



## Identitätsmanagement

---

Fachgruppen „Wirtschaftliche Potenziale und gesellschaftliche Akzeptanz“ und „Sicherheit“

# Impressum

## Herausgeber

Begleitforschung Smart Data  
www.smart-data-programm.de  
c/o FZI Forschungszentrum Informatik  
Außenstelle Berlin  
Friedrichstr. 60, 10117 Berlin

## Redaktion und Konzeption

Fachgruppen „Wirtschaftliche Potenziale und gesellschaftliche Akzeptanz“ und „Sicherheit“ der Smart-Data-Begleitforschung

## Schlussredaktion und Gestaltung

LoeschHundLiepold Kommunikation GmbH

## Stand

September 2018

## Bildnachweis

FZI Forschungszentrum Informatik, psdesign1/Fotolia (Titel),  
Karlsruher Institut für Technologie (Portrait Christof  
Weinhardt), Thomas Schünemann (Portrait Jan Sürmeli)

Gefördert durch:



Bundesministerium  
für Wirtschaft  
und Energie

aufgrund eines Beschlusses  
des Deutschen Bundestages

# Inhalt

Vorwort.....	4
Sicheres Identitätsmanagement – Sichere Prozesse.....	6
Die wichtigsten Prozessschritte .....	8
Evolution des Identitätsmanagements.....	11
Betrachtung aktueller Konzepte .....	13
Identitätsmanagement in einer smarten Datenwirtschaft .....	18
Ausblick – Identitätsmanagement zentral denken .....	22
Über die Autoren .....	23
Fußnoten .....	26



## Vorwort



Sehr geehrte Leserinnen und Leser,

Identitätsmanagement ist eines der wichtigsten Themen, wenn wir uns im Internet bewegen und für Unternehmen von hoher Bedeutung, um eigene Systemlandschaften vor dem unbefugten Zugriff durch Dritte zu schützen – Unternehmen kollaborieren in einer voranschreitenden Globalisierung so stark wie nie zuvor. Der Austausch sensibler, schützenswerter, zum großen Teil personenbezogener Daten steigt an, ihr Gewinn, ihre intelligente Vernetzung oder ihr Verlust entscheiden über Wettbewerbsvorteile und Marktstellungen. Gleichzeitig wächst durch diesen Datenaustausch der Anspruch an die IT-Sicherheit. Ein gutes Identitätsmanagement stellt hohe Ansprüche an sichere Softwarelösungen, muss den Faktor Mensch mitsamt seinen Stärken und Schwächen in seiner Funktionsweise berücksichtigen und kann so die Freilegung wirtschaftlicher Potenziale unterstützen.

Erstmals – und im Hinblick auf das nahende Ende der Smart-Data-Begleitforschung – haben sich die Fachgruppen „Wirtschaftliche Potenziale und gesellschaftliche Akzeptanz“ sowie die Fachgruppe „Sicherheit“ gemeinsam einem Thema gewidmet, an dem sich beeindruckend viele fachliche Schnittmengen ergeben. Diese Schnittmengen, technische Hintergründe und die wirtschaftlichen Implikationen eines guten Identitätsmanagements möchten wir Ihnen in dieser Publikation veranschaulichen.

Wir beobachten in den letzten Jahren eine Entwicklung weg von Insellösungen, hin zu standardisierten Frameworks. Neben den grundlegenden Funktionen wie Benutzermanagement und Authentifikation bieten sie auch Möglichkeiten zur Föderation von Diensten und Single Sign-on. Damit erhöhen moderne Lösungen nicht nur den Benutzerkomfort, sondern auch die Sicherheit in großen Anwendungskontexten.

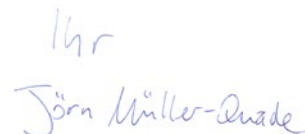
Mit der letzten Publikation der Fachgruppe „Wirtschaftliche Potenziale und gesellschaftliche Akzeptanz“ der Smart-Data-Begleitforschung Corporate Digital Responsibility haben wir an die unternehmerische Verantwortung in der Digitalisierung appelliert. Das Identitätsmanagement begreifen wir als eine Methode, sich einer Corporate Digital Responsibility anzunähern. Wann immer Datenaustausch inter- oder intrabetrieblich stattfindet, wird für Mensch und Maschine Zugang zum wertvollen Rohstoff Daten gewährt. Zur Verantwortung von Unternehmen zählt es daher, diesen Zugang zuverlässig, sicher und so einfach wie möglich zu halten.

Wir danken dem Autorenteam und den Fachgruppenmitgliedern für die intensive Mitarbeit und wünschen allen Leserinnen und Lesern eine erkenntnisreiche und informative Lektüre.

**Christof Weinhardt**

Leiter der Begleitforschung des Technologieprogramms „Smart Data – Innovationen aus Daten“

Leiter der Fachgruppe „Wirtschaftliche Potenziale und gesellschaftliche Akzeptanz“

**Jörn Müller Quade**

Sprecher und Initiator des Kompetenzzentrums für angewandte Sicherheitstechnologie (KASTEL)

Leiter der Fachgruppe „Sicherheit“

## Sicheres Identitätsmanagement – Sichere Prozesse

Das World Wide Web stellt seit jeher Anforderungen an das Identitätsmanagement – und die Relevanz, Identitäten hinsichtlich ihrer Zugangsberechtigung digital nachweisen zu können, verliert nicht an Gewicht. Im Gegenteil, mit steigender Anzahl der vernetzten Dienste, Personen, Geräte, Fahrzeuge und Sensoren – auch in Hinblick auf das Internet of Things (IoT) – steigt die Bedeutung. Es können dabei anonyme, pseudonyme oder auch identifizierte Zugänge zu den Diensten erfolgen – den kontrollierten Umgang rund um diese Thematik regelt das Identitätsmanagement. Gerade weil sich im World Wide Web zunehmend stärker Dienstleistungen etablieren, die individualisiert oder (sicherheits-)kritisch arbeiten, gewinnt das Thema ständig an Bedeutung. Nur mit einem Identitätsmanagement können personalisierte Lösungen angeboten werden, die einerseits dem Benutzer genau diesen beschriebenen Mehrwert bieten und andererseits dem Dienstleister auch gestatten, personalisierte Lösungen oder Dienste anzubieten. Die Definition von Identitätsmanagement schließt hierbei mit ein, dass der Dienstleister sich verlässlich darauf berufen kann, dass die Identität des Benutzers auch tatsächlich echt ist. Eine (digitale) Identität kann hierbei als Summe mehrerer personenbezogener Eigenschaften verstanden werden. Die Echtheit der digitalen Identität ist dann besonders relevant, wenn vertragliche Vereinbarungen getroffen werden, die nachhaltig gelten und belastbar sein sollen.

In dem Zusammenhang sei darauf hingewiesen, dass eine digitale Verifikation vielmehr die Aufgabe der Identitätsfeststellung hat: die Überprüfung, ob die digitale Identität mit der realen übereinstimmt, also

ein und dieselbe Person gemeint ist. Wurde eine digitale Identität erzeugt, kann eine Authentifizierung erfolgen. Während die Authentifizierung der digitalen Identität de facto notwendig ist, um etwa autorisiert zu werden, ist eine Verifikation der Person oftmals nicht notwendig. Oft genügen einzelne Attribute einer Person, wie beispielsweise ihr Alter oder ihr Wohnort, um den Dienst anzubieten. Identitäten sind dabei komplex und bestehen aus technischer Sicht aus einer Ansammlung von Attributen einer Entität – also eines Benutzers oder Dienstansbieters. Beispiele für Attribute sind Konto- oder Kreditinformationen, Anschrift, Vor- und Nachname. Aus Benutzersicht ist es beschwerlich, mit jeder neuen Registrierung all diese Attribute erneut hinterlegen zu müssen. Doch nicht nur die initiale Registrierung, auch die Pflege jener hinterlegten Daten ist zuweilen mit Umständen verbunden – ändert sich ein Attribut, wie etwa die Anschrift, macht das zunächst grundsätzlich Aktualisierungen überall dort erforderlich, wo diese nicht mehr aktuell sind, jedoch benötigt werden.

Angesichts der fortschreitenden digitalen Tertiärisierung – also der wachsenden Zahl der Beschäftigten im Dienstleistungssektor bei gleichzeitiger Abnahme der Beschäftigten in der Produktion – wächst das Bedürfnis nach Lösungen, die diese Umstände berücksichtigen und auflösen. Daher führen auch die Entwicklungen neuer Technologien sowie die steigenden Ansprüche an die Usability dazu, dass sich die Art und Weise ändert, wie Authentifizierung erfolgt. Dass sich der Dienstanbieter authentifiziert, indem Zertifikate ausgetauscht werden, die jeder Client lokal validieren kann, hat sich mittlerweile (zum Beispiel durch die



Nutzung von TLS) als Standard etabliert. Dass sich jedoch der Benutzer im Gegenzug ebenfalls mit seiner tatsächlichen Identität (personenbezogenen Attributen) authentifiziert – also eine bidirektionale Authentifizierung erfolgt – ist hingegen derzeit meist nur dort der Fall, wo es auch rechtlich vorgeschrieben ist, etwa bei der Eröffnung eines neuen Bankkontos.

