert ein Zusammenführen der Aktivitäten von Wirtschaft und Politik hinsichtlich der Anforderungen und Systemlösungen. Die Normung/Standardisierung ist hierbei ein Schlüsselinstrument, um die deutschen Interessen berücksichtigt zu wissen. Nur durch eine vereinigte Anstrengung aus den unterschiedlichen relevanten Branchen, die alle Schichten der Wirtschaft, z.B. direkt über die Verbände oder die Interessensgruppen, verbindet, wird die deutsche Position sichtbar und international relevant. Für diesen Mechanismus der Gesamtkoordination wird im folgenden ein Umsetzungsplan vorgeschlagen. Das Vorhaben hat die wesentliche Aufgabe aus pilot- und branchenspezifischen Lösungen die Themen und Aspekte herauszufiltern und aufzubereiten, dass ein standardisiertes und interoperables System entsteht.

Die Koordinierung von Standardisierung für Sichere Digitale Identitäten sollte unter Federführung von DIN und DKE durchgeführt werden. So würden im Sinne des Subsidiaritätsprinzip und in einem Legitimität schaffenden Prozesses, die konsensbasierte Normung und die bei Foren und Konsortien stattfindende Standardisierung und Spezifikationsarbeit zusammengeführt – und das über Organisations- und Branchengrenzen hinweg. Eine Grundlage der vorgeschlagenen Umsetzung des Gesamtvorhabens Sichere Digitale Identitäten basiert auf den Erfahrungen in der traditionellen Normung bei DIN und DKE. Sie beruht auf Relevanz, Freiwilligkeit, Konsensfindung, wenngleich die Ergebnisse nicht immer Dokumente sein müssen, die zu Normen, Standards und Spezifikationen führen.

Die Beteiligten am Gesamtvorhaben Sichere Digitale Identitäten verpflichten sich zur Mitarbeit Ihrer Experten in den entsprechenden Organisationen, die die Empfehlungen in Form von Normen und Standards umsetzen sollten. Die Beteiligung sollte so geregelt werden, wie es in den bestehenden Vorgaben der Beteiligung an der Normung in Komitees dargestellt ist. Hieraus ergeben sich keine kartellrechtlichen Bedenken.

Zur Umsetzung des Gesamtvorhabens Sichere Digitale Identitäten ergeben sich folgende Aufgaben:

- (a) Strategische Ausrichtung und politische Anbindung des Gesamtvorhabens SDI
- (b) Inhaltliche Gesamtsteuerung / Lenkung und Governance-Funktion
- (c) Aufbau eines >domänenübergreifenden Aktionsnetzwerkes SDI< zur koordinierten Zusammenarbeit mit bestehenden Arbeitsgruppen von Zukunftsprojekten und Branchen
- (d) Bearbeitung der Koordinierungsthemen (siehe 5.1) in Task Forces / Arbeitsausschüssen in Interaktion mit >domänenübergreifenden Aktionsnetzwerk SDI<
- (e) Vernetzung mit anderen Konsortien und Foren und Einbringen in internationalen Normung, u.a.
- (f) Kommunikation und Information nach außen zur Aufmerksamkeit und Wahrnehmung des Themas, Gewinnung weiterer Mitstreiter und Verbreitung der Resultate zur Implementierung

Hierfür müssen zudem diverse Supportaufgaben erfüllt werden, wie Regelung der personellen und Zusammenarbeit mit den bestehenden Gremien / Arbeitsgruppen, im Sinne des Aufbaus eines



Abbildung 44 – Aufgaben Umsetzung Gesamtvorhaben SDI

>domänenübergreifenden Aktionsnetzwerkes SDI<

Das Thema SDI ist ein Grundlagenthema der Digitalisierung und die Digitalisierung ist ein Querschnittsthema über die unterschiedlichsten Domänen und Branchen hinweg. Verschiedenste Akteursgruppen (Branchen, Konsortien, Zukunftsprojekte, etc.) haben im Hinblick auf die Digitalisierung Arbeitsgremien eingerichtet, die sinngemäß oder auch konkret Sichere Digitale Identitäten als Thema behandeln, mitbehandeln, behandeln wollen oder müssen - allerdings stets mit primärem Blick auf ihre Branche, Projekt, Produkt bzw. Anwendungsfall.

Zentral für das Gesamtvorhaben Sichere Digitale Identitäten ist daher, eine domänenübergreifende Einbindung dieser Gremien und Akteursgruppen zu erreichen. Nur so ist ein möglichst hoher Mehrwert im Sinne der Nutzung von Synergiepotentialen, aber auch im Sinne von Innovationspotentialen und vor allem einer zukunftsfähigen Harmonisierung und wachsenden auch domänenübergreifenden Interoperabilität herzuleiten. Besondere Relevanz kommt hierbei zu Zukunftsprojekten (vgl. Kap. 5.1) zugehörigen Gremien zu, da sie i.d.R. wesentliche Stakeholder sogar bereits domänenübergreifend zusammenbringen, z.B.:

- Industrie 4.0 → Plattform Industrie 4.0
- eMobility → Nationale Plattform Elektromobilität
- eHealth → gematik, u.a.
- Mittelstand 4.0 → Mittelstandszentren
- etc.

Das Aktionsnetzwerk soll die Basis bieten, damit sich diese Akteursgruppen zum Thema SDI austauschen, voneinander lernen können und an der Grundlagenarbeit des Vorhabens, Terminologie und Referenzarchitektur etc. sowie an interoperablen Bereichsspezifikationen mitarbeiten, diese initiieren, ggf. „anführen“, darüber informiert sind, Feedback geben, verifizieren etc. Ebenso kommt dem Netzwerk bei der späteren Anwendung und Implementierung wesentliche Bedeutung zu.

In diesem Sinne wird ein international einmaliges domänenübergreifendes Netzwerk geschaffen, welches das Gesamtvorhaben an sich und die Arbeit der Task Forces / Arbeitssausschüsse unterstützt und effektiv macht. Es ermöglicht unmittelbar und adhoc die verschiedensten Wirkungsbereiche des Themas einzubinden. Und es verleiht den Ergebnissen und somit den Interessen der deutschen Wirtschaft und Gesellschaft national, europäisch und international zusätzliches Gewicht.

