Fraunhofer FOKUS

FRAUNHOFER-INSTITUT FÜR OFFENE KOMMUNIKATIONSSYSTEME FOKUS

VERTRAUENSWÜRDIGE DIGITALE IDENTITÄT: BAUSTEIN FÜR ÖFFENTLICHE IT

Jens Fromm, Christian Welzel, Petra Hoepner, Jonas Pattberg

Kompetenzzentrum Öffentliche IT

IMPRESSUM

Autoren:
Jens Fromm, Christian Welzel, Petra Hoepner, Jonas Pattberg

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3436-7173
Telefax: +49-30-3436-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

1. Auflage Oktober 2013

VORWORT

Der Zeitpunkt könnte passender kaum sein: Die Frage nach vertrauenswürdiger Kommunikation über öffentliche IT-Systeme stellt sich für Bürgerinnen und Bürger aber auch für die deutsche Wirtschaft heute drängender denn je zuvor. Die Abwägung zwischen Sicherheit und staatlicher Verantwortung auf der einen und Freiheit und Datenschutz auf der anderen Seite entwickelt sich zu einer gesamtgesellschaftlichen Debatte. Orte der Privatheit gibt es in der realen Welt, muss es diese dann nicht auch im digitalen Raum geben?

Die Relevanz sicherer digitaler Kommunikation zeigt sich nicht nur in der aktuellen Diskussion um staatliche Abhörprogramme. Seit Längerem wird deutlich, dass die herkömmlichen Methoden zur digitalen Abbildung von Identitäten an ihre Grenzen stoßen. Gestohlene Nutzerdaten sind auch bei großen Internetplattformen keine Seltenheit mehr. Identitätsdiebstahl ist eine der am stärksten zunehmenden Kriminalitätsformen in modernen Dienstleistungsgesellschaften und damit eine zentrale Herausforderung für die öffentliche IT.

Durch die zunehmende Vernetzung und die dadurch entstehenden Abhängigkeiten steigt der Schutzbedarf der IT-Infrastrukturen und der darauf aufbauenden Systeme. Informationstechnologien gelten heute als neuralgischer Punkt. Sie sind nicht nur komplex, sondern aufgrund ihrer starken Vernetzung besonders schwer abzusichern. Der Trend zur Vernetzung wird sich trotzdem weiter fortsetzen. Die Herausforderung der Zukunft wird es sein, Mechanismen zu etablieren, die die Entwicklung und Festigung von Vertrauen in öffentliche IT-Systeme langfristig ermöglichen und Vertrauensräume aufspannen. Die Grundlage dafür bilden sichere digitale Identitäten.

In den letzten Jahren sind daher viele neue Technologien für digitale Identitäten entstanden. Sowohl staatliche Lösungen wie der neue Personalausweis oder De-Mail als auch privatwirtschaftliche Initiativen haben dabei ein vorrangiges Ziel: das Vertrauen in und die Sicherheit von öffentlichen IT-Systemen zu erhöhen. Die Philosophien dahinter sind jedoch sehr unterschiedlich: staatliche Ansätze konkurrieren dabei mit wirtschaftlichen Entwicklungen. Eine der spannenden Aufgaben der kommenden Jahre wird folglich sein, die Rolle des Staates für die Gewährleistung digitaler Identitäten zu bestimmen.

Eines hat uns die Entwicklung aller Technologien jedoch immer wieder gezeigt: Die Selbstbestimmtheit der Bürgerinnen und Bürger muss im Mittelpunkt der Konzeption und Entwicklung stehen, insbesondere wenn es darum geht, Vertrauen zu schaffen.

Mit diesem White Paper wollen wir Ihnen eine Einführung in das Thema digitale Identitäten geben. Dabei werden heutige und zukünftige Herausforderungen aufgezeigt und aktuelle Entwicklungen betrachtet. Anhand von acht Thesen wird die Bedeutung digitaler Identitäten in öffentlicher IT zusammengefasst und ein Ausblick auf die zukünftige Rolle des Staates gegeben.

Wir wünschen Ihnen eine spannende Lektüre und hoffen, Ihnen damit den einen oder anderen Denkanstoß geben zu können.

Berlin im Oktober 2013

Jens Fromm

UNTER ÖFFENTLICHER IT VERSTEHT MAN INFORMATIONSTECHNOLOGIEN, DIE IN EINEM ÖFFENTLICHEN RAUM DURCH DIE GESAMTGESELLSCHAFTLICHE RELEVANZ UNTER BESONDERER BERÜCKSICHTIGUNG DER STAATLICHEN VERANTWORTUNG STEHEN.

INHALTSVERZEICHNIS

1. VERTRAUENSWÜRDIGE ELEKTRONISCHE KOMMUNIKATION

Die Durchdringung öffentlicher Lebensbereiche mit Informationstechnologien nimmt stetig zu. Viele Bereiche des öffentlichen Lebens wären bereits heute ohne den Einsatz von IT kaum noch denkbar – sei es bei der Energieversorgung, der Kommunikation oder auch der organisationsübergreifenden Zusammenarbeit. Dem Staat fällt dabei eine immer komplexere Rolle hinsichtlich der Daseinsvorsorge zu. Insbesondere für die elektronische Kommunikation und Identifikation bildet der Faktor Vertrauen eine entscheidende Grundlage.

1.1 VERTRAUEN

Durch die wachsende Digitalisierung der Gesellschaft stehen viele Menschen einer immer höheren Komplexität ihrer Lebenswelten und einer zunehmenden Virtualisierung der sozialen Welt gegenüber. Dabei ist es häufig nicht möglich, alle technischen Hintergründe und Voraussetzungen zu verstehen. Vertrauen gewinnt somit zunehmend an Bedeutung als »Mechanismus der Reduktion sozialer Komplexität«.[1] Vertrauen wird zwar im täglichen Sprachgebrauch häufig auf die Qualität einer zwischenmenschlichen Beziehung beschränkt, ist aber ein elementarer Bestandteil des Lebens. Der Mensch ohne jegliches Vertrauen wäre nicht fähig, Kommunikation oder Kooperation zu vollziehen, wodurch es letztlich zu einer wichtigen Voraussetzung für die Nutzung öffentlicher IT wird.

Gerade bei elektronischer Kommunikation und der Erbringung elektronischer Dienste ist Vertrauen von herausragender Bedeutung. In einer Gesellschaft bildet es sich in einem kulturellen Prozess: es »wird von den jeweiligen Gewohnheiten, Sitten und Normen bestimmt – kurz gesagt von der Kultur«.[2] Vertrauen erfordert zunächst Zutrauen in die eigene Identität, darüber hinaus aber auch in die Kommunikationspartner und in deren Identitäten. Hinzu kommt bei der Digitalisierung der Beziehungen das Vertrauen in die zugrunde liegenden Technologien.