## Notwendigkeit von Identitätsmanagement in Big/Smart Data

Dienstleistungen rund um Big/Smart Data sind ohne Identitätsmanagement undenkbar. Dies beginnt bereits bei den Anforderungen an Systeme, die sich auf Big/Smart Data beziehen. Dauerhafte Verfügbarkeit, Robustheit und Sicherheit sind solche Anforderungen, wobei schon die dauerhafte Verfügbarkeit und die Sicherheit ein Identitätsmanagement bedingen. Auch werden Daten als neuer Produktionsfaktor bezeichnet, der sich daher neben den klassischen Produktionsfaktoren wie Boden, Kapital oder Arbeit einreicht. Während die klassischen Produktionsfaktoren die Eigenheit hatten, nicht ohne Weiteres kopierbar zu sein, lassen sich Daten mit verhältnismäßig geringem Aufwand vervielfachen. Sie sind also besonders schützenswert. Doch sie sind es nicht nur aus ökonomischen Gründen, wenn Daten beispielsweise Wettbewerbsvorteile oder Monopolstellungen begründen, sondern auch aus rechtlichen Gründen, gerade wenn es um personenbezogene Daten und Datenschutz geht. Big-/Smart-Data-Systeme brauchen also Sicherheit und sind klassischerweise dauerhaft verfügbar, um in andere Systeme integriert zu werden. Ein Da-

tenaustausch ist Sinn und Zweck der Integration, es findet also eine Interaktion zwischen Systemen statt, die im Zweifel sensible und wertvolle Daten austauschen. Daher ist eine Authentifizierung sowohl für Systeme als auch für Menschen erforderlich, um für Zugriffe verschiedenster Art (lesen/schreiben) autorisiert werden zu können. Es wäre fahrlässig, derart sicherheitsbedürftige Systeme nicht ausreichend vor dem Zugriff unbefugter Dritter zu schützen. Um diesen Schutz herzustellen, spielt Identitätsmanagement eine entscheidende Rolle. Wie sich Identitätsmanagement seitdem verändert hat und welche architektonischen Veränderungen stattfanden, wird in dieser Publikation beschrieben. Eine Vielzahl kommerzieller und auch freier Software und eine große Menge an Standards, teils mehr und teils weniger etabliert, unterstützen hierbei. Zudem werden ausgewählte Technologien vorgestellt.

## Die wichtigsten Prozessschritte

Unabhängig vom gewählten Konzept und den verwendeten Techniken, lassen sich bestimmte Prozessschritte zur Nutzung eines Online-Dienstes stets wiederfinden. Die nachfolgende Abbildung zeigt die Prozessschritte in einem einfachen, linear verlaufenden Sequenzdiagramm. Tatsächlich ist der Prozess in der Realität verzweigter und komplexer und variiert je nach eingesetzter Technologie.

### Registrierung

Bei der Registrierung, englisch auch „Client Onboarding“, meldet sich die Person erstmalig bei einem Dienst an. Meist legt der Dienst dabei ein Benutzerkonto in einer internen Datenbank an und erstellt einen Bezeichner, englisch „Identifier“, für die Person. Häufig werden hierbei auch persönliche Daten der Person an den Online-Dienst übertragen, um den Anforderungen des „Know-your-Customer“ zu entsprechen. Bei der Registrierung wird auch der Zugangsschutz für das Benutzerkonto festgelegt, heute immer noch häufig durch ein Passwort.

### Verifikation der Daten (Optional)

Je nach Dienst und den anzuwendenden Regularien werden die bei der Registrierung durch die Person freigegebenen persönlichen Daten möglicherweise verifiziert<sup>1</sup>. Beispielsweise sieht das Geldwäschegesetz vor, dass bei der Eröffnung eines Bankkontos die Identität der Person überprüft werden muss. Diese Leistung wird meist durch einen Drittanbieter erfüllt, wie beispielsweise im Postident-Verfahren durch einen Beschäftigten der Post. Doch auch ein Video-Streaming-Dienst muss möglicherweise das Alter seiner Kunden verifizieren.

### Identifikation

Nach der Registrierung ist es der Person möglich, sich gegenüber dem Online-Dienst zu identifizieren, sich „einzuloggen“ oder „anzumelden“. Dazu wird zunächst von der Person ihr Bezeichner an den Dienst übertragen, häufig durch Eingabe des Bezeichners in ein Text-

feld. Da Bezeichner freiwillig oder unfreiwillig in die Hände Dritter geraten könnten, wird anschließend mit der Authentifizierung fortgefahren.

### Authentifizierung

Während die Person bei der Identifikation nur ihren Bezeichner angibt, wird bei der Authentifizierung sichergestellt, dass die Person auch die ist, für die sie sich ausgibt. Dazu wird entsprechend dem bei der Registrierung festgelegten Zugangsschutz vorgegangen, also zum Beispiel ein Passwort angegeben oder eine SMS mit einem Sicherheitscode angefordert. Aus Komfort-Gründen wird häufig in dem Browser oder der App der Person eine nur schwer zu erratene Zeichenkette in Form eines Cookies hinterlassen, der bei der nächsten Verwendung des Dienstes die Authentifizierung vereinfacht.

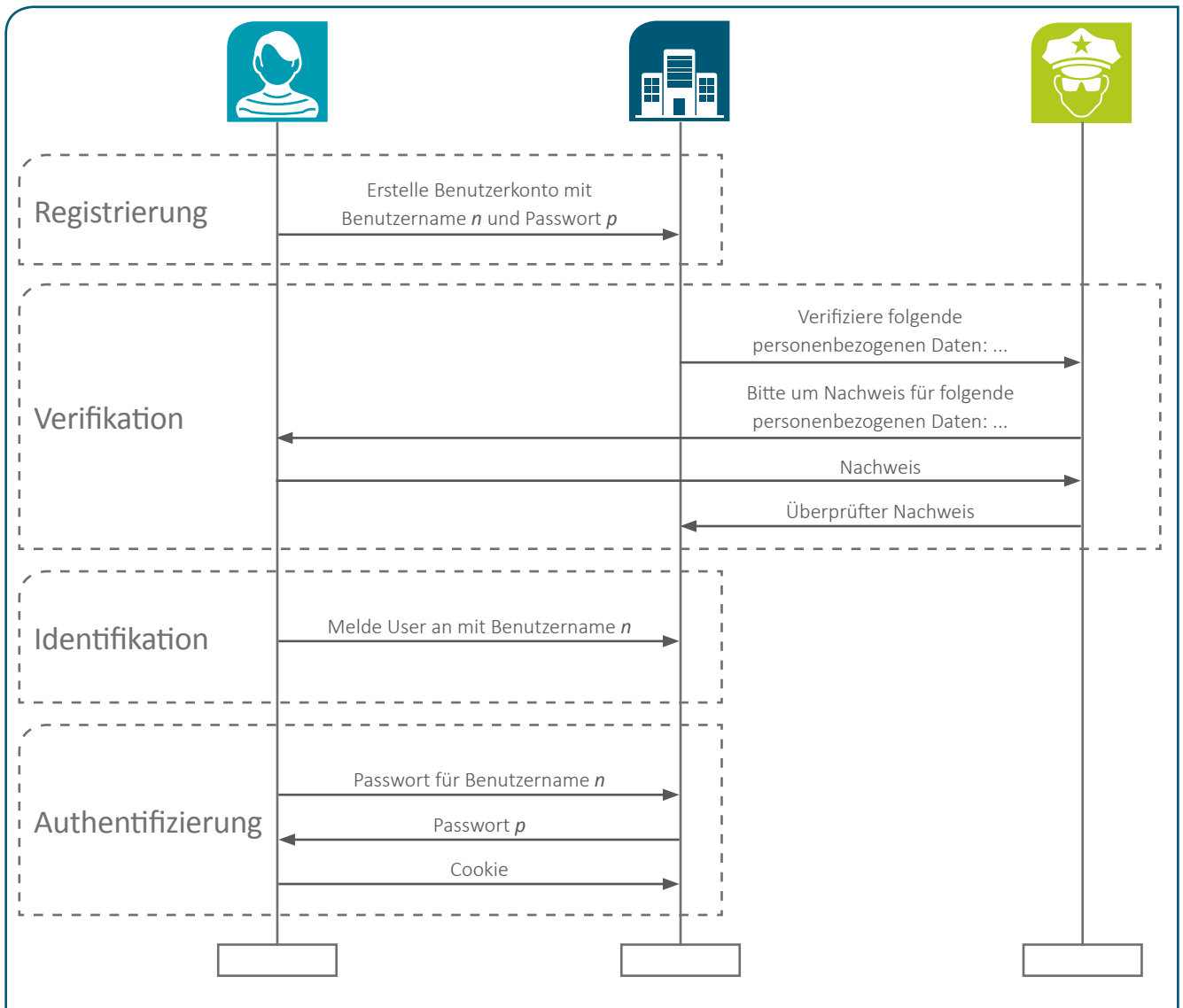
### Autorisierung

Ist die Person authentifiziert, kann der Dienst die Person mit ihrem Benutzerkonto verknüpfen und so den personalisierten Dienst anbieten. Häufig geht dies auch mit dem Zugriff auf bestimmte Daten (z. B. bei einem Cloudspeicher-Anbieter), Werte (z. B. bei einem Banking-Dienst) oder allgemeiner, der Möglichkeit Transaktionen durchzuführen, einher. Die Einräumung dieser Rechte wird als Autorisierung bezeichnet.

## Funktionale Aspekte von Identitätsmanagement

In den Anfangszeiten des modernen Internets wurde die Benutzerverwaltung noch von jedem Dienst selbst entworfen und implementiert. Das Ergebnis waren häufig Sicherheitsprobleme (beispielsweise bei der Passwortverwaltung) sowie fehlende Interoperabilität mit anderen Diensten. Das führte schnell zu Bestrebungen, standardisierte Lösungen für das Identitätsmanagement zu entwickeln und zu etablieren.





Aus dem vorangegangenen exemplarischen Ablaufdiagramm einer Anmeldung bei einem Dienst wird schnell klar, dass ein solches Identitätsmanagementsystem unterschiedliche funktionale Aspekte bereitstellen muss. Je nach System und Anwendungsfall können diese jeweils unterschiedlich stark ausgeprägt sein.