Das Aktionsnetzwerk muss professionell gesteuert werden. Die Moderation / Orchestrierung des Austauschs wird im Rahmen des Gesamtvorhabens von DIN und DKE vorgenommen. Hierbei werden Feedbackverfahren mit Taskforces etc. umgesetzt, die den produktiven Austausch in, mit und zum Netzwerk sicherstellen. Gleichzeitig werden gemeinsame Themen identifiziert, aufbereitet und so koordiniert, dass sie gemeinschaftlich vertreten werden können.

5.2.1 Strategische Ausrichtung und Anbindung des Gesamtvorhabens

Zur Umsetzung der strategischen Ausrichtung und Anbindung bedarf es eines Strategiekreises.

Der Strategiekreis bestimmt die strategische Ausrichtung des Gesamtvorhabens Sichere Digitale Identitäten. Er handelt auf konsensbasierten Prinzipien und agiert auf Beschluss der beteiligten und teilnehmenden Vertreter.

Seine Aufgabe ist im Wesentlichen die Sicherstellung der Governance. Der Strategiekreis sollte sich zusammensetzen aus Vertretern der einschlägigen Verbände, der Wissenschaft, der zuständigen Ministerien sowie Behörden, dem Datenschutzbeauftragten des Bundes und Vertretern der Industrie.

Tabelle 2 - (5.2.2) Kurzübersicht: Strategische Ausrichtung und Anbindung durch einen Strategiekreis

| | |
|------------------------|---|
| Zusammensetzung | <ul style="list-style-type: none"> • Leitung StS BMWi & StS BMI • Vertreter Lenkungskreis • Vertreter Verbände • Vertreter BMBF, BMG, BMVI, BMJV, BMI (BSI), BMWi (BNetzA) • Bundesbeauftragte für Datenschutz ... • Vertreter Wissenschaft • DIN / DKE • ... |
| Aufgaben | <ul style="list-style-type: none"> • Agenda-Setting für das Gesamtvorhaben SDI, • Politische Steuerung, • Strategieentwicklung, • Identifikation strategischer Partnerschaften • Empfehlungen für die Einbeziehung weiterer Partner • Multiplikator • ... |

5.2.2 Steuerung und Lenkung des Gesamtvorhabens

Zur Steuerung und Lenkung des Gesamtvorhabens sollte ein Lenkungskreis etabliert werden.

Der Lenkungskreis sollte sich aus berufenen Experten der verschiedenen Verbände, Unternehmen und sonstigen Organisationen zusammensetzen, die Lösungen oder Projekte mit digitalen Identitäten entwickeln, bereits umgesetzt haben oder entsprechende branchenspezifische Konzepte entwickelt haben. Dieses Gremium ist auch für das Identifizieren und Initiieren von neuen branchenübergreifenden Themen verantwortlich. Für die Bearbeitung branchenübergreifender Themen werden vom Lenkungskreis die Task Forces bzw. Arbeitsausschüsse definiert und bestimmt. Der Lenkungskreis gibt den Task Forces die Zielstellung und den zeitlichen Rahmen vor.

Der Lenkungskreis handelt unter Berücksichtigung der strategischen Vorgaben des Steuerungskreises. Wenn immer erforderlich werden die DIN Prozesse und Verfahren der vorwettbewerblichen Durchführung

von Normungs- und Standardisierungsaktivitäten angewendet. Anforderungen bezüglich Transparenz, Offenheit und Konsensfindung werden erfüllt.

Tabelle 3 - (5.2.3) Kurzübersicht: Steuerung und Lenkung des Gesamtvorhabens durch einen Lenkungskreis

| | |
|-----------------|---|
| Zusammensetzung | <ul style="list-style-type: none"> • Task Force / Arbeitsausschuss - Leiter • Experten der verschiedenen Verbände, Unternehmen und sonstigen Organisationen und branchenspezifischen Arbeitsgemeinschaften wie z.B. Industrie 4.0 • DIN/DKE • ... |
| Aufgaben | <ul style="list-style-type: none"> • Technische Koordinierung, • Operative Konkretisierung der strategischen Ausrichtung, • Entscheidung und Umsetzung • Identifikation von Arbeitsgruppen übergreifenden Themen: <ul style="list-style-type: none"> ➔ Einsetzen von Task-Forces / Ar ➔ Fortschrittskontrolle der Task-Forces • Unterstützung für die Einbeziehung weiterer Partner in die Kooperationsplattform • Operative Empfehlungen bzw. Einflußnahme hinsichtlich internationaler Normung, internationaler Vernetzung und hinsichtlich PR/Kommunikation |

Governance-Funktion des Lenkungskreises:

Neben der Steuerung der Task Forces / Arbeitsausschüssen hat der Lenkungskreis eine weitere wichtige Funktion: er soll Empfehlungen hinsichtlich Normung- und Standardisierung treffen. Diese Empfehlungen gehen in Richtung der Branchen dahin, dass hinsichtlich der Berücksichtigung von Normen und Standards in den Branchenlösungen, jene Normen und Standards bevorzugt werden, die den Interessen der deutschen Stakeholder am meisten entsprechen.

So wird sichergestellt, dass gute, bestehende Lösungselemente, die von den entsprechenden Normen/Standards getragen werden, eine breitere Verwendung finden und somit die Qualität der Lösungen oder der validierten Testszenarien/Pilotanwendungen immer besser werden.

Weiterhin gibt der Lenkungskreis aus den validierten Testszenarien, geprüften Pilotanwendungen und marktreifen Lösungen in Richtung Normung und Standardisierung Vorgaben, die die Vertretung der Interessen der Deutschen Wirtschaft und Gesellschaft widerspiegelt. Das heißt die Mitarbeit in der Normung sowie in Standardisierungsgremien, wie Foren oder Konsortien, wird vom Lenkungskreis beeinflusst werden. Damit können Anforderungen der in dem Gesamtvorhaben SDI organisierten Branchen mit entsprechendem Gewicht in die nationale und internationale Normung eingebracht werden.