Bei elektronischer Kommunikation kann Vertrauen sowohl unidirektional als auch bidirektional gerichtet sein. Für die Bereitstellung von Informationen, z. B. auf einer Webseite, ist das Vertrauen in den Informationsbereitsteller ausreichend und damit unidirektional. Immer dann, wenn es jedoch um bidirektionale Kommunikationsbeziehungen geht, zum Beispiel zur Abwicklung von Geschäftsprozessen, muss es auf Gegenseitigkeit beruhen.

Digitale Identitäten sind ein entscheidender Baustein öffentlicher IT, die dieses Vertrauen im digitalen öffentlichen Raum schaffen und damit verlässliche Kommunikation ermöglichen. Wird das erreicht, spricht man von vertrauenswürdigen Identitäten. Sie bilden zukünftig eine immer wichtigere Grundlage für die Gesellschaft und unser Wirtschaftssystem. Darüber hinaus dienen sie dem Aufbau von Reputation, einem weiteren vertrauensbildenden Faktor im digitalen öffentlichen Raum. Vertrauenswürdige Identitäten sollen eine sichere Authentisierung möglichst unabhängig von bestimmten Endgeräten oder Diensten ermöglichen.

1.2 WAS SIND DIGITALE IDENTITÄTEN?

In der öffentlichen Diskussion werden digitale Identitäten oftmals mit Identitäten von Personen, die sich im Internet bewegen, gleichgesetzt. Eine klassische Definition von digitaler Identität beschreibt diese als »jede mögliche Form von technisch abgebildeten Daten, die zu einer Person gehören«.[3]

Die Digitalisierung des öffentlichen Raumes beinhaltet allerdings mehr als nur die Kommunikation zwischen Personen. Individuen kommunizieren über das Internet mit Organisationen und nutzen elektronische Dienste. Beim Online-Banking etwa werden Geschäftsprozesse elektronisch abgewickelt, die sehr hohe Anforderungen an die Vertrauenswürdigkeit der Interaktionspartner setzen.

Die Digitalisierung des öffentlichen Raumes geht aber noch einen Schritt weiter. Bereits heute ist es möglich, reale Objekte zu identifizieren, mit ihnen zu kommunizieren oder diese zu steuern. Mit neuen Technologien, die auf IPv6[4] beruhen, ist es theoretisch möglich, jedem Objekt mehrere weltweit eindeutige Internet-Adressen zuzuweisen.

[1] Luhmann, Niklas (2000): »Vertrauen: ein Mechanismus der Reduktion sozialer Komplexität.« 4. Auflage. Stuttgart: Lucius und Lucius, S. 41.
[2] Fukuyama, Francis (1995): »Trust. The Social Virtues and the Creation of Prosperity« New York: Free Press, S. 42. Übersetzung aus dem Englischen.
[3] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: »Verkettung digitaler Identitäten«, https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf, 2007.
[4] Kompetenzzentrum Öffentliche IT: »Fortschrittliche Netze: Fundament für öffentliche Informationstechnologie«, 2013.

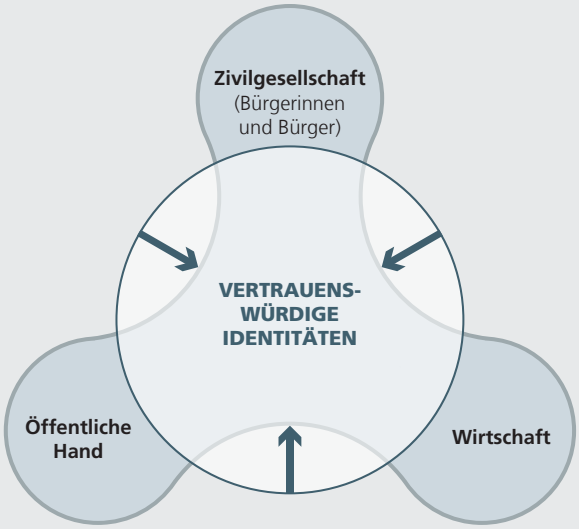

Abbildung 1: Vertrauenswürdige Identitäten im öffentlichen Raum

1

Unter dem Stichwort »Internet der Dinge« wird dieser Trend in Zukunft sowohl private als auch öffentliche Räume stark beeinflussen.[5]

Digitale Identitäten bilden einen entscheidenden Vertrauensanker zur Erkennung von Entitäten im digitalen Raum. Dazu gehören Personen, Organisationen, Dienste oder Objekte. Die klassische Definition muss daher um diese erweitert werden. Abbildung 2 stellt die vier Typen digitaler Identitäten grafisch dar.

»Digitale Identitäten sind Teilidentitäten einer realen oder einer Wunschidentität.«

Digitale Identitäten basieren auf einer Menge von Attributen. Wie auch in der realen Welt repräsentieren sie die Eigenschaften, Merkmale oder Präferenzen (Vorlieben, Interessen etc.) der ihr zugrunde liegenden Entität. Digitale Identitäten können sich über ihren Lebenszyklus hinweg verändern und dabei direkt oder indirekt, mit und ohne Wissen des Inhabers erstellt werden. Eine Entität kann mehrere Teilidentitäten beinhalten, die je nach Kontext eingesetzt werden. Bei Personenidentitäten sind zudem im digitalen Raum Wunschidentitäten zu finden, die von der realen Welt abweichen können.

Die Durchdringung persönlicher Lebenswelten mit öffentlicher IT führt zunehmend zu einem Wechselspiel digitaler und realer Identitäten. Beispielsweise hat ein Identitätsdiebstahl im Internet konkrete Auswirkungen auf die reale Lebenswelt einer Person. Werden etwa Kreditkarteninformationen gestohlen, hilft zumeist nur die Ausstellung einer neuen Kreditkarte.

[5] Siehe: Deutscher Bundestag, Wissenschaftliche Dienste: Aktueller Begriff Internet der Dinge, http://www.bundestag.de/dokumente/analysen/2012/Internet_der_Dinge.pdf, 2012.

1.3 WOZU WERDEN DIGITALE IDENTITÄTEN BENÖTIGT?

In der realen Lebenswelt stellen persönliche Begegnungen eine wichtige Grundlage der Vertrauensbildung dar. Dieses Vertrauens bedarf es auch in der digitalen Welt, deren digitale öffentliche Räume die Chance der persönlichen Begegnung nicht physisch ermöglichen. Daher ist es hier einfacher, eine scheinbare Vertrauenswürdigkeit vorzuspiegeln. Die Erfahrungen der Vergangenheit haben Bürgerinnen und Bürger ein gewisses Misstrauen bei der Nutzung von IT-basierten Diensten gelehrt.

Historisch betrachtet haben digitale Identitäten ihren technischen Ursprung in der Vernetzung von Personen. Bei der Kommunikation über Netzwerke benötigen die Kommunikationspartner eindeutige Adressen, bspw. sind für das Telefonieren eindeutige Telefonnummern oder im Internet eindeutige Internetadressen erforderlich. Sie waren die ersten technischen Attribute digitaler Identitäten.