### Usermanagement

Eine Anforderung an ein Identitätsmanagementsystem ist, dass es Benutzer und zugehörige Attribute speichern und verwalten kann. Dabei ist es nicht unbedingt notwendig, dass jedem Benutzer genau eine Identität zugewiesen wird. Es kann auch möglich sein, verschiedene Sichten auf die gleiche Identität zu definieren oder sogar mehrere unabhängige Identitäten pro Benutzer zu erlauben.



### **Authentifikation**

Ein Identitätsmanagementsystem stellt Mechanismen bereit, um Benutzer zu identifizieren und einem oder mehreren hinterlegten Accounts zuzuordnen. Dafür können ganz unterschiedliche Technologien zum Einsatz kommen. Während die Authentifizierungsmethode, die am häufigsten zum Einsatz kommt, aktuell noch das Passwort ist, werden sich in Zukunft möglicherweise hardware-basierte Authentifizierungsmerkmale (wie beispielsweise bei der „Universal Second Factor“-Authentifizierung, bei der ein sogenannter Token einen Schlüssel für jede einzelne Sitzung generiert) durchsetzen.

### **Rechte- und Rollenverwaltung/Autorisierung**

Eine weitere Anforderung ist es, Benutzern unterschiedliche Rechte und Zugriffsmöglichkeiten auf die verfügbaren Ressourcen zuweisen zu können und diese auch durchzusetzen. Bei modernen Identitätsmanagementsystemen kommt in der Regel entweder ein rollenbasierter oder ein attributbasierter Zugriffskontrollmechanismus zum Einsatz. Während es bei rollenbasierter Zugriffskontrolle (RBAC) nur möglich ist, den Zugriff auf eine Ressource an die aktuelle Rolle des authentifizierten Benutzers zu koppeln, ist es bei attributbasierter Zugriffskontrolle (ABAC) auch möglich, Attribute des Benutzers und der angefragten Ressource in die Entscheidung einzubeziehen. So könnte beispielsweise der Zugriff auf Ressourcen, die einer bestimmten Abteilung zugeordnet sind, nur Benutzern gestattet werden, die der Abteilung angehören.

### **Föderation**

Identitätsmanagementsysteme können die Funktionalität bereitstellen, sich mit anderen Systemen zu einer sogenannten „Föderation“ zusammenzuschließen. Ist so ein Zusammenschluss erfolgt, können die Systeme Informationen über die authentifizierten Benutzer untereinander austauschen und damit Zugriff auf verbundene Dienste und Ressourcen des jeweils anderen Systems ermöglichen ohne dass eine erneute Authentifizierung notwendig ist. Dies erfordert Vertrauen zwischen den Systemen der Föderation.

### **Single Sign-on (SSO)**

Das System bietet die Möglichkeit, Authentifizierungsinformationen für unterschiedliche Dienste bereitzustellen. Gerade in großen Unternehmen, deren technische Infrastruktur aus vielen verschiedenen Diensten zusammengesetzt ist, ist es eine wichtige Anforderung, dass nicht jeder Dienst ein eigenes Identitätsmanagementsystem benutzt und dass sich Mitarbeiter auch nicht bei jedem Dienst einzeln anmelden müssen. Die Idealvorstellung ist, dass sich Benutzer nur einmal zentral authentifizieren müssen, um dann Zugriff auf alle Dienste zu haben, für die sie autorisiert sind. Föderationen von Systemen sind eine Möglichkeit, SSO umzusetzen.

# Evolution des Identitätsmanagements

## **Blick in die Vergangenheit: Eine Identität pro Dienst – dienstzentrierte Identitäten**

Möchte eine Person einen personalisierten Dienst nutzen, muss der Dienst die Person zunächst einmal identifizieren können. Seit den Anfängen des Internets wurde dies entweder explizit durch die Registrierung eines Benutzer-Accounts oder implizit durch das Setzen von Cookies umgesetzt. Hier galt lange die Prämisse „neuer Dienst – neue Identität“, denn bei jeder Registrierung wurde eine neue digitale Identität erzeugt und alle Daten neu eingegeben. Theoretisch wusste die Person genau, welche Daten sie bei der Registrierung angab – es gab jedoch keine hinreichende Unterstützung, dies auch entsprechend zu protokollieren. Die ständige neue Registrierung war ebenso mühselig wie die Verwaltung der vielen redundanten digitalen Identitäten.

## **Die Zwischenform: Eine Identität für mehrere Dienste – föderationszentrierte Identitäten**

Um diesen Nachteilen entgegen zu wirken, wurde das Konzept der Federated Identity entwickelt. Die Idee bestand darin, dass Personen eine ganze Föderation von Diensten mit einer einzigen digitalen Identität nutzen konnten. Ein prominentes Beispiel war hier beispielsweise Microsoft Passport, das den Zugang zu allen Microsoft-Diensten (hotmail, MSN etc.) sowie zu weiteren ausgewählten Diensten erlaubte. Für die Person wurde die Identifikation bei diesen Diensten komfortabler, denn „neuer Dienst“ hieß damit nicht mehr zwangsweise auch „neue Identität“. Welcher Dienst eigentlich welche persönlichen Daten hielt, war für den Benutzer jedoch meist nicht ersichtlich.

## **Der State of the Art: Identität als Dienstleistung – personenzentrierte Identitäten**

Die Entkopplung von Dienst und Identität, die durch die Federated Identity begonnen hatte, nahm schließlich durch die Entstehung sogenannter Identitäts-Provider weiter zu: Anstatt sich bei jeder Föderation von Diensten anmelden zu müssen, erlaubt

ein Identitäts-Provider eine einmalige Registrierung. Der Identitäts-Provider bietet das Identitätsmanagement also als Dienstleistung an und erlaubt Dienst Anbietern den Zugriff auf die Identitäten über eine API-Schnittstelle. Vertrauen Person und Dienst dem Identitäts-Provider, wird eine explizite Registrierung bei Diensten vermieden und die Person muss bei dem Dienst keine Daten mehr eingeben, sondern kann diese direkt vom Identitäts-Provider sicher übertragen lassen. Theoretisch erlaubt dieser Ansatz – Vertrauen in den Identitäts-Provider vorausgesetzt – der Person eine Einsicht in die Übermittlung und Nutzung ihrer persönlichen Daten. In den letzten Jahren hat sich unter den Identitäts Providern ein Oligopol gebildet – die heute beliebtesten Identitäts-Provider in der westlichen Welt sind wohl Facebook und Google.

Die Bezahlung des Identitäts-Providers kann sowohl durch die Person als auch über den Dienst erfolgen. Eine weitere Einnahmequelle für Identitäts-Provider liegt in der hohen Anzahl von persönlichen – und damit wertvollen – Daten. Ein Identitäts-Provider kann beispielsweise Profile von Personen erstellen oder Daten verschiedener Personen zusammenführen. Da die Kontrolle vollständig beim Identitäts-Provider liegt, hat die Person keine Souveränität über ihre Identität, sondern ist eher einem Vendor-Lock-In ausgeliefert.

## **Blick in die Zukunft: Volle Souveränität – selbstverwaltete Identitäten**

Das Konzept der selbstverwalteten Identität, englisch Self-Sovereign Identity<sup>2</sup>, soll der Person die vollständige Souveränität über ihre Identität zusichern: Die Person kann ihre eigene Identität selbständig erzeugen, von dritter Seite verifizieren lassen, und diese verwenden, um sich bei Diensten zu identifizieren und den Zugriff auf persönliche Daten zu gewähren. Das heißt, die Identität existiert unabhängig von Diensten oder Identitäts Providern und ist unter der vollen Kontrolle der Person. Die Freigabe persönlicher Daten soll nur durch explizite Zustimmung der Person geschehen und

dem Prinzip der Datensparsamkeit folgen, das heißt, es sollen nur die Daten übertragen werden, die für die erfolgreiche Ausführung des Prozesses notwendig sind. Die Person soll auf diese Weise jederzeit vollständigen Zugang zu ihren eigenen Daten erhalten – ein Umstand, der durch die Transparenz von Systemen und Algorithmen verstärkt werden soll. Um die Nutzer-Erfahrung abzurunden, ist es erforderlich, dass digitale Identitäten portabel, interoperabel und langlebig sind. Der Ansatz zielt damit klar auf den Schutz der Persönlichkeitsrechte der Person und viele der Prinzipien lassen sich so auch in der Datenschutz-Grundverordnung der EU wiederfinden.

### Evolution der Konzepte

Die Evolution spiegelt sich auch in den später vorgestellten Konzepten wieder, wie aus Abbildung 1 entnommen werden kann. Alle diese Konzepte erfüllen den Zweck, dienstzentrierte Identitäten abzulösen. Technologien wie Kerberos, SAML 2.0, OAuth 2.0 und

Open ID Connect unterstützen föderationszentrierte Identitäten und können somit beispielsweise für mehrere Dienste innerhalb eines Firmennetzwerks verwendet werden. Des Weiteren bieten sie aber auch die Möglichkeit des personenzentrierten Identitätsmanagements. Das bedeutet, der Betreiber kann das Identitätsmanagement auch für Nutzer außerhalb des Unternehmens als Dienstleistung anbieten. Zu dieser Evolutionsstufe gehören auch Konzepte wie der elektronische Personalausweis (nPA), Verimi und Verime. Zudem entstehen aktuell einige Konzepte, wie UPort, Sovrin, Civic und Jolocom, die sich in die selbstverwalteten Identitätsmanagementsysteme einordnen. Diese verwenden Distributed-Ledger-Technologien wie Blockchains und darauf aufbauende Smart Contracts zur Verwaltung der digitalen Identitäten und versuchen so, zentrale Vertrauensinstanzen durch alternative Vertrauensmodelle zu ersetzen. Diese Systeme sind jedoch noch nicht ausgereift und können daher etablierte Systeme aktuell nicht sinnvoll ersetzen<sup>3</sup>.