5.2.3 Bearbeitung der Themen in Task Forces / Arbeitsausschüssen

Task Forces / Arbeitsausschüsse sind Arbeitsgremien, die vom Lenkungskreis einberufen werden. Sie führen die Koordinierungsarbeit bzgl. der in Kapitel 5.1 genannten Themen durch.

Hierbei greifen sie entweder die Ergebnisse der diversen bereits vorhandenen Insellösungen unterschiedlicher Branchen und Arbeitsgemeinschaften auf und leiten daraus branchenübergreifende und interoperable Lösungen ab oder konsolidieren sich zu neuen Themen.

Task Forces / Arbeitsausschüsse sind verantwortlich für das Erarbeiten und Abstimmen gemeinsamer Positionen sowie für die Erstellung von Szenarien, Empfehlungen, Leitfäden und Spezifikationen. Diese so erstellten Ergebnisse bilden den inhaltlichen Kern der Roadmap „Sichere Digitale Identitäten“.

Task Forces werden durch den Lenkungskreis gegründet und bekommen für die Erarbeitung eines Ziels / definierten Ergebnisses ein Zeitbudget. Dieses sollte bei vielen Themen nicht länger als 6-12 Monate dauern. Sicherlich wird es Themen geben, die in diesem Zeitraum ein erstes Ergebnis erstellen, die aber dann einer ständigen Überarbeitung bzw. Überprüfung bedürfen, um auf technologische Entwicklungen schnell reagieren zu können und Rückflüsse aufgrund des Einbringens der Themen in europäische und internationale Normungs- und Standardisierungsgremien aufgreifen zu können.

Neben den zeitbegrenzten Task Forces bedarf es zumindest eines dauerhaften Ausschusses Entwicklung der **Roadmap Sichere Digitale Identitäten**. Ggf. kann dieser derjenige sein, der das Koordinierungsthema Grundstruktur Referenzarchitektur behandelt. Die Roadmap ist für die Definition und das regelmäßige Update der Roadmap Sichere Digitale Identitäten verantwortlich. Die Roadmap beschreibt die zukünftigen Handlungsfelder, greift damit Prioritäten der einzelnen Task Forces auf und beschreibt die Maßnahmen, die hinsichtlich Normung und Standardisierung ergriffen werden soll. Innerhalb dieses dauerhaften Ausschusses werden die Spezifikationen identifiziert, die dann z.B. auf der Basis des DIN SPEC (PAS)-Verfahrens zur konkreten Bereicherung und Beeinflussung der deutschen, europäischen und internationalen Normung sowie als Input für Foren und Konsortien dienen. Die Roadmap ist ein „lebendes“ Dokument, welches regelmäßig veröffentlicht wird⁶⁴.

Die Task Forces / Arbeitsausschüsse sollten im Rahmen der Statuten der Satzung von DIN und DKE handeln. Insbesondere werden die DIN Verfahren der vorwettbewerblichen Durchführung von Standardisierungsaktivitäten verwendet, womit die Anforderungen der Kriterien bezüglich Transparenz, Offenheit und Konsensfindung erfüllt werden. Wenn möglich und sinnvoll werden die Ergebnisse in einer DIN SPEC dokumentiert.

Tabelle 4 - (5.2.4) Kurzübersicht: Task Forces und Arbeitsausschüsse

| | |
|------------------------|---|
| Zusammensetzung | <ul style="list-style-type: none"> • unterschiedlich, durch den Lenkungskreis eingesetzte Expertengruppe • DIN / DKE • ... |
|------------------------|---|

⁶⁴ Gegenwärtig besteht die Absicht die Roadmap jeweils nach Abschluss einer Task Force zu revidieren, um deren Arbeitsergebnisse so aktuell wie möglich zu visualisieren.

| | |
|-----------------|---|
| Aufgaben | <ul style="list-style-type: none"> • Branchenübergreifende Diskussion gemeinsamer Themen für Wissensaustausch, Know-how Transfer und um Synergien zu finden. • Schaffung von branchenübergreifenden Harmonisierungsansätzen • Branchenübergreifende Bearbeitung der Themen mit dem Ziel Leitfäden, DIN SPEC, etc. zu gestalten • TaskForces konsultieren die AGs und greifen deren bereits vorhandenen Ergebnisse auf • Hieraus resultierende Normungsvorhaben werden in die internationale Normung eingebracht – möglichst über bestehende NAs • Rückspielen der Aktivitäten in die AGs • ... |
|-----------------|---|

Task Force Themen:

Die in Kap. 5.1. „Inhaltliche Koordinierungsaktivitäten “ genannten Themen sind für das Gesamtvorhaben SDI die Initial-Themen.

5.2.4 Bereitstellung der personellen und sonstigen Ressourcen (Geschäftsführung / hauptamtliche Unterstützung)

Es bedarf einer Geschäftsstelle, die das Gesamtvorhaben SDI unterstützt.

Betrieben von DIN und DKE handelt sie im Rahmen der Statuten und der Satzung, nach der insbesondere die DIN-/DKE- Prozesse & Verfahren der vorwettbewerblichen Durchführung von Standardisierungsaktivitäten verwendet werden. Hierdurch werden die Anforderungen der Kriterien bezüglich Transparenz, Offenheit und Konsensfindung erfüllt. Die Geschäftsordnung sollte es erlauben, dass die Geschäftsstelle für bestimmte Aufgaben Tätigkeiten ausschreiben und Dritte beauftragen darf.