Heute erfüllen digitale Identitäten eine wesentlich komplexere Aufgabe. Neben der Etablierung der technischen Kommunikation bilden sie die Grundlage für den Aufbau von Vertrauensbeziehungen und der Wiedererkennung von Nutzern. Sie sind ein wichtiger Baustein für die elektronische Verfahrensabwicklung, insbesondere für Geschäfts- und Verwaltungsprozesse. Sie dienen der Autorisierung bzw. Genehmigung von Aktionen im Internet, bspw. dem Kauf von Produkten, der Autorisierung von Finanztransaktionen oder auch dem Nachweis von Zugangsvoraussetzungen, wie etwa einer Altersbestätigung.

Vertrauenswürdige digitale Identitäten erfüllen also eine Fülle von unterschiedlichen Funktionen. Sie sollen Vertrauen aufbauen, die Grundlagen für eine elektronische Kommunikation und die Abwicklung von Geschäftsprozessen legen und müssen dabei zuverlässig, glaubhaft und zumindest innerhalb eines Kontextes eindeutig und ggf. rechtssicher sein.

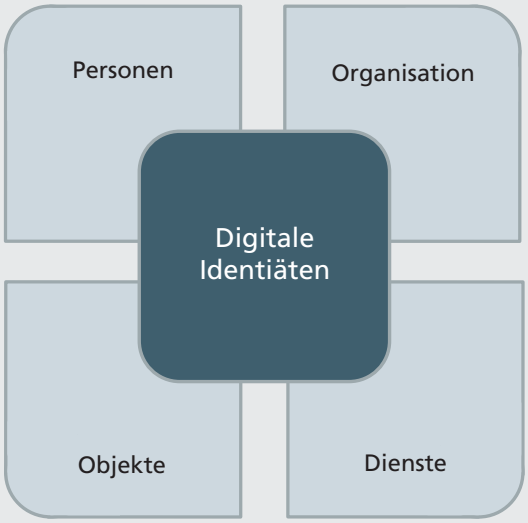

Abbildung 2:
Typen digitaler Identitäten

2

1.4 DIGITALE IDENTITÄTEN IN ÖFFENTLICHER IT

Im Kontext öffentlicher IT spielen digitale Identitäten eine zentrale Rolle. Wann immer Personen, Organisationen, Objekte oder Dienste im öffentlichen Raum miteinander kommunizieren, werden Mechanismen für sichere und vertrauenswürdige Identitäten benötigt. Sicher und vertrauenswürdig bedeutet in diesem Fall nicht die vollständige Offenlegung persönlicher Daten, sondern lediglich die Sicherstellung ihrer Authentizität. Für Personen ist dabei der Grad der Anonymität häufig Gegenstand gesellschaftlicher Debatten. Er gibt an, mit welchem Aufwand es möglich ist, auf eine reale Identität schließen zu können. Der Grad der Anonymität bestimmt zugleich den Grad der Privatheit. Er variiert dabei von vollständig anonym über pseudonym, teilweise anonym bis hin zu eindeutig identifiziert. So wie wir uns heute in physischen öffentlichen Räumen mit einem angemessenen Grad an Anonymität sicher bewegen können, muss es diese Formen auch im digitalen öffentlichen Raum geben.

»So wie es heute in der analogen Welt Orte der Privatheit gibt, muss es diese auch im digitalen Raum geben.«

Betrachtet man den Umgang mit Identitäten im digitalen öffentlichen Raum, so trifft man auf eine Reihe von Individuallösungen, oftmals geschaffen für einen speziellen Anwendungszweck. Das Niveau von Sicherheit und Datenschutz variiert dabei stark. Da solche Lösungen immer nur für einen spezifischen Zweck entwickelt werden, sind sie nur selten gegen Nebeneffekte aus missbräuchlicher Verwendung abgesichert. Ein Beispiel dafür ist die Kennung von Drahtlosnetzwerken (WLAN). Diese Kennung wird per Funk in der Umgebung verteilt, um Geräte drahtlos über ein Netzwerk zu verbinden. Nicht berücksichtigt wurde bei der Entwicklung, dass bei einer flächendeckenden Verbreitung von Drahtlosnetzwerken auch eine Ortung auf Grundlage eben dieser Kennung (ESSID) möglich ist. Unternehmen machen sich dies zunutze und erstellen darauf aufbauend Landkarten von Drahtlosnetzwerken. Ortsabhängige Anwendungen sind dann nicht mehr auf GPS Daten angewiesen, sondern müssen nur das Drahtlosnetzwerk kennen, um die Position zu bestimmen. Diese neue Möglichkeit der Ortung bietet Chancen, aber auch Risiken, die nun nachträglich in jedem Drahtlosnetzwerk individuell zu betrachten sind.

Da elektronische Kommunikation zwangsläufig immer über eine technische Infrastruktur erfolgt, sind Mechanismen der Vertrauensbildung bereits bei der Konzeption der ihr zugrunde liegenden Systeme miteinzubeziehen. Für zukünftige Entwicklungen bedarf es daher gemeinsamer Kriterien und Prinzipien zum Umgang mit digitalen Identitäten. Die folgenden Grundgedanken sollten dabei bedacht werden.

Ein wichtiger Grundsatz bei der Konzeption von Identitätstechnologien für bidirektionale Kommunikation ist die Gegenseitigkeit, d. h., Identitätsinformationen werden von beiden Seiten in angemessener Form offengelegt. Erste Technologien und Algorithmen dafür existieren bereits, müssen aber weiterentwickelt werden. Darüber hinaus ist es wichtig, die Preisgabe von Informationen immer dem Kontext angemessen erfolgen zu lassen, also dem Prinzip der Datensparsamkeit zu genügen. Außerdem sollten die zugrunde liegenden Verfahren für die Nutzer transparent und verständlich gestaltet sein. Um elektronische Geschäftsprozesse zu ermöglichen, ist zudem die Vertrauenswürdigkeit der Identitäten und Verfahren sicherzustellen. Zudem bedarf es einheitlicher Vorgaben zum Verwendungskontext der Identitätsinformationen (bspw. privat, öffentlich oder eingeschränkt auf einen definierten Nutzerkreis). Diese Grundsätze gelten für alle Formen digitaler Identitäten, also Personen, Organisationen, Dienste und Objekte. Im Mittelpunkt steht dabei immer die Selbstbestimmtheit des Nutzers.

DIGITALE IDENTITÄTEN SIND EINE MENGE VON ATTRIBUTEN DIE ZU EINER ENTITÄT GEHÖREN. ENTITÄTEN KÖNNEN PERSONEN, ORGANISATIONEN, DIENSTE ODER OBJEKTE SEIN.