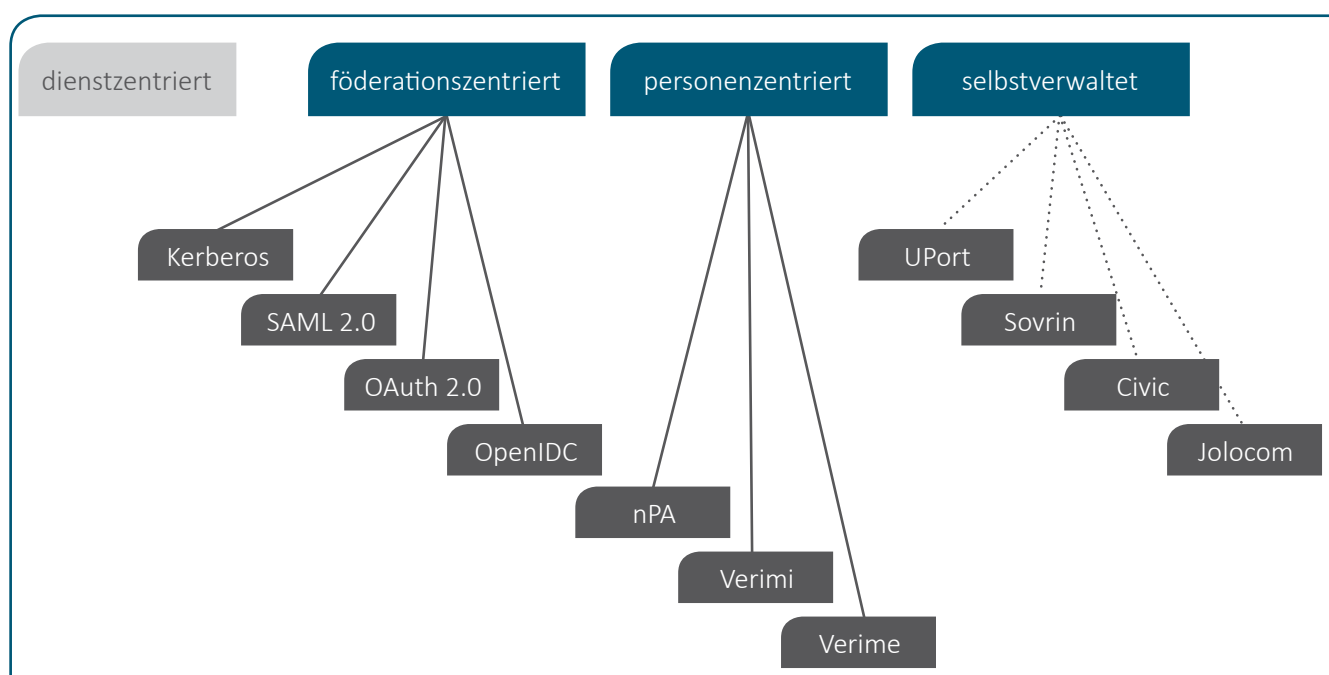


Abbildung 1: Evolution der Technologien.

# Betrachtung aktueller Konzepte

## (Fachgruppe Sicherheit)

Im Folgenden werden aktuelle technische Konzepte des Identitätsmanagements vorgestellt. Dabei betrachten wir ein breites Spektrum von Technologien und beleuchten, welche Aspekte des Identitätsmanagements diese unterstützen.

### **Kerberos**

Kerberos<sup>4</sup> ist ein Authentifizierungsprotokoll für Netzwerke. Das Protokoll wurde 1978 am MIT entwickelt – aktuell in der Version 5. Mit Kerberos lassen sich Single-Sign-on-Systeme umsetzen. Neben dem Serviceprovider und dem Client sind noch ein Authentifizierungsserver und der Ticket-Granting-Server vorhanden. Mit Hilfe dieser Server wird das Protokoll zum Anmelden bei Service Providern ausgeführt. Hierbei erhält der Client ein Ticket, das als Autorisierungsnachweis gegenüber dem Serviceprovider benutzt wird.

Hierbei sind Authentifizierungsserver und Ticket-Granting-Server für einen bestimmten Zusammenschluss von Service Providern, Realm genannt, zuständig. Es besteht auch die Möglichkeit, dass ein Ticket-Granting-Server ein Ticket für einen Ticket-Granting-Server eines anderen Realms erstellt, so dass auch die Authentifikation zwischen unterschiedlichen Realms und somit Föderationen möglich sind.

Kerberos nutzt ausschließlich symmetrische Verschlüsselungsverfahren und erfordert daher den Austausch eines gemeinsamen Geheimnisses zwischen Client und Authentifizierungsserver, beispielsweise in Form eines Passworts. Dadurch ist der Authentifizierungsserver jedoch auch ein attraktives Ziel für Angreifer.

### **Security Assertion Markup Language 2.0 (SAML2.0)**

SAML2.0<sup>5</sup> ist ein Protokollstandard zum Austausch von Authentifikationsdaten gegebener Identitäten. Dieser wurde von der Non-Profit-Organisation OASIS entwickelt und standardisiert.

An den Protokollen nehmen in der Regel drei Akteure teil. Zum einen ein zuerst nicht authentifizierter Nutzer, welcher die Dienste eines zweiten Akteurs, des Serviceproviders in Anspruch nehmen möchte. Um die Authentizität der Identität des Nutzers zu prüfen, verlangt der Serviceprovider eine sogenannte „Assertion“ (Zusicherung) vom „Identity Provider“, dem dritten Akteur. Die Assertions beinhalten nichtmanipulierbare Informationen über die Authentizität der Identität des Subjekts und können bei Bedarf auch Attribute der Identität beinhalten.

Es stehen mehrere Möglichkeiten zur Verfügung, SAML2.0 in die eigene Infrastruktur zu integrieren: Basierend auf der Spezifikation kann man eine eigene Lösung implementieren. Dies erfordert jedoch ein tiefes Verständnis der Spezifikation und Sicherheitsmechanismen im Allgemeinen. Alternativ kann man existierende APIs wie z. B. Spring Security SAML oder OpenSAML3 verwenden, die einige Details abstrahieren. Die einfachste Möglichkeit der Integration besteht darin, eine bereits implementierte Lösung, wie beispielsweise Shibboleth, zu verwenden. Dies ist eine Open Source Lösung, die Single Sign-on mittels SAML2.0 umsetzt.

OASIS bietet zudem einen weiteren Protokollstandard namens XACML, der es ermöglicht, attributbasierte Zugriffskontrolle umzusetzen. Dieser lässt sich auch mit SAML kombinieren.

### **OAuth 2.0**

OAuth 2.0<sup>6</sup> ist ein Protokollframework für die Delegation von feingranularen Zugriffsrechten mit zeitlicher Beschränkung. Das zugrundeliegende Szenario sieht wie folgt aus: Ein Nutzer möchte einem Dienst Zugriff auf Ressourcen gewähren, die bei einem Serviceprovider gespeichert sind, ohne seine eigenen Zugangsdaten preiszugeben. Dazu kann sich der Nutzer Access-Tokens ausstellen lassen, die Zugriffsrechte auf die Ressource definieren und eine begrenzte Gültigkeits-



dauer haben. Der Nutzer wird von dem Dienst, der Zugriff auf eine Ressource erhalten soll, an den Authentifizierungsserver weitergeleitet. Stimmt er dem Zugriff zu, so wird ein Access-Token ausgestellt und an den Dienst übertragen. Mit diesem Access-Token kann der Dienst auf die Ressource zugreifen. Da es sich um eine offene Spezifikation handelt, wird die Interoperabilität von unterschiedlichen Implementierungen ermöglicht und dadurch der Integrationsaufwand reduziert. OAuth 2.0 wird beispielsweise von Dropbox und GitHub unterstützt.

### OpenID Connect

OpenID Connect<sup>7</sup> ist ein Protokollframework, das OAuth 2.0 um einen Identitätsbegriff erweitert und dadurch Authentifizierung ermöglicht. Dazu wird ein sogenanntes ID Token eingeführt. Generell erlaubt das Protokoll einem Serviceprovider die Identität eines Nutzers zu überprüfen, die von einem Authentifizierungsserver festgestellt wird. Ein Nutzer, der ein Konto bei einem OpenID-Provider hat, kann sich somit bei einem Serviceprovider einloggen ohne bei diesem ein Benutzerkonto anzulegen. Natürlich muss der Serviceprovider dem Authentifizierungsserver vertrauen. Die Benutzerdaten und Authentifizierungsinformationen müssen dadurch nur bei einem Anbieter abgelegt werden und lassen sich dadurch effektiver von dem Benutzer verwalten. Andererseits ist der Authentifizierungsserver dadurch auch ein attraktives Angriffsziel und erfordert eine stärkere Absicherung. Der Ablauf des Protokolls sieht folgendermaßen aus: Der Nutzer wird vom Serviceprovider zu dem vom Nutzer gewählten OpenID-Provider weitergeleitet. Dort authentifiziert sich der Nutzer. Der Authentifizierungsmechanismus ist nicht standardisiert und somit können unterschiedliche Verfahren verwendet werden. Der OpenID-Provider stellt ein ID-Token und ein Access-Token aus. Das ID-Token erlaubt dem Dienst, Informationen über den Nutzer abzurufen. Mit OpenID Connect lässt sich Single Sign-on mit wenig Aufwand umsetzen. Es ist noch ein recht junges Protokoll, je-

doch stellen bereits mehrere Unternehmen, wie beispielsweise Google, Authentifizierungsserver zur Verfügung, die für den Login auf der eigenen Webseite oder App verwendet werden können. Zudem ist es möglich einen eigenen Authentifizierungsserver zu betreiben, beispielsweise mit Keycloak.