Zu den Hauptaufgaben der Geschäftsstelle gehören:

- Dokumentation und Koordinierung des Aufbaus des domänenübergreifenden Aktionsnetzwerkes SDI / Einbindung weiterer Branchen und die Gewinnung von Experten zur Mitarbeit
- Organisation und Koordination des Strategiekreises, Lenkungskreises und der Task Forces / Arbeitsausschüsse, einschließlich des Projektmanagements (z.B. Führen der Fortschrittskontrolle)
- Organisation und Anregung zu branchen- und gremienübergreifenden Austausch und Zusammenarbeit
- Koordination von Normung und Standardisierung, d.h. auch Koordination mit relevanten Foren und Konsortien
- Kommunikation und Veröffentlichung der Ergebnisse sowie PR und Öffentlichkeitsarbeit

- Erzeugung der Sichtbarkeit des Themas SDI auf nationaler, europäischer und internationaler Ebene
- Planen und Durchführen von Veranstaltung wie einer Jahreskonferenz und Workshops

Tabelle 5 - (5.2.5) Kurzübersicht: Bereitstellung der personellen und sonstigen Ressourcen (Geschäftsführung / hauptamtliche Unterstützung)

| | |
|------------------------|--|
| Zusammensetzung | <ul style="list-style-type: none"> • DIN / DKE |
| Aufgaben | <ul style="list-style-type: none"> • Netzwerkaufbau und -koordination • Organisation • Projektmanagement • interne und externe Kommunikation • Interessenvermittlung • Operativer Impulsgeber • ... |

Kommunikations-Funktion der Geschäftsstelle

Die externe Kommunikation gehört zu den Kernaufgaben der Geschäftsstelle. Dazu wird ein entsprechender Internetauftritt vorgesehen. Über diese Internetpräsenz wird die Geschäftsstelle das Gesamtvorhaben Sichere Digitale Identitäten maßgeblich nach außen kommunizieren und interessierten Personen auch die Möglichkeit der Kontaktaufnahme mit der Geschäftsstelle bieten. Da die kontinuierliche Informationsbereitstellung und eine gute Beobachtung der Informationslage gewährleistet sein müssen, sollte das Projekt eine eigene Ressource zur Sicherstellung der Kommunikation vorsehen.

Aufgaben in der externen Kommunikation sind

- Mediengerechte Aufbereitung des Themas (auch für Nicht-IT Experten und Laien)
- Bereitstellung von Informationsmaterial (für Experten)
- Vermittlung von Sprechern
- Aufarbeitung und Darstellung von Ergebnis-/Positionspapieren
- Unterstützung in der Vorbereitung und Durchführung der Jahreskongress
- Ansprechpartner für die AGs zu allen Kommunikationsfragen
- Vorbereitung für die Verbandskommunikation
- politische Kommunikation
- internationale Kommunikation
- Entwurf und Pflege eines Logo (CD/CI)
- etc.

5.2.5 Schirmherrschaft

Aufgrund der Bedeutung für Wirtschaft, Gesellschaft und Politik ist eine starke Unterstützung durch die Bundesregierung unbedingt geboten. Es empfiehlt sich eine Schirmherrschaft auf ministerieller Ebene. Hierbei tangiert das Thema zwar die Arbeitsbereiche einiger Ministerien, doch ohne zum jetzigen Zeitpunkt eine mögliche Neuaufstellung der Ministerien berücksichtigen zu können, lässt sich festhalten, dass dem Thema insbesondere aus wirtschaftspolitischer und innenpolitischer Sicht höchste Bedeutung beizumessen ist. Es wäre daher an dieser Stelle ein Schulterschluss zwischen dem Bundesministerium für Wirtschaft und Energie (BMWi) und dem Bundesministerium des Innern (BMI) zu überlegen. Die Bundesminister würden hierbei in Person als Schirmherren der Initiative stehen.

Eine Doppelschirmherrschaft würde dem Thema zudem die Aufmerksamkeit und Bedeutung verschaffen, die Grundlagenthemen der Digitalisierung jetzt bedürfen und somit den gemeinsamen politischen Willen zeigen. Beinhalten sollte diese möglichst die Eröffnung der KickOff-Veranstaltung und Jahreskonferenzen, Begleitung der Kommunikationsmaßnahmen.

Tabelle 6 - (5.2.6) Kurzüberblick: Schirmherrschaft

| | |
|------------------------|---|
| Zusammensetzung | <ul style="list-style-type: none"> • Bundesminister/in für Wirtschaft und Energie • Bundesminister/in des Inneren • ggf. dann zuständiges Ministerium |
| Aufgaben | <ul style="list-style-type: none"> • Generierung der Sichtbarkeit • Darstellung des politischen Willens • Politische Flankierung • Motivierung wichtiger Stakeholder zur aktiven Unterstützung • ... |

5.2.6 Jahreskongress

Ein weiteres zentrales Element des Gesamtvorhabens SDI wäre eine wiederkehrende öffentlichkeitswirksame Veranstaltung, welche gleichzeitig der Umsetzung unterschiedlicher Aufgaben des Gesamtvorhabens dient.

Ein Jahreskongress kann Ergebnisse und zum Teil auch Zwischenergebnisse vor allem aus der Arbeit der Task Forces / Arbeitsausschüsse der interessierten Öffentlichkeit vorstellen. Die Struktur der Jahreskongresse sollte erkennen lassen, dass hier nicht einseitig von und über das Gesamtvorhaben informiert wird, sondern die Möglichkeit des Dialogs geboten wird. Daher sollen Vertreter von Branchenarbeitsgruppen sowie von Verbänden auch ihre bisherigen „Insellösungen“ und damit ihre Sichtweise und Bedarfe in Sachen Sichere Digitale Identitäten vorstellen können. Auf diese Weise sollen diese dann in die weitere Arbeit der Plattform integriert werden können. Ferner soll so auch das Themen- und Arbeitsspektrum der Plattform aktualisiert werden.

Des Weiteren kann der Kongress der übergeordneten Strategieweichtung und Anbindung dienen und insbesondere der internationalen Verknüpfung.