1.5 DIE ROLLE DES STAATES

Die Rolle des Staates bei digitalen Identitäten kann je nach Kontext variieren und ist unter verschiedenen Sichtweisen zu betrachten.

Die primäre Rolle des Staates ist die des Rahmengebers. Mit rechtlichen Vorgaben und Richtlinien können Nutzung, Verwendung und Sicherheitsniveaus je nach Kontext definiert werden. Dazu zählen Datenschutzvorgaben genauso wie IT-Sicherheitsrichtlinien, aber auch die Entwicklung und Vorgabe von Standards stellen eine Möglichkeit der Rahmengebung dar. Im Kontext der elektronischen Verwaltung geschieht dies bspw. mit »XML in der öffentlichen Verwaltung« (XÖV), SAGA[6] oder den technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Darüber hinaus tritt der Staat als Identitätsanbieter auf. Bei Personen erfolgt dies in Form von Pässen oder Ausweisen, wie dem neuen Personalausweis und seiner Online-Ausweisfunktion. Auch für wirtschaftliche Einrichtungen tritt der Staat als Identitätsanbieter auf, beispielsweise mit dem Gewerbe- oder Handelsregister. Selbst für Objekte werden staatliche Identitäten vergeben, wenn auch bislang nur in Teilbereichen. Amtliche Kennzeichen aus dem Kfz-Bereich oder Schifffahrtswesen sind ein Beispiel dafür. Der Bedarf, diese Identitäten auch in elektronischer Form bereitzustellen, wird zukünftig steigen.

Des Weiteren kann der Staat in bestimmten Bereichen die Rolle eines Infrastrukturbetreibers einnehmen. Dies erfolgt in der Regel dann, wenn ein privatwirtschaftlicher Betrieb beispielsweise aus rechtlichen Gründen nicht möglich ist. So betreibt der Staat im Rahmen des neuen Personalausweises den hoheitlichen Bereich der Public-Key-Infrastruktur (PKI), also der Infrastruktur, die das Vertrauen in die Technologie und die Identitäten gewährleistet.

[6] Siehe: SAGA, http://www.cio.bund.de/DE/Architekturen-und-Standards/SAGA/Hintergrund/saga_hintergrund_node.html

2. HERAUSFORDERUNGEN

Zu den zentralen Herausforderungen öffentlicher IT zählen heute Themen wie Sicherheit, Datenschutz, vertrauenswürdige Kommunikation oder auch der Schutz der Privatsphäre. Vertrauenswürdige Identitäten müssen diese Aspekte adressieren und bilden eine wichtige Voraussetzung zum Erreichen dieser Ziele. In den folgenden Abschnitten werden einige Herausforderungen beschrieben, denen sich Entwickler, Betreiber oder Nutzer öffentlicher IT heute ausgesetzt sehen. Sie lassen auf vielfältigen Handlungs- und Forschungsbedarf schließen.

2.1 SICHERHEIT UND DATENSCHUTZ

Mit der zunehmenden Vernetzung und den dadurch entstehenden Abhängigkeiten von IT-Systemen steigt der Schutzbedarf von Infrastrukturen und darauf aufbauender Systeme. Informationstechnologien gelten heute als neuralgischer Punkt. Sie sind nicht nur komplex, sondern aufgrund ihrer Offenheit immer schwerer abzusichern.

Mit Sicherheitskonzepten, Risikoanalysen und Datenschutzkonzepten versucht man, diese Komplexität zu strukturieren und handhabbar zu machen. Oftmals handelt es sich dabei jedoch um eine Momentaufnahme, d. h., es werden die zu diesem Zeitpunkt bekannten Angriffsmuster und typischen Schwachstellen analysiert. Eine fortlaufende Analyse und Weiterentwicklung ist aufwändig, aber unerlässlich. Nicht betrachtete oder neue Bedrohungen führen dabei häufig zu hohen Anpassungserfordernissen.

Angesichts des oftmals unterlassenen Aufwandes ist es nicht verwunderlich, dass mittlerweile jeder zweite Internetnutzer Erfahrungen mit kriminellen Vorfällen im Internet gemacht hat. Dies zeigen Statistiken des Verbandes BITKOM aus dem Jahr 2012.[7] Ein beachtlicher Teil der Internetkriminalität entfällt auf den Bereich Diebstahl von Personenidentitäten.

Herkömmliche technische Verfahren zur Etablierung vertrauenswürdiger elektronischer Kommunikation stoßen zunehmend an ihre Grenzen. Das auch heute noch am weitesten verbreitete Verfahren zum Nachweis von Personenidentitäten ist eine Kombination aus Benutzername und Passwort, obwohl das Sicherheitsniveau hier als gering einzustufen ist. Bei diesem Verfahren handelt es sich um eine sogenannte Ein-Faktor-Authentisierung, d. h. mit nur einem Faktor, nämlich dem Wissen um ein Passwort, kann eine digitale Identität bestätigt werden. Das Verfahren ist einfach und universell einsetzbar, allerdings auch sehr leicht angreifbar und damit für Anwendungsfälle mit sensiblen Transaktionen unsicher und unzureichend.

Um die Sicherheit etwas zu erhöhen, wird bspw. empfohlen, alle drei Monate jedes Passwort zu ändern,[8] was weder praxisnah noch nutzerfreundlich ist. Die Verfahren zur Abbildung digitaler Personenidentitäten müssen in Zukunft höheren Ansprüchen genügen und dabei mehrere unabhängige Faktoren zur Authentisierung einbeziehen. Neben dem Faktor Wissen (Geheimnis, z.B. Passwort oder PIN), stehen hier noch die Faktoren physischer Besitz (bspw. Besitz einer Karte) und Biometrie (unveränderliches körperliches Merkmal) zur Verfügung.

Neben den offensiven Angriffen auf persönliche Daten bestehen für die Nutzer öffentlicher IT-Systeme jedoch noch weit mehr Herausforderungen. Die Technik macht es heute möglich, jede Nutzung öffentlicher IT-Systeme nachzuverfolgen und langfristig zu speichern. Ein Eintrag in einem sozialen Netzwerk, ein Einkauf oder eine Bewertung in einem Online-Shop stellt einzeln betrachtet kaum ein Risiko dar. In der Kombination und langfristigen Beobachtung liefern sie jedoch oft ein sehr genaues Bild über eine Person, oftmals ohne dass die betroffenen Personen darüber informiert sind.[9]

[7] BITKOM: »Pressekonferenz von BITKOM und BKA; Cyberkriminalität und IT-Sicherheit«, http://www.bitkom.org/files/documents/Praesentation_PK_BITKOM_BKA_IT-Sicherheit_17_09_2012.pdf, 2012.
[8] BITKOM: »Deutsche sind ihren Passwörtern zu treu«, http://www.bitkom.org/64370_64365.aspx, 2010.
[9] Beispiel 1: Zeit Online: »Was du twitterst, verrät wer du bist«, http://www.zeit.de/digital/internet/2013-06/twitter-psychologie-persoenlichkeit, 2013.
Beispiel 2: Michal Kosinski, David Stillwell, Thore Graepel »Private traits and attributes are predictable from digital records of human behavior« in Proceedings of the National Academy of Sciences of the United States of America, http://www.pnas.org/content/early/2013/03/06/1218772110, 2013.