OpenID Connect bietet eine sehr ähnliche Funktionalität wie SAML2.0. SAML2.0 ist etwas ausgereifter als OpenID Connect, bringt jedoch auch mehr Komplexität mit sich. Daher muss vor dem Einsatz untersucht werden, welches der beiden Protokollframeworks sich in dem speziellen Fall besser eignet.

### Der Elektronische Personalausweis

Der neue Personalausweis (nPA<sup>8</sup>) besitzt einen RFID-Chip mit kryptographischen Funktionen und bietet dadurch eine Verifikation und Authentifizierung des Nutzers. Zudem sind personenbezogene Daten, wie beispielsweise die Anschrift, gespeichert. Um die Online-Ausweisfunktion nutzen zu können, benötigt man ein passendes Lesegerät und einen eID-Client, z. B. die AusweisApp2.

Ein Serviceprovider benötigt dagegen ein behördliches Zertifikat für die Daten, die er vom nPA auslesen möchte. Zudem muss er einen eID-Server betreiben, der eine Verbindung zur behördlichen Public-Key-Infrastruktur hat. Sind diese Voraussetzungen erfüllt, so findet der Übertragungsprozess folgendermaßen statt:

Zuerst müssen die Daten mithilfe der sechsstelligen PIN auf dem Ausweis entsperrt werden. Anschließend werden Sicherheitsparameter über einen Link des Serviceproviders durch den Browser an die AusweisApp2 weitergeleitet. Nach dem Austausch und der Überprüfung der Zertifikate seitens des Serviceproviders und des Ausweises wird eine sichere Punkt-zu-Punkt-Verbindung zwischen der AusweisApp2 und dem eID-Server aufgebaut. Nun können die angeforderten personenbezogenen Daten übertragen werden.



Die Integration der Online-Ausweisfunktion des nPAs in den eigenen Web-Dienst benötigt keine besonderen Architekturänderungen am eigenen Dienst. Vielmehr besteht die Hürde in der behördlichen Zustimmung, um ein Zertifikat für die gewünschten Leserechte zu erhalten. Ist der eID-Server entsprechend den BSI-Spezifikationen eingerichtet, kann man die Authentifikation in einer transparenten Weise nutzen. Des Weiteren wird in den Spezifikationen des BSI auch eine Möglichkeit beschrieben, den nPA auch im Kontext von SAML einzusetzen.

### Web Authentication API

Die Web Authentication API<sup>9</sup> wurde eingeführt, um Personen die Möglichkeit zu geben, sich über den Browser bei Webdiensten zu authentifizieren ohne ein Passwort zu verwenden.

Der Benutzer benötigt einen „Authenticator“, ein Gerät, das mit dem Browser kommunizieren und Daten signieren kann. Zuerst muss der Nutzer seinen öffentlichen Schlüssel beim Webdienst registrieren. Für jeden Dienst wird ein neues Schlüsselpaar erzeugt und mit einem langlebigen privaten Schlüssel signiert.

Bei der Authentifikation sendet der Webdienst eine Nachricht an den Authenticator, welche von ihm mit dem erzeugten privaten Schlüssel signiert und an den Webdienst zurückgeschickt wird. Der Webdienst kann anschließend die Signatur auf Korrektheit prüfen. Ein Vorteil dieser Methode besteht darin, dass bei einem erfolgreichen Angriff auf einen Dienst keine Geheimnisse abhanden kommen, da dort lediglich die öffentlichen Schlüssel abgelegt werden.

Bei der Web Authentication API handelt es sich um ein Authentifizierungsprotokoll und kein vollständiges Identitätsmanagementsystem. Jedoch kann die Web Authentication API auch in anderen Systemen, die den Authentifizierungsmechanismus nicht festlegen, wie beispielsweise OpenID Connect, verwendet werden.

### Verimi

Verimi<sup>10</sup> ist ein Partnerprojekt, an dem Firmen aus unterschiedlichen Bereichen beteiligt sind. Hierzu gehören Allianz, Axel Springer, Daimler, Deutsche Bank, Lufthansa und Telekom.

Verimi ist, im Gegensatz zu reinen Authentifikationssystemen wie Kerberos, ein Identitätsmanagementsystem. Hierbei werden verschiedene Identitätsattribute des Benutzers gespeichert. Dazu gehören Name, Adresse, Geburtsdatum, Geburtsort, Telefonnummer, E-Mail-Adresse und Bankverbindungen. Diese Daten können nun bei Service Providern nach der Authentifizierung verwendet werden, ohne dass diese die gespeicherten Identitätsattribute selbst erheben müssen. Die Kenntnis dieser Attribute ist teilweise für die Vertragsabwicklung nötig und teilweise, um Regularien zu erfüllen. Zu diesen Regularien gehört die Legitimationsprüfung zur Verhinderung von Geldwäsche, die Kreditinstitute vornehmen müssen. Ziel eines Identitätsmanagementsystems ist es also, zeitaufwändige Gänge zu Behörden und Banken durch Online-Interaktionen zu ersetzen.

Eine Herausforderung hierbei ist die Verifikation der Identität des Benutzers nach der Erstellung des Benutzerkontos. Verimi bietet hier zwei Möglichkeiten. Zum einen kann man die Identität über vertrauenswürdige Serviceprovider, bei denen sich die Benutzer bereits registriert haben, sicherstellen. Zum anderen gibt es die Möglichkeit, auf Videoidentifikation zurückzugreifen. Hierbei wird das Verfahren Video-Ident von der webID Solutions GmbH verwendet. Dabei wird über ein Videotelefonat mittels eines Ausweisdokumentes die Identität des Benutzers überprüft. Es gibt auch andere Videoidentifikationssysteme, beispielsweise IDNow. Bei diesem kann man die Videoidentifikation in ein vorhandenes Authentifikationssystem einbauen, um die Identität des Benutzers zu verifizieren.

Um eine Single-Sign-on-Authentifikationsfunktionalität zu bieten wird OpenID Connect verwendet. Verimi legt nach eigener Aussage Wert auf Datenschutz und Sicherheit und orientiert sich am Leitfaden zur Erstellung von Kryptokonzepten<sup>11</sup> des BSI. Daten, die in Verimi aufgenommen werden, müssen verifiziert werden. Diese Verifikation ist datenspezifisch (z. B. SMS bei Mobilnummern).

Ein Ziel von Verimi ist es, dass Nutzerinnen und Nutzer jederzeit die Kontrolle über die von ihnen zur Verfügung gestellten Daten haben. Hierzu gehört, dass die Benutzerinnen und Benutzer entscheiden, welcher Serviceprovider wann welche Daten erhält. Zusätzlich werden die Transaktionen gespeichert, damit die Nutzerinnen und Nutzer nachvollziehen können, welche Serviceprovider zu welchen Zwecken Daten von Ihnen erhalten haben.

### Verime

Verime<sup>12</sup> ist ein blockchainbasiertes Identitätsmanagementsystem. Die Zielsetzung von Verime ist ähnlich der von Verimi. Es soll ein Identifikationsdienst bereitgestellt werden.

Verime verwendet auch ein Videoidentifikationsverfahren zur Verifikation der Identität. Hierbei wird allerdings eine Machine-Learning-gestützte Gesichtserkennung verwendet. Es ist zu beachten, dass die Sicherheit von Machine Learning gegenüber Angreifern noch unzureichend untersucht wurde. So lassen sich manche Machine-Learning-Systeme durch spezielle Bearbeitung von Bildern, aber auch realen Objekten, in die Irre führen. Bei einer Gesichtserkennung könnte das System z. B. durch die Verwendung von speziellen Brillen zu einer Fehlerkennung gebracht werden<sup>13</sup>.