Tabelle 7 - (5.2.7) Kurzübersicht: Jahreskongress

| | |
|------------------------|---|
| Zusammensetzung | <ul style="list-style-type: none"> • Sämtliche genannten Akteure • zudem Vertreter internationaler Initiativen und Gremien • interessiertes Fachpublikum • ... |
| Aufgaben | <ul style="list-style-type: none"> • Vorstellung von Ergebnissen (Zwischenbericht) • Erzeugung der Sichtbarkeit auf nationaler und internationaler Ebene • jährliche Strategieausrichtung • Austausch mit / Bericht von Vertretern von Akteursgruppen von Zukunftsprojekten, Verbänden, etc. • ... |

6 Anhang

Der Anhang befindet sich aufgrund der Größe der Dokumente in einer separaten Datei. Diese Datei wurde parallel als PDF per Mail an das BMWi übersandt.

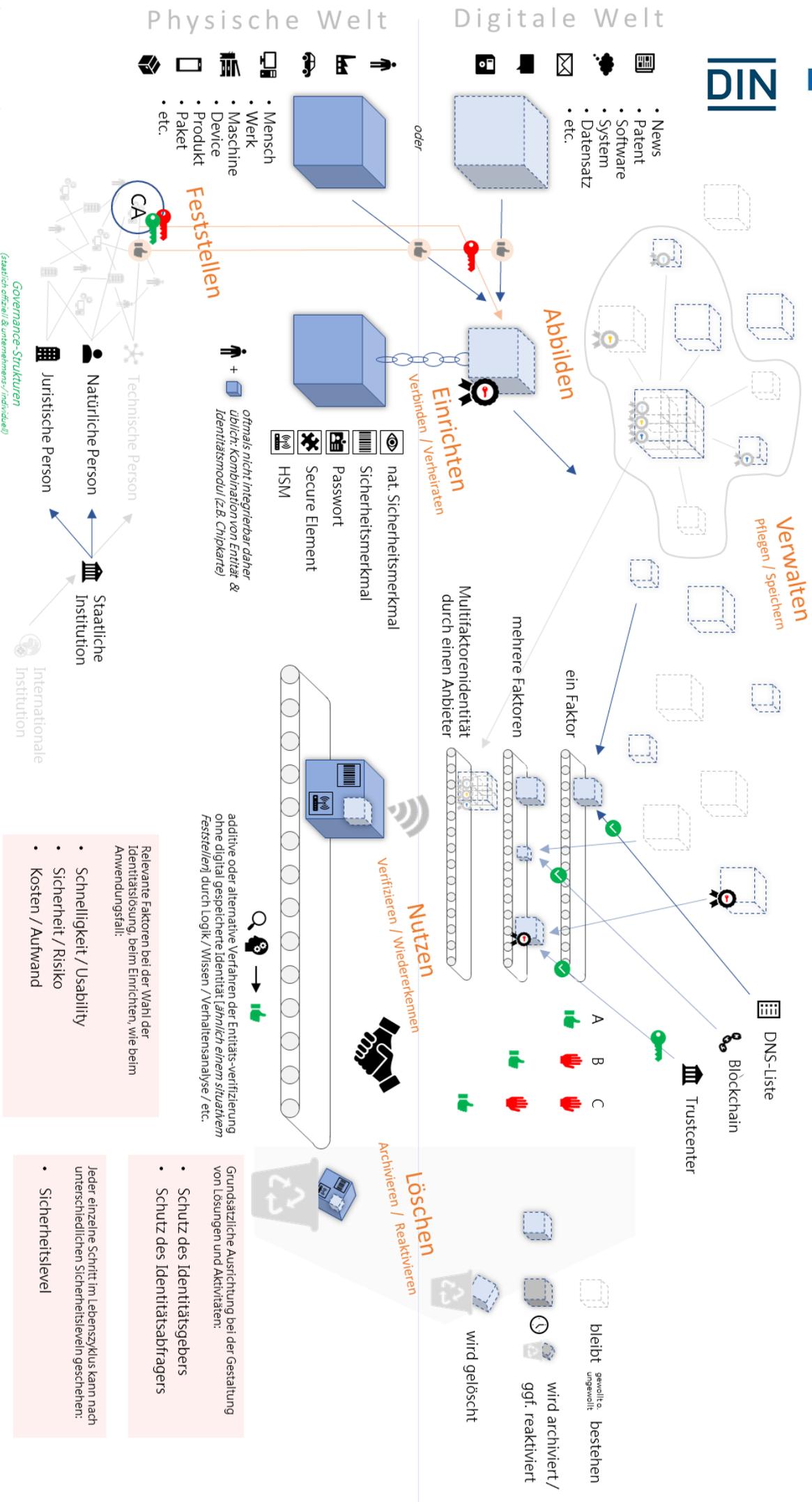
In diesem Dokument befinden sich die Anhänge:

- Anhang 6.1 Schaubild zum Gesamtsachverhalt SDI
- Anhang 6.2 Gesamtverzeichnis Kontaktpersonen / Key-Player

In einer separaten PDF-Datei befinden sich die Anhänge:

- Anhang 6.3 Kapitel 2.1.1 - Bericht 1. Beiratssitzung 2017-03-02 mit ausgewählten Präsentationen
- Anhang 6.4 Kapitel 2.1.3 - Anschreiben (Mail), Begleitschreiben und Adressaten für Fragebogen
- Anhang 6.5 Kapitel 2.1.3 - Fragebogen
- Anhang 6.6 Kapitel 2.1.5 - internes Ergebnispapier Themen-Workshop - 22. Juli 2017
- Anhang 6.7 Kapitel 2.1.6 - Einladungsschreiben (Mail) und Agenda für Stakeholder-Workshop
- Anhang 6.8 Kapitel 2.1.6 - Präsentation Stakeholder-Workshop – Begrüßung und Allgemein / Normenrecherche / Rechtsrecherche
- Anhang 6.9 Kapitel 2.1.6 - Zwischenbericht - Zusammenfassung der Diskussion der Zwischenergebnisse
- Anhang 6.10 Kapitel 2.3.2 – Normungsrecherche relevante Gremienarbeit /Normen
- Anhang 6.11 ohne Kapitel - Themenwebsite auf www.din.de
- Anhang 6.12 ohne Kapitel - Themenwebsite auf www.dke.de