TECHNISCHE LÖSUNGEN FÜR DIGITALE IDENTITÄTEN ERFORDERN IMMER EINE GESELLSCHAFTLICHE DEBATTE UM NUTZEN, SICHERHEIT UND DATENSCHUTZ IN EINKLANG ZU BRINGEN.

Darüber hinaus ist der Weg, den Informationen über öffentliche Netze wie das Internet nehmen, häufig nicht abgesichert, sodass das Abhören an Knotenpunkten durchaus möglich ist. Das systematische Abhören und Sammeln von Daten stellt nicht nur eine Bedrohung für den einzelnen Nutzer dar, sondern auch für die Wirtschaft, die in einem erheblichen Maß von elektronischer Kommunikation abhängig ist. Gerade global agierende Unternehmen benötigen Mechanismen zur sicheren und vertrauenswürdigen internen und externen Kommunikation.

2.2 VERNETZUNG VON OBJEKTEN

Mit der steigenden Automatisierung und Vernetzung öffentlicher IT rücken digitale Identitäten von Objekten und Diensten zunehmend in den Fokus der Betrachtung. Vernetzte Industrieanlagen und öffentliche IT-Infrastrukturen sind oftmals besonders gefährdet, da Störungen in diesen Systemen große Auswirkungen haben können,[10] wovon auch Bürgerinnen und Bürger direkt betroffen sind.

»Die zunehmende Vernetzung von Objekten erfordert einen Vertrauensraum, der rechtlich geregelt und technisch konzipiert werden muss.«

Darüber hinaus zeigen Trends bereits heute die zunehmende Automatisierung der Umgebung, sei es bei der Heimautomatisierung, der Kommunikation im Straßenverkehr – zwischen Autos und der Verkehrsinfrastruktur – oder auch der Vernetzung von Alltagsgegenständen. Diese Objekte interagieren künftig mit einer Reihe unterschiedlicher Kommunikationspartner. Die Absicherung dieser Kommunikation und die Schaffung eines Vertrauensraumes zu und zwischen den Objekten ist dabei ein zentrales Thema. Neben technischen Fragestellungen sind auch insbesondere rechtliche Aspekte zu erörtern.

Der Bedarf an sicheren Identitätslösungen für Objekte wird daher in Zukunft weiter steigen. Hierbei müssen auch gesellschaftliche Debatten geführt werden, um Nutzen, Sicherheit und Datenschutz miteinander in Einklang zu bringen.

2.3 INTEROPERABILITÄT

Eine weitere Herausforderung öffentlicher IT-Systeme ist deren Interoperabilität, also die Fähigkeit mit anderen Systemen zusammenzuarbeiten. Dadurch werden Mehrwerte geschaffen, teure Insellösungen vermieden und bewährte Verfahren langfristig nutzbar gemacht. Interoperabilität benötigt einheitliche und übergreifende Standards. Aber auch ein gemeinsames Verständnis und abgestimmte rechtliche Rahmenbedingungen stellen wichtige Voraussetzungen für die Interoperabilität dar.

Obwohl es auch im Bereich digitaler Identitäten bereits technische Standards gibt,[11] zeigt sich, dass gerade das Identitätsmanagement in vielen Bereichen noch eine Individualentwicklung ist. In Europa existieren derzeit eine Reihe von nationalen Identitätsdokumenten mit elektronischen Funktionen. Trotz schon bestehender Standards müssen diese teilweise sehr unterschiedlichen Ansätze harmonisiert werden. Dabei zeigt sich, dass weniger die technischen als vielmehr die rechtlichen Rahmenbedingungen die größten Herausforderungen darstellen.

[10] Beispiel: Heise Online: »Kritische Schwachstelle in hunderten Industrieanlagen«, http://www.heise.de/-1854385.html, 2. Mai 2013.
[11] Beispiele: SAML, OpenID, diverse ISO-Standards, European Citizen Card und viele weitere.

AUF EUROPÄISCHER UND INTERNATIONALER EBENE BEDARF ES VERGLEICHBARER KRITERIEN FÜR DIE VERTRAUENSWÜRDIGKEIT VON DIENSTEN.

2.4 VERGLEICHBARE KRITERIEN

Digitale Identitäten sind ein elementarer Baustein öffentlicher IT-Systeme und bilden einen entscheidenden Vertrauensanker, um Sicherheit zu gewährleisten. Dabei wird es zunehmend wichtiger, vergleichbare Kriterien zur Beurteilung der Sicherheit und des Vertrauensniveaus für die verwendeten Technologien und Verfahren zu etablieren. Sie helfen bei der Auswahl von geeigneten Verfahren für einen bestimmten Anwendungsfall. Derartige Kriterienkataloge werden bereits von verschiedenen Organisationen erstellt.[12] Diese sind jedoch sehr unterschiedlich und lassen eine Vergleichbarkeit nur bedingt zu.

In einer global vernetzten Welt sind lokale oder regionale Regelungen oftmals nicht ausreichend. Auf europäischer und internationaler Ebene bedarf es daher vergleichbarer Kriterien für die Vertrauenswürdigkeit von Diensten. Damit im Zusammenhang stehen gemeinsame technische Standards, vergleichbare Mechanismen und Vorgehensweisen zur Bewertbarkeit der Authentisierung sowie gemeinsame Rahmenbedingungen, auch für den Umgang mit Identitätsmissbrauch und den dadurch entstehenden Haftungsrisiken. Dies gilt für digitale Identitäten von Personen genauso wie für Objekt-, Organisations- und Dienstidentitäten.

[12] Beispiele: BSI IT-Grundschutz, ISO/IEC 27034-1:2011, Kantara Initiative: Identity Assurance Framework.

3. AKTUELLE ENTWICKLUNGEN

Den oben beschriebenen Herausforderungen wird versucht, mit unterschiedlichen Ansätzen zu begegnen. Im Folgenden werden einige aktuelle Entwicklungen aus dem staatlichen und privatwirtschaftlichen Umfeld beschrieben. Generell kann man unterscheiden in digitale Identitäten für Personen, Dienste und Organisationen, sowie für Objekte. Während im Bereich digitaler Identitäten für Personen und Dienste, teilweise auch für Organisationen, bereits viele Erfahrungen vorliegen und diverse technische Lösungen existieren, ist der Bereich der Objektidentitäten noch relativ neu, sodass dieser Aspekt hier separat behandelt wird.