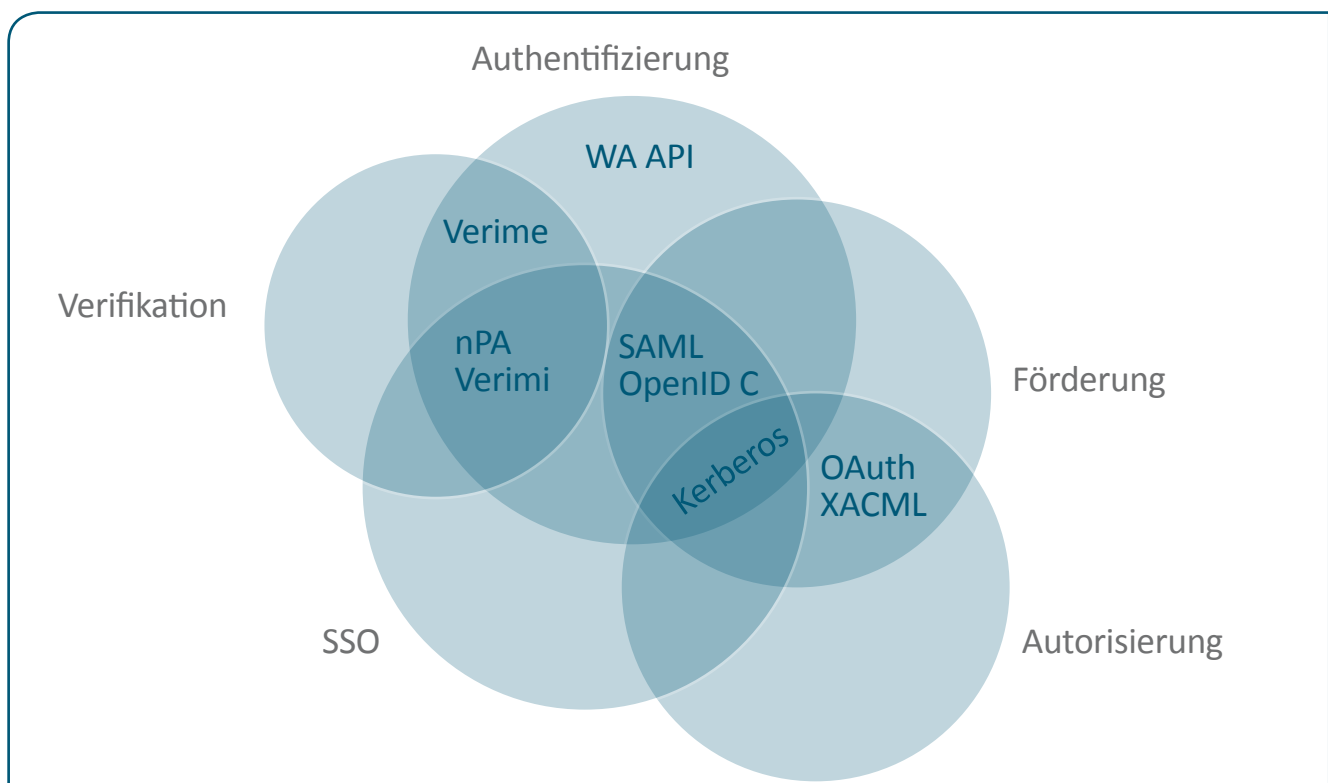


Abbildung 2: Unterstützte Aspekte des Identitätsmanagements der vorgestellten Technologien.

Daher ist es fraglich, ob eine solche Erkennung vor absichtlicher Manipulation schützt.

### **Überblick**

Die vorgestellten Technologien decken alle vorgestellten funktionalen Aspekte des Identitätsmanagements ab. Jedoch gibt es keine Technologie, die für alle Einsatzzwecke optimal ist. Abbildung 1 stellt die unterschiedlichen Aspekte des Identitätsmanagements und die Technologien, die diese erfüllen, dar. Anhand der benötigten Aspekte kann dadurch die Auswahl der Technologie für ein bestimmtes Szenario eingeschränkt werden. Teilweise können die Technologien auch kombiniert werden, beispielsweise kann die Web Authentication API als konkretes Authentifizierungsprotokoll in abstrakteren Protokollframeworks wie SAML 2.0 verwendet werden. Zudem können Verifikationsdienste als Baustein bei der Benutzerregistrierung eingesetzt werden.



# Identitätsmanagement in einer smarten Datenwirtschaft

Identitätsmanagement ermöglicht das sichere digitale Wirtschaften und ebnet so der smarten Datenwirtschaft den Weg. Oder auch: Das digitale Wirtschaften wird durch Identitätsmanagement nicht nur erst möglich, sondern bietet darüber hinaus viel Potenzial, geschäftliche Abläufe effizienter zu machen und zudem weitere Potenziale der überbetrieblichen Zusammenarbeit zu eröffnen. Ein digitales Wirtschaften ohne Datenaustausch ist nahezu unmöglich. Wie einleitend beschrieben betrachten wir Daten auch als Rohstoff des 21. Jahrhunderts sowie als neuen Produktionsfaktor neben Kapital, Boden und Arbeit. Es ist also ein Rohstoff oder Faktor, der dem Unternehmen einerseits – als Rohstoff – von außen zugeführt wird und andererseits – ganz klassisch – als Faktor eingesetzt wird, um Wertschöpfung zu generieren. Identitätsmanagement soll nicht nur, sondern muss unbedingt eine tragende und flächendeckende Rolle einnehmen, sodass Datenaustausch und digitale Kollaboration nicht mit vernachlässigten Sicherheitsrisiken einhergehen. Die Digitalisierung darf nicht durch IT-Sicherheitsprobleme oder entsprechende Gegenbewegungen gebremst werden – es gilt, wirksam und effektiv mithilfe eines guten Identitätsmanagements dagegen anzusteuern.

## Identity Analytics

Die Vielzahl und Komplexität moderner IT-Landschaften, gepaart mit der hohen Änderungsgeschwindigkeit, führt zu neuen Anforderungen an das Identitätsmanagement. Traditionelle regelbasierte Systeme sind diesen Herausforderungen häufig nicht gewachsen und können die Fülle unterschiedlicher Identitäten, die zu unternehmensweiten Benutzerverwaltungssystemen (LDAP, AD etc.) hinzukommen, wie durch Mobiltelefonen oder Cloud-Speicher, nicht unter einen Hut bringen. Bei Identity Analytics handelt es sich um einen durch das Marktforschungsunternehmen Gartner geprägten Begriff, der versucht, unterschiedliche

risikobasierte Ansätze des Identitätsmanagements zu vereinen. Dabei steht die Idee im Vordergrund, dass Big-Data-Systeme nicht nur die Daten für eine evidenzbasierte Zugriffskontrolle enthalten, sondern auch bei entsprechender Konzeption über die technische Reaktionsgeschwindigkeit verfügen, wenn automatisierte Entscheidungen getroffen werden müssen.

Im Mittelpunkt steht dabei die Bedingung, dass bei der Vielzahl unterschiedlicher Systeme und der Geschwindigkeit, in der neue Anwendungen hinzukommen und alte abgelöst werden, langwierige Standardisierungen des Identity und Access Managements (IAM) nicht mehr akzeptabel sind. Das Zeitalter der Digitalisierung erfordert ein agiles IAM, mit dem Unternehmen flexibel auf neue Anforderungen reagieren können und eins, das die zentrale Verwaltung mehrerer Identitäten unterstützt.

Identity Analytics unterstützt hier, indem die in größeren Unternehmen milliardenfach vorliegenden Identitäts- und Zugangsbeziehungen kontinuierlich überwacht und analysiert werden. Dabei werden zuvor im verborgenen liegende Beziehungen zwischen einzelnen Identitäten aufgedeckt oder stillgelegte Accounts identifiziert. Zusätzlich können über Korrelationsanalysen des Zugriffsverhaltens einzelner Nutzer, unkorrelierte Nutzer identifiziert werden. Dies führt zu der Möglichkeit, merkmalsgleiche Nutzergruppen zu identifizieren und mit Risikobewertungen zu bemessen – siehe auch Abbildung 3.

Diese kontinuierliche Überwachung und Analyse unterstützt zudem bei der begründeten Einführung neuer Sicherheitsverfahren. So könnten Accounts, die besonderen Risiken ausgesetzt sind, mit Verfahren wie der Multi-Factor Authentication (MFA)<sup>14</sup> zusätzlich gesichert werden. Die zentralisierte und flexible Verwaltung des IAM-Systems ermöglicht zudem ein schnelles Ausrollen derartiger Maßnahmen.

Zusätzlich werden Lösungen, die zu Identity Analytics befähigen, mit Möglichkeiten versehen, die analysierten Daten entsprechend zu visualisieren. Dies geschieht auf der einen Seite mit flexiblen Dashboards und auf der anderen Seite mit managementfreundlichen Reports, die als Entscheidungsgrundlage dienen.

Die gesteigerten Möglichkeiten, komplexe Auswertungs- und Analyseverfahren einzusetzen, verändern auch das Identitätsmanagement. Anbieter von IAM-Lösungen erweitern ihre Produkte, um den Anforderungen moderner IT-Landschaften gerecht zu werden.

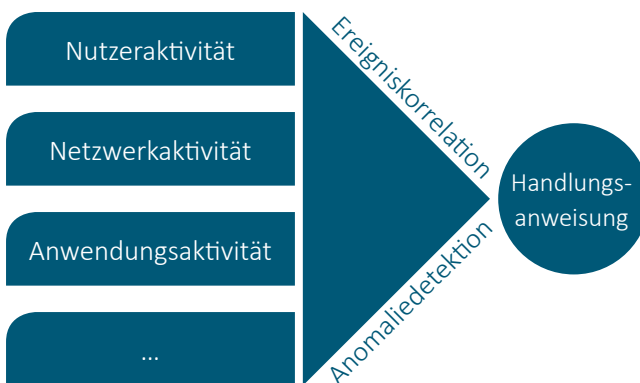


Abbildung 3 - Identity Analytics

Neben den technischen Entwicklungen, die Identity Analytics möglich und erforderlich machen, bieten sich aber auch eine Vielzahl an ökonomischen Mehrwerten sowie die Möglichkeit zu einer gesteigerten Transparenz im Management von Identitäten an. Zu diesem wirtschaftlichen Potenzialen kommt die Möglichkeit dazu, für gesteigerte Transparenz aus der Perspektive von IT-Sicherheits- und -Management zu sorgen. Die Möglichkeit, wesentliche Teile des IAM zu automatisieren und dennoch mit reduziertem Risiko und erhöhtem Grad an Harmonisierung in Organisationen zu etablieren, führt zu einem enormen Einsparpotenzial. Hinzu kommt, dass die Aufwände für die Migration und Neueinführung von Systemen und Anwendungen deutlich sinken. Die so steigende Flexibilität macht es für Organisationen einfacher, unter-

schiedliche Systeme zu testen und zu evaluieren, was wiederum positive Auswirkungen auf die Aktualität und Modernität der Systemlandschaft insgesamt und der Endanwendersysteme im Speziellen hat.