6.1 Schaubild zum Gesamtsachverhalt SDI (zu Kapitel 3.4)



6.2 Gesamtverzeichnis Kontaktpersonen

| Bereich | Anrede | Titel | Vorname | Name | Organisation |
|-------------|--------|-----------|---------|------|--------------|
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Forschung | Herr | | | | |
| Unternehmen | Herr | | | | |
| Umsetzung | Herr | | | | |
| Unternehmen | Herr | | | | |
| Verbände | Herr | | | | |
| Behörden | Herr | | | | |
| Verein | Frau | | | | |
| Behörden | Herr | Dr. | | | |
| Unternehmen | Herr | Prof. Dr. | | | |
| Plattformen | Herr | Dr.-Ing. | | | |
| Unternehmen | Frau | | | | |
| Verbände | Herr | Prof. Dr. | | | |
| Verbände | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Forschung | Frau | Prof. Dr. | | | |
| Umsetzung | Frau | | | | |
| Unternehmen | Herr | | | | |
| Ministerien | Herr | | | | |
| Verbände | Frau | | | | |
| Forschung | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Forschung | Frau | | | | |
| Unternehmen | Herr | | | | |
| Verbände | Herr | | | | |
| Forschung | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Unternehmen | Herr | Dr. | | | |
| Unternehmen | Herr | | | | |
| Verbände | Frau | Dr. | | | |
| Behörden | Herr | | | | |
| Behörden | Herr | | | | |
| Unternehmen | Herr | | | | |
| Umsetzung | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Verbände | Herr | Dr. | | | |
| Unternehmen | Frau | | | | |
| Unternehmen | Frau | | | | |
| Unternehmen | Herr | | | | |
| Verbände | Herr | | | | |
| Unternehmen | Herr | | | | |

Personenbezogene Daten aus Gründen des Datenschutzes hier nicht sichtbar

| Bereich | Anrede | Titel | Vorname | Name | Organisation |
|-------------|--------|-----------|---------|------|--------------|
| Umsetzung | Herr | | | | |
| Umsetzung | Herr | | | | |
| Forschung | Herr | | | | |
| Umsetzung | Herr | | | | |
| Unternehmen | Frau | | | | |
| Unternehmen | Herr | Dr. | | | |
| Unternehmen | Herr | Dr. | | | |
| Ministerien | Frau | | | | |
| Umsetzung | Herr | | | | |
| Forschung | Herr | Prof. Dr. | | | |
| Unternehmen | Herr | Dr. | | | |
| Plattformen | Herr | | | | |
| Ministerien | Herr | | | | |
| Umsetzung | Herr | Dr. | | | |
| Unternehmen | Herr | Dr. | | | |
| Verbände | Herr | | | | |
| Umsetzung | Herr | | | | |
| Unternehmen | Herr | | | | |
| Verbände | Herr | | | | |
| Behörden | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Forschung | Frau | | | | |
| Unternehmen | Frau | | | | |
| Unternehmen | Herr | | | | |
| Verbände | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Verbände | Herr | | | | |
| Verbände | Herr | | | | |
| Unternehmen | Herr | | | | |
| Forschung | Herr | Prof. Dr. | | | |
| Unternehmen | Herr | | | | |
| Ministerien | Herr | Dr. | | | |
| Forschung | Herr | | | | |
| Unternehmen | Herr | | | | |
| Verbände | Herr | Dr. | | | |
| Umsetzung | Herr | | | | |
| Verbände | Herr | | | | |
| Verbände | Herr | | | | |
| Unternehmen | Herr | | | | |
| Forschung | Herr | Prof. Dr. | | | |
| Unternehmen | Herr | Dr. | | | |
| Forschung | Frau | Dr. | | | |
| Ministerien | Herr | | | | |
| Forschung | Herr | Prof. Dr. | | | |
| Verbund | Herr | | | | |
| Forschung | Herr | Dr. | | | |
| Forschung | Herr | Prof. Dr. | | | |
| Unternehmen | Herr | | | | |

Personenbezogene Daten aus Gründen des Datenschutzes hier nicht sichtbar

| Bereich | Anrede | Titel | Vorname | Name | Organisation |
|-------------|--------|-------|---------|------|--------------|
| Umsetzung | Herr | | | | |
| Ministerien | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | | | | |
| Unternehmen | Herr | Dr. | | | |
| Verbände | Herr | | | | |
| Unternehmen | Herr | | | | |
| Umsetzung | Herr | | | | |
| Umsetzung | Herr | Dr. | | | |
| Unternehmen | Herr | | | | |
| Verbände | Herr | | | | |
| Unternehmen | Herr | | | | |
| Forschung | Herr | Dr. | | | |
| Unternehmen | Herr | | | | |
| Umsetzung | Herr | | | | |
| Unternehmen | Herr | | | | |

Personenbezogene Daten aus Gründen des Datenschutzes hier nicht sichtbar

Tabellenverzeichnis

| | |
|--|-----|
| Tabelle 1 - Gegenüberstellung Arbeitspakete und Resultate/Aktivitäten gemäß Projektantrag | 24 |
| Tabelle 2 - (5.2.2) Kurzübersicht: Strategische Ausrichtung und Anbindung durch einen Strategiekreis | 156 |
| Tabelle 3 - (5.2.3) Kurzübersicht: Steuerung und Lenkung des Gesamtvorhabens durch einen Lenkungskreis | 157 |
| Tabelle 4 - (5.2.4) Kurzübersicht: Task Forces und Arbeitsausschüsse | 158 |
| Tabelle 5 - (5.2.5) Kurzübersicht: Bereitstellung der personellen und sonstigen Ressourcen (Geschäftsführung / hauptamtliche Unterstützung)..... | 160 |
| Tabelle 6 - (5.2.6) Kurzüberblick: Schirmherrschaft | 161 |
| Tabelle 7 - (5.2.7) Kurzübersicht: Jahreskongress..... | 162 |