3.1 DIGITALE IDENTITÄTEN FÜR PERSONEN, DIENSTE UND ORGANISATIONEN

Seit 2010 stellt der deutsche Staat seinen Bürgerinnen und Bürgern mit dem neuen Personalausweis eine elektronische Identität aus. Seit dem 1. September 2011 gibt es zudem den elektronischen Aufenthaltstitel für Drittstaatsangehörige mit Wohnsitz in Deutschland. Beide Dokumente sind mit einem elektronischen Chip ausgestattet und erlauben damit das »Sichausweisen« im Internet. Ermöglicht wird dies durch die Online-Ausweisfunktion, die der gegenseitigen Authentisierung von Partnern bei Geschäftsprozessen im Internet dient. Eine der herausragenden Eigenschaften ist dabei der gegenseitige Identitätsnachweis, d. h., sowohl Nutzer als auch Anbieter eines Dienstes weisen sich einander aus. Realisiert wird dies durch ein staatliches Zertifikat, dem Berechtigungszertifikat, das den Anbieter zum Auslesen bestimmter Daten berechtigt. Diese Berechtigung bildet die elektronische Identität einer Organisation bzw. eines Dienstes ab. Der Chip im Ausweis prüft technisch, ob die Organisation bzw. der Dienst berechtigt ist, die Daten auszulesen. Die Berechtigung garantiert, dass der Anbieter nur die Daten auslesen kann, die für seinen jeweiligen Prozess erforderlich sind.

Außerdem müssen Anbieter bestimmte Mindestanforderungen an Datenschutz und Datensicherheit gewährleisten. Für jedes Auslesen wird zudem die aktive Zustimmung des Inhabers benötigt. Dies erfolgt durch die Eingabe einer sechsstelligen Geheimnummer (PIN). Nur wenn der Anbieter berechtigt ist und der Nutzer per Häkchen für jede Datenkategorie zugestimmt hat, gibt der Ausweis die Daten frei. Mit der Kombination aus Ausweiskarte (Besitz) und Geheimnummer (Wissen) ist eine Zwei-Faktor-Authentisierung gegeben, die ein hohes Sicherheitsniveau erreicht.

Für öffentliche IT-Systeme bietet die Online-Ausweisfunktion eine sichere Alternative zu heutigen Registrierungs-, Identifizierungs- und Login-Prozessen. Die hohe Sicherheit hat jedoch auch ihren Preis. Die Nutzerfreundlichkeit ist an vielen Stellen noch ausbaufähig und stellt besondere Anforderungen an die Nutzer, wie den Einsatz eines geeigneten Kartenlesegeräts, um den Ausweis zuhause nutzen zu können.[13]

Eine weitere staatliche Lösung ist der E-Mail-Dienst De-Mail. De-Mail ist ein Pendant zur klassischen E-Mail und erweitert diese um Aspekte der Vertraulichkeit, Nachweisbarkeit und Identität. De-Mails sind automatisch verschlüsselte E-Mails, deren Versand und Erhalt rechtssicher nachweisbar sind. Um De-Mails senden oder empfangen zu können, benötigen beide Kommunikationspartner eine De-Mail-Adresse. Bei der Registrierung dieser Adresse ist eine rechtssichere Identifikation der natürlichen Person notwendig, wo für bspw. die Online-Ausweisfunktion genutzt werden kann.

De-Mail liegt ein Gesetz des Bundes sowie eine Sammlung technischer Spezifikationen und Vorgaben des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) zugrunde, die von den Produkten der privatwirtschaftlichen Anbieter eingehalten werden müssen. Die Anbieter müssen dazu einen Zertifizierungsprozess durchlaufen und können anschließend ein geeignetes Geschäftsmodell darauf aufbauen. Die Einhaltung der Vorgaben wird regelmäßig durch das BSI geprüft.

Neben dem sicheren und nachvollziehbaren Versand von elektronischen Nachrichten bietet De-Mail weitere Zusatzdienste an. Obwohl bereits mit dem neuen Personalausweis eine staatliche Infrastruktur für eine elektronische Identifikation geschaffen wurde, ermöglicht auch De-Mail eine weitere Möglichkeit der Identitätsfeststellung auf Grundlage eines vom De-Mail-Anbieter per De-Mail übermittelten Datensatzes. Außerdem

[13] Siehe: vertiefende White Paper zum neuen Personalausweis erhältlich unter: www.ccepa.de/whitepaper.

Abbildung 3: Gegenseitiger Identitätsnachweis mit der Online-Ausweisfunktion

wird ein Verfahren zur sicheren Aufbewahrung von Dokumenten definiert. Beide Zusatzdienste werden derzeit noch nicht produktiv angeboten.

Kritisiert wird zuweilen, dass das Verfahren De-Mail eine Ende-zu-Ende-Verschlüsselung nicht zwingend vorschreibt. Zwingend vorgeschrieben bei De-Mail ist die Verschlüsselung zwischen Nutzer und De-Mail-Anbieter, sowie zwischen den De-Mail-Anbietern, sodass De-Mails bei ihrer Übermittlung über das Internet immer verschlüsselt übertragen werden. Eine zusätzliche Ende-zu-Ende-Verschlüsselung zwischen zwei Nutzern ist möglich, wenn Nutzer zusätzliche Soft- und/oder Hardware auf ihren Endgeräten installiert haben.

Neben der Online-Ausweisfunktion und De-Mail gibt es in Deutschland bereits seit 2001 mit dem Signaturgesetz (SigG) die rechtlichen Rahmenbedingungen, um Dokumente elektronisch zu unterschreiben. Sogenannte qualifizierte elektronische Signaturen (qeS) mit den dafür notwendigen Signaturzertifikaten bilden das elektronische Pendant zur eigenhändigen Unterschrift und sind dieser in vielen Anwendungsfällen juristisch gleichgesetzt. Die Ausgabe der Signaturzertifikate erfolgt durch privatwirtschaftliche Unternehmen, die nach dem SigG ihren Dienst anzeigen müssen. Eine Akkreditierung dieser Unternehmen bietet ein zusätzliches Sicherheitsniveau. Obwohl die Rahmenbedingungen und die dazugehörigen Technologien seit mehr als 10 Jahren vorhanden sind, hat sich der Einsatz der qeS in der öffentlichen IT nur in wenigen Teilbereichen etabliert, bspw. dem elektronischen Gerichtsverkehr. Die Gründe dafür sind vielfältig. Zunächst sind die Signaturzertifikate teuer in der Anschaffung und rechnen sich dadurch nur für Vielnutzer. Ferner ist die Technologie komplex und stellt nicht unerhebliche Anforderungen an die Nutzer (Lesegeräte, Software, Geheimnummern, etc.).