## Plattform der Plattformen

Im Internet haben sich über die letzten Dekaden hinweg eine Vielzahl verschiedener Plattformen etabliert: Google hat nicht nur eine, sondern gleich mehrere (etwa Youtube, Google Plus). Mit Facebook ist eine der größten Plattformen mit Fokus Social Network entstanden. Viele weitere Plattformen wie etwa Uber oder Airbnb sind im Zuge der Sharing Economy entstanden, die Angebot und Nachfrage koordinieren beziehungsweise das Potenzial ungenutzter Ressourcen nutzbar machen. Haben diese Plattformen eine kritische Masse überwunden und profitieren von positiven Netzwerkeffekten (der Nutzen steigt mit der Anzahl der User), werden sie größer und größer. Nach dem „Winner-takes-it-all“-Prinzip wechseln User allmählich zum Monopolisten, da nach der Theorie der Plattformökonomie dort der Nutzen am höchsten ist. Schafft es eine Plattform hingegen nicht, die Hürde der kritischen Masse zu erreichen, ist das Gegenteil der Fall: Nach dem Prinzip „Loser-gets-nothing“ ist der Nutzen viel zu klein, um entweder auf der Plattform zu bleiben oder sich erst dort anzumelden – die Plattform wird sich langfristig nicht bewähren können.

Das hier diskutierte Konzept der Plattform der Plattformen mag zunächst etwas verwirrend klingen, knüpft aber genau an diesem Punkt an. In digitalen Dienstleistungsangeboten und auf dem Softwaremarkt, wo Erfolg mit positiven Netzwerkeffekte steht und fällt, zählt also nicht einzig Wertversprechen und Akzeptanz (und auch nicht nur Qualität und Preis), sondern insbesondere auch die Anzahl der User oder die Vertrautheit der Marke. Ist letzteres gegeben, kann dies Anreiz genug sein, ein Angebot (auch) zu nutzen. Während



große Ökosysteme wie Google oder Facebook weniger mit oben bereits genannten Netzwerkeffekten hadern, sondern vielmehr davon profitieren, kann eine Plattform der Plattformen bei der Koordination helfen. Gemeint ist damit eine Art Meta-Plattform, die mehrere separate Plattformen kombiniert.

Diese Meta-Plattform, also Plattform der Plattformen, bietet wirtschaftliches Potenzial genau für diejenigen, die nicht zu den Großen gehören. Wirtschaftliches Potenzial entsteht in der Theorie hierbei dadurch, dass eine Art Allianz gebildet wird, der mehrere verschiedene separate Plattformen beitreten. Die Allianz bündelt in diesem Ansatz das Identitätsmanagement, was stark in die oben diskutierte Richtung bezüglich Federated Identity geht. Es gibt also pro Person genau eine Identität, mit der sich jede Person gegenüber jeder Plattform authentifizieren kann. Der wirtschaftliche Vorteil für die Plattformen: Je geringer die Wechselkosten, um von einer Plattform auf eine alternative Plattform zu wechseln, desto eher spielt das Preis-Leistungs-Verhältnis eine übergeordnete Rolle. Wechselkosten entstehen auf verschiedene Arten und beginnen mit der vertrauten Bedienung einer Plattform bis hin zur Integration einer Plattform in die eigene IT-Landschaft. Auch der Registrierungsprozess, der optional noch einen Verifikationsprozess einschließt, kann solche Wechselkosten darstellen. Die Einstiegshürde in andere Plattformen, die dieser Meta-Plattform angehören, reduziert sich dadurch – gerade dann, wenn Vertrauen gesteigert werden kann, etwa durch ein gemeinsames Corporate Identity, reduziert sie sich erneut.

Eine Plattform der Plattformen ist ein Konzept, das gerade kleineren Plattformen eine Chance bietet, sich am Markt zu etablieren. Die existentiell-wichtigen Netzwerkeffekte bekämen Rückenwind durch ein etwa zentral organisiertes Identitätsmanagement und der

User profitiert, da nicht überall eine Registrierung geschehen muss, beziehungsweise die Verwaltung der digitalen Identität zentral erfolgen könnte. Für Monopolisten ist hingegen der Anreiz dieses Konzepts aufgrund ihrer dominanten Marktstellung geringer, denn jeder Monopolist verfolgt sein eigenes Ökosystem und strebt Lock-In-Effekte an, möchte die User also an sein Ökosystem binden und durch Wechselkosten vermeiden, dass andere Angebote wahrgenommen werden. Je höher die Wechselkosten sind, desto geringer die Wechselwahrscheinlichkeit – ganz unabhängig davon, ob ein attraktives Preis-Leistungs-Verhältnis gegeben ist oder nicht.

In diesem visionären Konzept könnte sich die Wettbewerbssituation zulasten der Monopolisten verändern. Wird argumentiert, dass durch die Senkung der Einstiegshürde Nutzergewinne verzeichnet werden, wird die Plattform der Plattformen größer und größer und profitiert ähnlich von positiven Netzwerkeffekten wie etwa derzeitige Monopolisten. Der Unterschied, der auch als Vorteil verstanden werden kann, ist nun auch: Durch die Offenheit des Systems und die grundsätzliche Unabhängigkeit der Plattformen untereinander, wird Potenzial hinsichtlich etwaiger horizontaler (alternative, in Wettbewerb zueinander stehende Angebote) oder vertikaler (bezüglich vor- oder nachgelagerter Angebote) Diversifikation freigelegt. Auch „Coopetition“ (steht für Cooperation und Competition gleichermaßen) wäre somit möglich, wenn die Plattform der Plattformen Kooperation ebenso wie Konkurrenz zuließe. Wie eingangs erwähnt, spielen Netzwerkeffekte bei der Auswahl der Plattform eine tragende Rolle. Bei künftigen Entscheidung gegen oder für solche Angebote, könnte im Plattformen-der-Plattformen-Konzept somit die Schwerpunktsetzung wieder mehr zugunsten von Qualität, Wertversprechen oder Preis erfolgen.



## Wertschöpfungsnetzwerke und Kollaboration

Optimierung von Produktionsprozessen, Effizienz im Austausch von digitalen, aber auch physischen Gütern, reibungslose Zusammenarbeit bei der Organisation entlang überbetrieblicher Aktivitäten – ganz gleich, mit welcher Granularität in irgendeinen Bereich inter-organisationaler Kollaboration geschaut wird, Wertschöpfungsnetzwerke sind nicht mehr vom digitalen Austausch zu trennen. Der digitale Austausch ist hierbei nicht als notwendiges Übel zu betrachten, sondern als unterstützender Faktor, der die oben genannten Einleitungspunkte beflügelt.

Wertschöpfungsnetzwerke schließen hierbei horizontale wie vertikale Kooperationsformen ein – oder, wie im Zuge der digitalen Transformation zunehmend häufiger zu beobachten ist, laterale Kooperation: Mit lateraler Kooperation ist diejenige gemeint, bei der Partner zu Kollaborations- und Wertschöpfungszielen zusammenkommen, die aus unterschiedlichen Branchen stammen, also etwa Adidas mit Streamingdiensten, die gemeinsam das Sporterlebnis durch musikalische Ergänzung verbessern. Überall, wo eine Kollaboration entlang von Wertschöpfungsnetzwerken erfolgt, ist Identitätsmanagement relevant. Es muss so sicher sein, dass langfristiges Vertrauen zwischen den Partnern entsteht. Wertschöpfungsnetzwerke sind für umfangreiches Identitätsmanagement nicht nur deshalb besonders gut geeignet, sie exemplifizieren auch die Notwendigkeit der Anwendung und Förderung etablierter und innovativer Konzepte zum Identitätsmanagement. Die Zusammenarbeit über Unternehmensgrenzen hinweg kommt oft auch mit der Zusammenarbeit über Systemgrenzen hinweg einher. Das bedeutet, Unternehmen tauschen zwischen separaten betrieblichen Systemgrenzen hinweg Daten aus, wo

Authentifizierung selbstverständlich ist. Es treffen also verschiedene Authentifizierungssysteme aufeinander und Schnittstellen müssen integriert werden, um einen höheren Automationsreifeegrad zu erreichen. Je populärer und verbreiteter einerseits, desto bekannter und vertrauter sind Identitätsmanagementsysteme andererseits. Etablierte Standards können die Zusammenarbeit unterstützen, da der Weg in die digitale Zusammenarbeit einfacher scheint, denn die Integrationshemmnisse reduzieren sich, wenn etablierte Standards eingesetzt werden, die getestet, bewährt und den Partnern vertraut sind. Kollaborieren Unternehmen untereinander, findet ein Tausch und Transfer von teils sehr sensiblen Rohstoffen statt, deren Existenz oder Verlust über Wettbewerbsvorteile entscheiden können. Daten gelten als Rohstoff des 21. Jahrhunderts und als neuer Produktionsfaktor, sie haben also gerade in datengetriebenen Geschäftsmodellen einen erfolgsentscheidenden Gegenwert. Sie müssen als schützenswertes Gut verstanden werden, was auch durch Aktivitäten in Zusammenhang mit der Corporate Digital Responsibility getrieben sein kann

## Ausblick – Identitätsmanagement zentral denken

Identitätsmanagement ist zentrale Aktivität im unternehmerischen Handeln. Im Zuge der digitalen Transformation gewinnt diese Aktivität weiter an Bedeutung. Da die Menge an Big, aber auch Smart Data stetig zunimmt, steigt auch der Austausch von Daten, dies sowohl intra- als auch interbetrieblich. Die Kollaboration entlang von Wertschöpfungsnetzwerken wird wichtiger und Kernkompetenzen werden gebündelt, damit kreative Geschäftsmodelle ihr wirtschaftliches Potenzial entfalten können – dies eröffnet neue Wertschöpfungsmöglichkeiten. Doch damit diese Wertschöpfungsmöglichkeiten auch genutzt werden, also auch tatsächlich zur wirtschaftlichen Verwertung führen – sei es durch Verfahrensoptimierung, durch mehr Kollaboration oder durch Kostensenkungen –, darf die Sensibilität für das Wirtschaftsgut Daten nicht in Vergessenheit geraten. Um einer Corporate Digital Responsibility, also der unternehmerischen Verantwortung im digitalen Wirtschaften, gerecht werden zu können, kann ein solides Identitätsmanagement helfen. Identitätsmanagement regelt den Zugang zu Infrastruktur und Daten, deren Wettbewerbswert, deren Personenbezug, deren teils ungeahntes Potenzial schützenswert sind. Identitätsmanagement ist daher als zentrale Unternehmensaktivität zu begreifen – dies bedeutet einerseits bewährte, sichere (und in dieser