Abbildungsverzeichnis

| | |
|--|----|
| Abbildung 1 – beispielhafte domänenübergreifende Referenzarchitektur SDI..... | 13 |
| Abbildung 2 – Vernetzung bestehender Gremien zur Entwicklung einer Referenzarchitektur SDI..... | 14 |
| Abbildung 3 – Aufteilung der Verantwortungsbereiche in der Normung..... | 23 |
| Abbildung 4 – Entscheidungsdiagramm für die Normenrecherche (Quelle: DKE)..... | 44 |
| Abbildung 5 – Übersicht der betrachteten Organisationen..... | 45 |
| Abbildung 6 – Publikationsarten (Quelle: IEC Guide 120)..... | 48 |
| Abbildung 7 – Digitale Signaturgenerierung und Validierung (Quelle: ITU-T X.509)..... | 51 |
| Abbildung 8 – Beziehungen zwischen Entitäten, Identitäten und Attributen (Quelle: ITU-T X.1252)..... | 52 |
| Abbildung 9 – Lebenszyklus des Evaluationsgegenstands (Quelle: DIN EN 419211-1:2014-12)..... | 54 |
| Abbildung 10 – zwei Parteien identitäts-Föderation (Quelle: ISO/IEC 24760-3:2016(E))..... | 55 |
| Abbildung 11 – komplexe Identitätsföderation (Quelle: ISO/IEC 24760-3:2016(E))..... | 55 |
| Abbildung 12 – Gateway-Gemeinschaftsmodell (Quelle: ISO/IEC 24760-3:2016(E))..... | 56 |
| Abbildung 13 – Aufbau der Normenreihe IEC 62443 (Quelle: E DIN IEC 62443-3-3 (VDE 0802-3-3))..... | 58 |
| Abbildung 14 – Beispiel aus der verfahrenstechnischen Industrie mit Zonen und Conduits..... | 60 |
| Abbildung 15 – Beispiel aus der Fertigungsindustrie mit Zonen und Conduits..... | 61 |
| Abbildung 16 – Identitätsgeber und -abfrager..... | 78 |
| Abbildung 17 – Lebenszyklus von digitalen Identitäten..... | 80 |
| Abbildung 18 – SDI im abgeschlossenen Verantwortungsbereich..... | 81 |
| Abbildung 19 – Anforderungen an ein zu integrierendes Produkt..... | 82 |
| Abbildung 20 – Interaktion von Domänen..... | 82 |
| Abbildung 21 – Lebenszyklus der Digitalen Identität eines Postpaketes (einfache Grundstruktur)..... | 88 |
| Abbildung 22 – Entitäten..... | 89 |
| Abbildung 23 – Feststellen einer Identität..... | 90 |
| Abbildung 24 – Abbilden einer Identität..... | 91 |

| | |
|---|-----|
| Abbildung 25 – Einrichten einer Identität | 92 |
| Abbildung 26 – Verwalten einer Identität | 100 |
| Abbildung 27 – Nutzen / Einsatz der Identitätslösung | 101 |
| Abbildung 28 – Ende des Lebenszyklus von Identitäten..... | 104 |
| Abbildung 29 – Gesamtsachverhalt SDI mit seinen Handlungsschritten/ebenen (große Version s. Anhang 6.1) | 105 |
| Abbildung 30 – SDI machen es möglich, mit dem Smartphone Produkte auf Echtheit prüfen..... | 106 |
| Abbildung 31 – Sicherheit ist nicht auf Dauer – Standards können den Umgang mit neu entdeckten Sicherheitslücken regeln und so bspw. im Rahmen von Sicherheitsleveln Updateverweigerungen einen Riegel vorschieben..... | 107 |
| Abbildung 32 – Fake or Real? - Um diese Frage entscheiden zu können, gibt es bessere Lösungen als ein eingefügtes Logo oder Quellenbezug der vermeintlichen Quelle. | 108 |
| Abbildung 33 – Viele Informationen über eine Entität zu besitzen, kann das Identifizieren einfacher und sicherer machen. Es ist aber nicht notwendig..... | 109 |
| Abbildung 34 – Industrie 4.0 und die digitalen Zukunftsprojekte bedürfen Identitätslösungen vom Datensatz bis hin zur Werksanlage, vom Mensch bis zur Maschine | 111 |
| Abbildung 35 – Knoten- und Zusatzpunkt mit hochsicheren Identitäten können zur Steigerung der Sicherheit damit verbundener Entitäten dienen..... | 113 |
| Abbildung 36 – domänenübergreifende Referenz-architektur SDI (Beispiel) – Details vgl. Kapitel 5 | 128 |
| Abbildung 37 – Schaubild Gesamtsachverhalt SDI (s. Anhang 6.1)..... | 130 |
| Abbildung 38 – domänenübergreifende Betrachtung von Identitäts-lösungen (Redundanzen, Synergie- und Innovationspotentiale) | 144 |
| Abbildung 39 – exemplarische Auflistung von Stakeholdern mit bestehenden oder zu aktivierenden Gremien oder ansprechbaren Stellen, die im Sinne eines Aktionsnetzwerkes zum Thema eingebunden werden sollen | 145 |
| Abbildung 40 – kooperative Entwicklung einer Referenzarchitektur durch neutralen Akteur | 146 |
| Abbildung 41 – Koordinierungsaufgabe Grundstruktur Referenzarchitektur | 148 |
| Abbildung 42 – Koordinierungsaufgabe harmonisierte Sicherheitslevel | 151 |
| Abbildung 43 – Koordinierungsaufgabe Schnittstellenprojekte / -matrix | 152 |
| Abbildung 44 – Aufgaben Umsetzung Gesamtvorhaben SDI | 154 |

Literaturverzeichnis

Buchmann, E. (kein Datum). Datenschutz und Privatheit in vernetzten Informationssystemen IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe "Privacy Awareness in Information Systems" KIT. Universität des Landes Baden-Württemberg und nationales Forschungszentrum in der Helmholtz-Gemeinschaft, (S. Kapitel 2: Digitale Identitäten).