Trotz dieser Technologien sind passwortbasierte Lösungen auch heute noch die am weitesten verbreiteten Mechanismen zur Identitätsbestätigung in öffentlichen IT-Systemen. Neue Lösungen müssen nicht nur hohen Sicherheitsanforderungen genügen, sondern auch kosteneffektiv und insbesondere einfach nutzbar sein.

Basierend auf offenen Standards wie bspw. OpenID können Alternativen zu passwortbasierten Logins angeboten werden. Das Konzept von OpenID sieht einen unabhängigen dritten Akteur als Identitätsanbieter vor, der die Identität eines Nutzers gegenüber einem Diensteanbieter bestätigt. Globale Unternehmen treten dabei in der Regel als OpenID-Identitätsanbieter auf. Soziale Netzwerke wie Facebook bieten mit proprietären Lösungen wie dem Facebook-Login eine ähnliche Form des Single-Sign-On für andere Webseiten an. Beide Lösungen basieren auf einer Ein-Faktor-Authentisierung, sodass das Schutzniveau nicht signifikant höher als bei passwortbasierten Lösungen ist. Trotz alledem sind entsprechende Lösungen global agierender Unternehmen weit verbreitet.

Sowohl die stark angestiegene Zahl von Cyberangriffen auf die Datenbestände der Unternehmen wie auch das relativ einfache Abfangen von Passwörtern für Laien, verstärkt auf beiden Seiten, bei Nutzern und Anbietern, das Interesse an sicheren Lösungen. In den letzten Jahren sind so eine Reihe neuer Initiativen und Aktivitäten im Bereich digitaler Identitäten entstanden.

Unternehmen wie Google,[14] Apple[15] oder Microsoft[16] arbeiten an eigenen Konzepten für eine Zwei-Faktor-Authentisierung. Übergreifende Lösungen werden in verschiedenen Verbünden erarbeitet. Die FIDO alliance bspw. entwickelt ein Identitätsma-

[14] Siehe: »A more secure cloud for millions of Google Apps users«, http://googleenterprise.blogspot.de/2010/09/more-secure-cloud-for-millions-of.html, 2010.
[15] Siehe: »Apple ID: Frequently asked questions about two-step verification for Apple ID«, http://support.apple.com/kb/HT5570, 2013.
[16] Siehe: »Microsoft Account Gets More Secure«, http://blogs.technet.com/b/microsoft_blog/archive/2013/04/17/microsoft-account-gets-more-secure.aspx, 2013.

TECHNOLOGIEN ZUM SCHUTZ DER KOMMUNIKATION MÜSSEN EINEN DIGITALEN RAUM SCHAFFEN, DER EINE VERTRAUENSVOLLE KOMMUNIKATION ERMÖGLICHT.

nagementsystem, das vollständig ohne Passwörter auskommen will. Im Rahmen der Initiative Liberty Alliance Project[17] haben ca. 150 Unternehmen, Forschungseinrichtungen und Organisationen bereits seit 2002 unterschiedliche Konzepte und Lösungen rund um digitale Identitäten erarbeitet. Diese Arbeiten werden nun im Kontext der Kantara Initiative[18] fortgeführt.

Die vielfältigen Entwicklungen zeigen den steigenden Bedarf an neuen Lösungen, insbesondere an Alternativen mit einem höheren Vertrauensniveau für digitale Identitäten. Dabei muss allerdings immer die rechtliche Grundlage bedacht werden.

3.2 DIGITALE IDENTITÄTEN FÜR OBJEKTE

Neben Personen, Organisationen oder Diensten werden auch die uns umgebenden Objekte zunehmend mit Identitäten versehen und vernetzt. Dieser Trend wird unter dem Stichwort »Internet der Dinge« zusammengefasst. Internet der Dinge bezeichnet einen Verbund von Objekten und Dingen des alltäglichen Lebens in einem Netzwerk und dessen Synthese unterschiedlicher Technologien. Häufig zum Einsatz kommen hier Funktechnologien wie RFID oder Drahtlosnetzwerke (WLAN), Sensorik oder auch Nanotechnologien.

So werden Gegenstände – markiert durch einen RFID-Tag – auch zu Objekten im virtuellen Raum, die ihren Weg durch das Internet der Dinge bspw. autonom finden oder auch die Systeme steuern, in denen sie sich bewegen. In der Logistik wird bereits seit Langem mit Objektidentitäten gearbeitet. Pakete, Paletten oder Behälter werden durch einen Chip gekennzeichnet, der neben Informationen zu Produkt und Datum zusätzlich auch das Transportziel speichert. So lassen sich Produktionsketten oder Kühlketten nachvollziehbar gestalten.

Die Vernetzung von Objekten beginnt im Endanwenderbereich. Viele Hersteller setzen auf diesen Trend und erstellen Produkte zur Heimautomatisierung, die über Smartphones oder das Internet gesteuert werden können. Hier kommen vielfältige Sensoren, fernsteuerbare Steckdosen und intelligente Haushaltsgeräte zum Einsatz. Im Bereich der Energie werden bereits heute viele Haushalte mit sogenannten Smart-Meter-Geräten ausgestattet. Der Einsatz dieser elektronischen Energie-Messsysteme ist bereits für viele Bereiche durch eine europäische Richtlinie[19] sowie nationale Gesetze vorgeschrieben. Jedoch bedarf es abgestimmter Datenschutz- und Datensicherheitsrichtlinien, um diese Systeme gegen Missbrauch zu schützen. Hier gibt es unterschiedliche nationale Regelungen.

Im Bereich der öffentlichen Infrastruktur steht vor allem das Verkehrswesen vor großen Veränderungen. Unter dem Stichwort »Car2X Kommunikation« wird intensiv an sicheren Kommunikationsmechanismen zwischen Fahrzeugen oder Fahrzeugen und anderen Systemen geforscht. Zielsetzung ist dabei die Sicherheit im Straßenverkehr sowie den Fahrkomfort zu erhöhen. Derartige Systeme sind bereits im produktiven Status. Eines der am weitesten entwickelten Systeme ist das eCall-System[20] (emergency call), ein automatisches Notrufsystem für Fahrzeuge. Die Europäische Kommission hat beschlossen, eCall bis 2015 EU-weit einzuführen. Notrufmeldungen können dabei automatisch oder manuell ausgelöst werden. Die Effektivität solcher Kommunikationsbeziehungen hängt aber stark von ihrer Vertrauenswürdigkeit ab.[21] Bereits vor der Einführung gibt es Interesse an einer Zweitnutzung des Systems zum Beispiel durch Versicherer. Dazu bedarf es sowohl kryptografischer

[17] Siehe: http://www.projectliberty.org
[18] Siehe: http://kantarainitiative.org/confluence/display/GI/Home
[19] Siehe: EU-Energieeffizienzrichtlinie (2012/27/EU): http://ec.europa.eu/energy/efficiency/eed/eed_de.htm
[20] Siehe: http://ec.europa.eu/information_society/activities/esafety/ecall/index_en.htm
[21] Siehe beispielhaft: Hendrik Schweppe, Yves Roudier, Benjamin Weyl, Ludovic Apvrille, Dirk Scheuermann: »Car2X Communication: Securing the Last Meter« in WIVEC 2011, 4th IEEE International Symposium on Wireless Vehicular Communications, http://www.eurecom.fr/en/publication/3422/download/rs-publi-3422.pdf, 2011

Mechanismen zur Absicherung der Kommunikation und sicherer Verfahren zur eindeutigen Identifikation als auch internationaler Standards und Richtlinien.

Das Internet der Dinge erstreckt sich jedoch noch weit über das Verkehrswesen hinaus. Im Kontext von »Smart Cities« werden grundlegende Infrastrukturen ganzer Städte vernetzt und mit Sensoren ausgestattet. So sollen Verkehr, Energie, Gesundheit, Umwelt und viele weitere Domänen eingebunden werden. Diese Vernetzung der Umgebung erfordert nicht nur klare Rahmenbedingungen, sondern auch vertrauensbildende Technologien, welche von Anfang an mitgedacht werden müssen.

Neue Technologien zum Schutz der Kommunikation müssen dazu einen digitalen Raum schaffen, der eine vertrauensvolle Kommunikation zulässt und neue Entwicklungen fördert. Ein solcher Vertrauensraum muss ad hoc kreiert werden können. Dafür bedarf es Strategien und Lösungen, die angemessene Vertrauensbeziehungen zwischen nahezu beliebigen Objekten ermöglichen. Dies kann nur durch die Definition übergreifender Standards und vergleichbarer Vertrauensniveaus und Sicherheitsstufen erreicht werden. Entsprechende technologische Entwicklungen existieren bereits. Mit Trusted Computing etwa wird ein Vertrauensanker in Form von nicht manipulierbarer Hardware in die Geräte verbaut, was die Manipulation und unberechtigtes Auslesen von Daten erschwert. Zusätzlich kann das Prinzip der fairen und gegenseitigen Identifikation als Grundlage für den Aufbau von Vertrauensräumen dienen.

Das Internet der Dinge bietet ein hohes Innovationspotenzial für die Zukunft. Die Kommunikation mit und zwischen Objekten sowie die Schaffung eines Vertrauensraumes stehen dabei im Vordergrund. Im Sinne öffentlicher IT müssen Individuallösungen vermieden und Identitätsmanagement als ein zentraler Baustein weiterentwickelt werden. Hier besteht unmittelbarer Forschungsbedarf. Interessante Ansätze aus etablierten Bereichen wie dem der Personenidentitäten können dabei als Vorbild dienen.

5. ACHT THESEN ZU DIGITALEN IDENTITÄTEN

Ausgehend von den bisherigen Betrachtungen werden in den folgenden Thesen zukünftige Anforderungen an digitale Identitäten und entsprechende Handlungsempfehlungen zusammengefasst.

- Die Ausgabe digitaler Identitäten darf nicht allein globalen IT-Unternehmen überlassen werden. Hier sind der Staat oder auch vertrauenswürdige Dritte gefordert. Mechanismen zur Etablierung vertrauenswürdiger Kommunikation sollten von marktwirtschaftlichen Interessen getrennt werden. Dies gilt im Übrigen auch für die Antithese: Muss der Staat in Konkurrenz zur Privatwirtschaft auftreten? Hier sind regelmäßige gesellschaftliche Debatten erforderlich.
- Heutige Verfahren wiegen den Nutzer zu oft in falscher Sicherheit. Falsche oder nicht-vertrauenswürdige Nachweise werden von den Nutzern häufig ignoriert oder nicht verstanden. Hier müssen neue Technologien gefördert werden, die einfach und verständlich sind. Mechanismen zum Schutz im Internet müssen global abgestimmt werden, um erfolgreich zu sein. Die Medienkompetenz der Bürgerinnen und Bürger muss frühzeitig gefördert werden.
- Anonymität und Pseudonymität müssen als legitime Konzepte gesellschaftlich etabliert und fundiert werden. Der Beigeschmack des »Ungesetzlichen« bzw. des »Verheimlichens« muss einem natürlichen Verständnis und Umgang mit diesen Konzepten weichen. Der Grad der Anonymität muss dem in der realen Welt entsprechen.
- Vertrauenswürdige Kommunikation erfordert eine gegenseitige Identifikation. Um eine vertrauensvolle bidirektionale Kommunikation zu ermöglichen, müssen Mechanismen der gegenseitigen Identifikation etabliert werden. Gegenseitiges Vertrauen wird nur dann erreicht, wenn ein fairer und ausgewogener Austausch von Identitätsinformationen stattfindet. Als Vorbild kann hier die Online-Ausweisfunktion dienen. Zukünftig werden verstärkt digitale Identitäten für Dienste und Objekte vergeben; auch hier muss dieser Grundsatz gelten.
- Für die Kommunikation mit Objekten werden Mechanismen zum Aufbau von Vertrauensräumen benötigt. Vertrauensräume sind digitale Räume, in denen alle Kommunikationspartner vertraulich und sicher kommunizieren können. Hier sind Staat, Wirtschaft und Forschung gleichermaßen gefragt, Regularien, Lösungen und Standards zu entwickeln, die einen schnellen und sicheren Aufbau von Vertrauensräumen ermöglichen.
- Zukünftig benötigen wir automatisierte Prozesse für den Umgang mit gestohlenen Identitäten. Viele Internet-Dienstleister sind heute global aktiv. Um tatsächlich ein wirkungsvolles Zurückziehen (Revoke) einer digitalen Identität umzusetzen, greifen nationale Alleingänge zu kurz. Daher sind international abgestimmte Rahmenbedingungen notwendig.
- Die Selbstbestimmtheit des Nutzers ist unantastbar. Jeder Nutzer muss die Möglichkeit haben, sich individuell seine eigene Teilidentität zu erstellen. Er muss frei entscheiden können, wem er welche Informationen zur Verfügung stellt. Die dem zugrunde liegenden Technologien und Verfahren müssen für den Nutzer verständlich sein.
- Neue Lösungen müssen global gedacht werden und internationalen Standards und Kriterien genügen. Der Erfolg künftiger Technologien erfordert die Schaffung und Einhaltung grenzüberschreitender einheitlicher Standards und Rahmenbedingungen. Es müssen gemeinsame Kriterien für Authentisierungsverfahren entwickelt werden, um eine Vergleichbarkeit und Interoperabilität gewährleisten zu können.

GEFÖRDERT VOM

Bundesministerium
des Innern

KONTAKT

Jens Fromm
Leiter Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
jens.fromm@fokus.fraunhofer.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de

kre | 13010 (Fotos: Matthias Heyde / Fraunhofer FOKUS)