Publikation vorgestellte) Techniken zum Identitätsmanagement einzusetzen. Andererseits bedeutet dies aber auch, den Faktor Mensch mit in die Betrachtung mit einzubeziehen. Das Management von Identitäten sollte bequem und einfach erfolgen, damit die Zusammenarbeit im, aber auch über Unternehmensgrenzen hinweg nicht durch technische Seiteneffekte negativ ausgebremst wird. So kann Identitätsmanagement, wenn es effektiv eingesetzt wird, richtig effizient sein. Da hin und wieder Mitarbeiter – als Faktor Mensch – eines der größten Sicherheitsrisiken darstellen, da etwa fahrlässiger Umgang beispielsweise mit Credentials (Stichwort Identitätsdiebstahl) oder vernachlässigtes Bewusstsein ernsthafter Umsetzung von Sicherheits-Guidelines IT-Sicherheitsprobleme verursachen können. Daher ist hier die Aufgabe, Mitarbeiter für das Thema Identitätsmanagement zu sensibilisieren. Da technische – genau wie wirtschaftliche – Potenziale gerade beim Thema Identitätsmanagement eng mit dem Thema Akzeptanz einhergehen, ist bei der Konzeption, der Einführung und der alltäglichen Aktivität darauf zu achten, dass nicht komplexe Authentifizierungsvorgänge den Alltag dominieren, sondern Lösungen so integriert und genutzt werden können, dass sie für jeden Mitarbeiter gut bedienbar und erlebbar sind.

## Über die Autoren



PROF. DR. CHRISTOF WEINHARDT

... ist Leiter des Lehrstuhls für Information and Market Engineering am Karlsruher Institut für Technologie und Direktor am FZI Forschungszentrum Informatik. Seine Forschung konzentriert sich auf interdisziplinäre Themen aus dem Bereich Market Engineering mit Anwendungen in der IT-Dienstleistungsindustrie, der Energiewirtschaft sowie in Finanz- und Telekommunikationsmärkten.



SVEN WILLRICH

... studierte Wirtschaftsinformatik und war in der Industrie tätig, bevor er wissenschaftlicher Mitarbeiter am FZI Forschungszentrum Informatik wurde, wo er in der Leitung der Fachgruppe Wirtschaftliche Potenziale und gesellschaftliche Akzeptanz der Smart-Data-Begleitforschung ist. Das Thema Identitätsmanagement begleitet ihn schon seit Studienzeiten sowohl aus wirtschaftlicher als auch aus technischer Sicht.



DR.-ING. NICO RÖDDER

... promovierte im Bereich quantitativer Risikoanalyse und Failure Forecasting im IT-Service-Management am Karlsruher Institut für Technologie. Am FZI Forschungszentrum Informatik leitet er die Abteilung Information Management & Analytics, in der zahlreiche Forschungs- und Industrieprojekte im Bereich Data Analytics, Service und Information Engineering bearbeitet werden.



DR. JAN SÜRMEI

... forscht an der Technischen Universität Berlin und am FZI Forschungszentrum Informatik an sicheren digitalen Identitäten für Menschen und Dinge sowie am Einsatz von Distributed-Ledger-Technologien. Vorher promovierte er in Informatik an der Humboldt-Universität zu Berlin, forschte dort im Bereich Modellierung und Analyse verteilter Systeme und Geschäftsprozesse und war zeitweise als Berater tätig.



### PROF. DR. JÖRN MÜLLER-QUADE

... ist Leiter der Forschungsgruppe Kryptographie und Sicherheit am KIT und Direktor am FZI. Er ist Sprecher und Initiator des Kompetenzzentrums KASTEL. Seine Forschungsschwerpunkte sind unter anderem sicheres Cloud Computing, sichere Mehrparteienberechnung, Sicherheitsdefinitionen und -modelle, sowie Hardware-Vertrauensanker. Das von ihm und seiner Gruppe entwickelte Wahlverfahren „Bingo Voting“ wurde 2008, das Softwareschutzverfahren „Blurry Box Cryptography“ 2014 mit dem deutschen IT-Sicherheitspreis ausgezeichnet.



### DR. DIRK ACHENBACH

... leitet das Kompetenzzentrum IT-Sicherheit am FZI Forschungszentrum Informatik. Davor forschte er am Karlsruher Institut für Technologie im Bereich der Kryptographie. Thematische Schwerpunkte sind formale Sicherheitsmodelle und der Einsatz von kryptographischen Werkzeugen in praktischen Anwendungen.



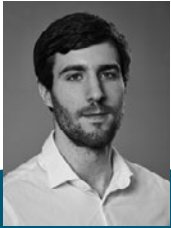
### WASILIJ BESKOROVAJNOV

... studierte Informatik am Karlsruher Institut für Technologie (KIT) mit Schwerpunkten Algorithmentechnik, sowie Sicherheit und Kryptographie. Seit November 2017 ist er Wissenschaftlicher Mitarbeiter am FZI im Kompetenzzentrum IT-Sicherheit. Im Rahmen seiner laufenden Promotion liegt der Forschungsschwerpunkt auf den mathematischen Grundlagen der Kryptographie und der Sicherheit von kryptographischen Protokollen.



### ROLAND GRÖLL

... studierte Informatik am Karlsruher Institut für Technologie. Hierbei vertiefte er sich in den Schwerpunkten Kryptographie und Algorithmentechnik. Am FZI beschäftigt er sich im Kompetenzzentrum IT-Sicherheit mit Kryptographie und Sicherheitsmodellen.



TIMON HACKENJÖS

... studierte Informatik am Karlsruher Institut für Technologie mit den Schwerpunkten Kryptographie und Sicherheit sowie Telematik. Am FZI ist er als wissenschaftlicher Mitarbeiter im Kompetenzzentrum IT-Sicherheit tätig. Dabei beschäftigt er sich mit Kryptographie und Sicherheit von praktischen Systemen.



JOCHEN RILL

... studierte Informatik am Karlsruhe Institut für Technologie mit den Schwerpunkten Kryptographie und Sicherheit, sowie Compilerbau. Am FZI ist er als Leiter des Themenfelds Kryptographie im Kompetenzzentrum IT-Sicherheit tätig. Seine Forschung beschäftigt sich mit dem Nachweis von Sicherheitseigenschaften.

## Fußnoten

- <sup>1</sup> Manchmal wird dieser Prozessschritt auch als Authentifizierung bezeichnet. Da dieser Begriff jedoch auch für den Schritt der Authentifizierung nach der Identifikation verwendet wird, wird in dieser Publikation der Begriff der Verifikation verwendet.
- <sup>2</sup> The Path to Self-Sovereign Identity (2016, April). Abgerufen von <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>
- <sup>3</sup> A First Look at Identity Management Schemes on the Blockchain. (2018, Januar). Abgerufen von <https://arxiv.org/pdf/1801.03294.pdf>
- <sup>4</sup> Microsoft Kerberos. (2018, Mai). Abgerufen von <https://docs.microsoft.com/en-us/windows/desktop/secauthn/microsoft-kerberos>
- <sup>5</sup> SAML V2.0 Technical Overview. (2018, März). Abgerufen von <http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html>
- <sup>6</sup> The OAuth 2.0 Authorization Framework. (2012, Oktober). Abgerufen von <https://tools.ietf.org/html/rfc6749>
- <sup>7</sup> OpenID Connect Core 1.0. (2014, November). Abgerufen von [http://openid.net/specs/openid-connect-core-1\\_0.html](http://openid.net/specs/openid-connect-core-1_0.html).
- <sup>8</sup> Der Personalausweis. (2018, Juni). Abgerufen von [https://www.personalausweisportal.de/DE/Home/home\\_node.html](https://www.personalausweisportal.de/DE/Home/home_node.html)
- <sup>9</sup> Web Authentication: An API for accessing Public Key Credentials Level 1. (2018, März). Abgerufen von <https://www.w3.org/TR/webauthn/>
- <sup>10</sup> Sicherheit VERIMI. (2018, April). Abgerufen von [https://verimi.de/VERIMI\\_Security\\_White\\_Paper\\_DE.pdf](https://verimi.de/VERIMI_Security_White_Paper_DE.pdf)
- <sup>11</sup> Erstellung von Kryptokonzepten. (2018, Juli). Abgerufen von [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptokonzept.pdf?\\_\\_blob=publicationFile&v=2](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptokonzept.pdf?__blob=publicationFile&v=2)
- <sup>12</sup> Whitepaper VeriME. (2018, Juni). Abgerufen von <https://www.verime.mobi/static/dl/whitepaper.pdf>
- <sup>13</sup> Adversarial Generative Nets: Neural Network Attacks on State-of-the-Art Face Recognition. (2017, Dezember). Abgerufen von <https://arxiv.org/pdf/1801.00349.pdf>
- <sup>14</sup> Bei der MFA muss der Nutzer den Beweis seiner Identität über zwei unterschiedliche Wege erbringen. Also z.B. über ein Kennwort und einen Zufallstoken, der auf sein Mobiltelefon gesendet wird.