Bundesministerium für Wirtschaft und Energie. (2017). Abgerufen am 5. April 2017 von BMWI "IT-Sicherheit": <https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/it-sicherheit.html>

Collignon, D. R. (März 2009). Die sichere digitale Identität, Definition, Herausforderungen und technologische Entwicklungen in Deutschland. Science Allemagne [Das Informationsblatt der Abteilung für Wissenschaft und Technologie der französischen Botschaft in der Bundesrepublik].

Dehning, O. (27. 9 2017). IT Rebellen. Abgerufen am 2017 von <http://it-rebellen.de/2017/02/02/digitale-identitaeten-verhindern-kennwort-klau/>

Deloitte. (2016). Picture Perfect: A blueprint for digital Identity. New York.

Delvaux, M. (2016). Draft Report with recommendations to the Commission on Civil law Rules on Robotics. European Parliament Committee on Legal Affairs, (S. Initiative-Rule 46 of the rules of procedure).

et.al, F. I. (März 2017). Sicheres Identitätsmanagement im Internet -Eine Analyse des ISAEN Konzepts (Individual personal data auditable address). Begleitforschung Smart Data im Auftrag des Bundesministeriums für Wirtschaft und Energie.

Ferdous, S. e. (Mai 2015). Managing dynamic identity Federations using Security Assertion Markup Language (SAML). Journal of Theoretical and Applied Electronic Commerce Research.

Fromm, J. e. (2013). Vertrauenswürdige digitale Identität: Baustein für öffentliche IT.

Fuchs, A. e. (April 2017). Positionspapier| Task Force: "GERÄTEIDENTITÄT UND -INTEGRITÄT IM INTERNET DER DINGE". Fraunhofer Positionspapier.

Heiles, J. (2017). IoT Week 2017 - Workshop on "Globally Interoperable IoT Identification and Data Processing" Identifiers in IoT. AIOTI -Alliance for Internet of things Innovation, S. IOT Week 2017.

Hoye, N. (2010). Digitale Identitäten im Kontext von E-Government-Anwendungen: Ausführungen zu einer sicheren Kommunikation zwischen Bürgern und Verwaltung. Hamburg: Diplomica.

Inigo Barreira, I. e. (2016). Analysis of standards related to Trust Service Providers Mapping of Requirements of eIDAS to existing standards. European Union Agency for network and Information Security Mapping of requirements of eIDAS to existing standards, (S. Version 1.1).

Jänicke, D. e. (April 2016). Technischer Überblick: Sichere Identitäten. Ergebnispapier der Plattform Industrie 4.0.

Kunze, C. P. (2003). Digitale Identität und Identitätsmanagement. Hamburg.

Leichsenring, D. H. (24. Oktober 2016). Der Bank Blog. Abgerufen am 2017 von Der Bank Blog: <https://www.der-bank-blog.de/digitale-identitaet-finanzdienstleistung/studien/digitalisierung-finanzdienstleistung/23559/>

Letzkus, F. (April 2016). Sichere Identitäten entscheidend. Computerwoche.

Marquardt, M. (2013). 7 Laws of Identity by Kim Cameron. Technische Universität Dresden. Dresden: Fakultät Informatik, Institut für Systemarchitektur, Professur Datenschutz und Datensicherheit.

McWaters, R. J. (2016). A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity. An Industry Project of the Financial Services Community | Prepared in collaboration with Deloitte.

Meier, A. (27. 9 2017). Goethe Institut. Abgerufen am 2017 von „Ich dokumentiere, also bin ich“: <https://www.goethe.de/de/kul/med/20640599.html>

Otto, P.-I. B. (2016). Industrial data space -digitale Souveränität über Daten-. Fraunhofer White Paper.

Rheinland, T. (kein Datum). Identity und Access Management (IAM): Professionelle Verwaltung von Identitäten und Berechtigungen für mehr IT-Sicherheit. TÜV Rheinland.

RSA. (2015). INFORMATIONSBASIERTES IDENTITÄTS- UND ZUGRIFFSMANAGEMENT. RSA White Paper.

Schallaböck, J. (2014). Verbraucher-Tracking;. iRights.Law -Anwälte für die digitale Welt-.

Schmitz, P. e. (Mai 2017). Identity Protection: Schutz für digitale Identitäten "Identity-Trends und die Folgen für die Sicherheit, Schutz durch und Schutz für biometrische Daten, Neue Ansätze zum Schutz für digitale Identitäten". Security Insider.

Schnajkin, D. M. (März 2017). endlich cloudsicher. Bdrive. CeBIT Folienvortrag der Bundesdruckerei.

Seibertmedia. (27. Oktober 2010). Youtube. Abgerufen am 2017 von Youtube: <https://www.youtube.com/watch?v=oj4Vjn8NXiY>

Seifert, I. e. (2016). Sichere Softwarearchitekturen für Industrie 4.0. Begleitforschung AUTONOMIK für Industrie 4.0 VDI/VDE Innovation+Technik GmbH, S. Leitfaden Band 5.

Tietz, C. e. (2017). Management digitaler Identitäten -Aktueller Status und zukünftige Trends-. Technische Berichte des Hasso-Plattner-Instituts für Softwaretechnik an der Universität Potsdam, S. Bericht Nr.114.

Vosseler, M. (23. August 2016). Digital Finance Experts. Abgerufen am 2017 von Digital Finance Experts: <http://digital-finance-experts.blogspot.de/2016/08/digital-identity-teil-1-ein-thema-fur.html>

Wladawsky-Berger, I. (September 2016). Digital Identity: The Key to Privacy and Security in the Digital World. MIT Initiative on the Digital Economy.

DIN e.V.

Am DIN-Platz, Burggrafenstraße 6
10787 Berlin
Telefon: +49 30 2601-0
Internet: www.din.de

DKE

Deutsche Kommission Elektrotechnik
Elektronik Informationstechnik
in DIN und VDE

Stresemannallee 15
60596 Frankfurt
Telefon: +49 69 6308-0
Internet: www.dke.de

Gefördert durch:



Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages