Deutscher Bundestag **Drucksache 19/4987**

19. Wahlperiode 02.10.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Frank Sitta, Manuel Höferlin, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/4321 –

Digitale Identitäten

Vorbemerkung der Fragesteller

Digitale Identitäten bilden die Grundlage zum Handeln im Internet. Sie ermöglichen Onlinebanking-Konten, Zugang zu sozialen Medien, Einkäufe bei Onlinehändlern, aber auch Dateneinträge bei Bürgerämtern und vielen weiteren Onlinediensten. Daher ist es üblich, dass Bürger eine Vielzahl solcher Identitäten anhäufen. Zur einfacheren Verwaltung dieser digitalen Identitäten bieten US-amerikanische Unternehmen, wie Google, Facebook oder LinkedIn, auf ihren Plattformen sogenannte Single-Sign-On-Systeme an. Die bereits gespeicherten Daten der Nutzer, wie beispielsweise der Name, das Geschlecht oder das Geburtsdatum, werden dafür zentral auf den Servern dieser Unternehmen gespeichert und bei Bedarf an andere Dienste freigegeben. Eine solche zentrale Datenverwaltung schränkt die Datensouveränität der Nutzer ein.

Das Konzept der Self-Sovereign-Identity (SSI) ermöglicht ein solches Single-Sign-On-System zur Verwaltung unterschiedlicher Konten, während Nutzer allerdings stets die vollständige Kontrolle über ihre Daten behalten. Verschiedene Anbieter bieten dafür Apps an, die einen Datentresor auf einem Mobiltelefon einrichten. Die Verwaltung der digitalen Identität liegt daher nicht bei einer zentralen Instanz, sondern beim Nutzer selbst. Nutzer können so frei entscheiden, welche Daten mit welchem Dienst geteilt werden. Nachdem eine Behörde die hinterlegten Daten einmal verifiziert, kann so die digitale Identität für behördliche Leistungen wie zur digitalen Signatur der Steuererklärung, sowie zum Nutzen privater Dienste, wie dem Onlinebanking genutzt werden.

Als erste Stadt der Welt ermöglicht die schweizerische Stadt Zug ihren Bürgern eine blockchainbasierte digitale Identität (www.stadtzug.ch/digitale-id). Dabei werden die Daten nicht zentral auf einem Server, sondern ausschließlich auf dem Mobiltelefon der Nutzer, durch die dafür entwickelte uPort-App gespeichert. Da die gespeicherten Daten von der Einwohnerkontrolle der Stadt verifiziert werden, ermöglicht die digitale Identität den Zugang zu Behördenleistungen der Stadt, zum Ausleihen von Büchern in der Bibliothek, zum blockchainbasierten Fahrradverleih und zum digitalen Parking-Management. Weitere staatliche und privatdienstliche Leistungen sollen demnächst folgen.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 28. September 2018 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

1. Welche Rolle sieht die Bundesregierung für den Staat bei der Verwaltung digitaler Identitäten?

Die zweifelsfreie Feststellung der Identität ist die Basis einer jeden Vertrauensbeziehung, die wiederum allen elektronischen Geschäfts- und Verwaltungsprozessen zugrunde liegt. Die Bundesregierung sieht es als originäre staatliche Aufgabe, Identitäten von Bürgern zu verwalten und zu bestätigen. Dies gilt für die physische, wie auch die digitale Welt gleichermaßen. Solche Identitäten dienen in der Regel als Basis für abgeleitete Identitäten weiterer Systeme.

Bund und Länder stellen für die Abwicklung digitaler Onlineleistungen Nutzerkonten bereit, über die sich Nutzer für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich identifizieren können (§ 3 Absatz 2 des Onlinezugangsgesetzes, OZG). Darüber hinaus wird mit der Bereitstellung einer eID-Funktion im Personalausweis und elektronischen Aufenthaltstitel für die Bürger die Möglichkeit der sicheren, zweifelsfreien und einfachen Identifizierung bei Handel und Dienstleistungen geschaffen, wo immer der Anbieter eine solche Identifizierung für erforderlich hält.

2. Beschäftigen sich Mitarbeiter in Bundesministerien mit dem Thema digitaler Identitäten?

   Wenn ja, in welchen Bundesministerien sind diese Mitarbeiter angestellt, und wie viele Mitarbeiter pro Bundesministerium arbeiten konkret an diesem Thema?

   Wenn nein, warum nicht?

Mitarbeiterinnen und Mitarbeiter in Bundesministerien und in nachgeordneten Behörden befassen sich im Rahmen ihrer Linientätigkeit in unterschiedlichen Zusammenhängen mit digitalen Identitäten. Die Bundesregierung passt die Anzahl der Mitarbeiterinnen und Mitarbeiter in diesem Themengebiet bedarfsgerecht an. Auf Ebene der Ministerien verteilen sich diese wie folgt:

BMF	15
BMI	elf
AA	zwei
BMJV	zwei
BMEL	vier
BMG	sechs
BMWi	fünf.

Da die Befassung mit Identitätsmanagement ein integraler Bestandteil der Fachaufgabe bei der Registerführung ist, kann eine Aussage zu den Vollzeitäquivalenten für vorgenannte Zahlen nicht getroffen werden.

3. Wie schätzt die Bundesregierung ihre Rolle als vertrauenswürdiger Verifikationsanbieter für ein System zur Verwaltung digitaler Identitäten ein?

Die Bundesregierung sieht es als originäre staatliche Aufgabe, Identitäten von Bürgern zu verwalten und zu bestätigen. Dies gilt für die physische, wie auch die digitale Welt gleichermaßen. Solche Identitäten dienen in der Regel als Basis für abgeleitete Identitäten weiterer Systeme.

Die Bundesregierung hat mit der Bereitstellung einer eID-Funktion im Personalausweis und elektronischen Aufenthaltstitel für die Bürger die Möglichkeit der sicheren, zweifelsfreien und einfachen Identifizierung bei Handel und Dienstleistungen geschaffen, wobei dem Staat die Rolle der Identitätsprüfung und Bestätigung im Rahmen des Antrags- und Ausstellungsprozess zukommt. Die Bundesregierung hat über die Notifizierung nach eIDAS-Verordnung (Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG) die Voraussetzung geschaffen, dass diese Funktion europaweit für Verwaltungsdienstleistungen eingesetzt werden kann.

4. Plant die Bundesregierung eine Zusammenarbeit mit privaten Unternehmen, um ein vertrauenswürdiges System für die Nutzung von digitalen Identitäten zu schaffen?

   Wenn nein, warum nicht?

Die Bundesregierung ist interessiert an Vorhaben, mit denen gesetzeskonforme, datenschutzfreundliche, sichere und nutzerfreundliche elektronische Identifizierungs- und Authentisierungsmittel auf den Markt gebracht werden. In diesem Zusammenhang beobachtet die Bundesregierung auch die Entwicklung und den Aufbau von privatwirtschaftlichen Initiativen, die den Fokus auf vertrauenswürdige Systeme/Plattformen für die Nutzung von digitalen Identitäten legen.

Die Bundesregierung agiert dabei grundsätzlich marktneutral, der Austausch wird mit allen Unternehmen, die Produkte entwickeln, die die o. g. Kriterien erfüllen, gleichermaßen gepflegt.

5. Inwiefern wird die Ethereum Blockchain als eine angemessene Technologie für ein System zur dezentralen Verwaltung von digitalen Identitäten gesehen?

Ob bestimmte Blockchains für die Verwaltung digitaler Identitäten geeignet sind, hängt nicht nur von der gewählten Blockchain ab, sondern auch von dem vorgesehenen Konzept der Identitätsverwaltung. Eine pauschale Beantwortung der Frage ist daher nicht möglich. Bei öffentlichen Blockchains wie Ethereum sind alle hinterlegten Daten für jedermann einsehbar. Nicht nur wegen des Öffentlichkeitsfaktors ist äußerste Vorsicht geboten, dass keine personenbezogenen und personenbeziehbaren Daten in der Blockchain gespeichert werden. Sondern auch weil im Falle des Bestehens eines Änderungs- oder Löschungsanspruchs des Betroffenen nach der Datenschutz-Grundverordnung (DSGVO) eine nachträgliche Änderung oder Löschung von Daten aufgrund der Unveränderbarkeit der Blockchain nicht möglich wäre. Weitere technische Fragen sind bisher im Zusammenhang mit Blockchain-Technologie nicht ausreichend erforscht, dazu gehören zum Beispiel Anonymität der Nutzer, Langzeitsicherheit, Austausch veralteter Kryptoalgorithmen. Stand heute sind öffentliche Blockchains für die Verwaltung digitaler Identitäten im Allgemeinen nicht geeignet. Für Ethereum ergeben sich zudem Probleme aus mangelndem Datendurchsatz und Skalierbarkeit. Überlastungen des Ethereum-Netzwerks, führten in der Vergangenheit bereits zum Anstieg der Transaktionsgebühren auf zwischenzeitlich über 5 US-Dollar pro Transaktion sowie zu längeren Wartezeiten bis zu ihrer Bestätigung. Ein großflächiger Einsatz in der digitalen Verwaltung würde diese Skalierungsprobleme noch verschärfen. Nutzern könnte keine zeitnahe und kostentransparente Bearbeitung ihrer Transaktionen garantiert werden.

6. Werden andere zentrale oder dezentrale Technologien von der Bundesregierung für die Verwaltung von digitalen Identitäten in Betracht gezogen?

   Wenn ja, welche Technologien?

Bei der Etherum Blockchain oder vergleichbaren Systemen zugrundeliegenden Distributed-Ledger-Technologien (DLT) handelt es sich um eine vergleichsweise junge Technologie, deren Potenzial derzeit sehr schwer einzuschätzen ist. Die Anwendungen der Technologie befinden sich zum Großteil noch in der Erprobungsphase. Dennoch teilt die Bundesregierung grundsätzlich die Auffassung, dass sich die Distributed-Ledger-Technologie als innovative Technologie im Bereich der Identitätsverwaltung etablieren kann. Die Bundesregierung befindet sich im Dialog mit Entwicklern, Wissenschaft, Verbänden und Pilotanwendern, auch um potenzielle Anwendungen und Einsatzgebiete für Identitätsmanagement im eigenen Verantwortungsbereich zu identifizieren.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet, untersucht und erprobt zentrale und dezentrale Technologien zur Verwaltung von digitalen Identitäten in Bezug auf sicherheitstechnische Eigenschaften. Voraussetzung für die Verwaltung von digitalen Identitäten ist hierbei stets das Vorhandensein von vertrauenswürdigen digitalen Identitäten, wie die Onlineausweisfunktion des Personalausweises. Die Bundesregierung plant zudem elektronische Identitäten für ihre mobile Nutzung sicher auf mobilen Endgeräten speichern zu können. Zu diesem Zweck existieren bereits Projekte wie OPTIMOS, in denen eine Umsetzung konzipiert wird.

7. Kennt die Bundesregierung das Pilotprojekt der Stadt Zug in der Schweiz?

Die Existenz dieses Pilotprojektes ist bekannt.

8. Wie bewertet die Bundesregierung das Projekt?

Da die Bundesregierung nicht in das Pilotprojekt eingebunden ist, kann eine abschließende Bewertung erst nach Abschluss des Pilotprojektes erfolgen, sofern die Projektergebnisse in ausreichender Detailtiefe publiziert werden.

9. Kann die Bundesregierung sich den Einsatz von blockchainbasierten Systemen für digitale Identitäten in Deutschland vorstellen?

   Wenn ja, plant die Bundesregierung regionale Pilotprojekte, um den Einsatz von digitalen Identitäten auf der Blockchain zu prüfen?

   Wenn nein, warum nicht?

Ein Grundgedanke der Blockchain-Technologie ist, Vertrauen und Transaktionstransparenz in einer Gruppe von Akteuren ohne eine vertrauenswürdige Instanz zu etablieren. In allen Anwendungsbereichen für elektronische Identitäten in der öffentlichen Verwaltung ist allerdings eine vertrauenswürdige Instanz vorhanden oder sogar gesetzlich vorgeschrieben. Besonders unter den spezialgesetzlichen Anwendungen sind keine, die derzeit ohne eine zentrale Instanz auskommen könnten. Auch der Einsatz einer privaten Blockchain kann diese Diskrepanzen nicht vollständig auflösen. Datenschutzrechtliche Grundsätze wie Vertraulichkeit und die Rechenschaftspflicht, aber auch Betroffenenrechte, inklusive dem Recht auf Berichtigung personenbezogener Daten und dem Recht auf Vergessenwerden, können nur umgesetzt werden, wenn von der ursprünglichen Idee einer dezentral verwalteten Datenbank abgewichen wird. Der ursprüngliche Vorteil der Blockchain als eine Technologie, die kryptografische Garantien für die Integrität

und Aktualität gespeicherter Daten bietet, relativiert sich hierdurch. In der Form einer „permissioned redactable Blockchain“ unterscheidet sich die Blockchain nur noch unwesentlich von herkömmlichen Methoden der kryptografisch abgesicherten und redundanten Speicherung. Die Bundesregierung ist im Austausch mit der Initiative „Blockchain in der Verwaltung Deutschland“, die sich mit digitalen Identitäten auf der Blockchain auseinander setzt.

10. Sieht die Bundesregierung datenschutzrechtliche Bedenken in Bezug auf die Verwendung von SSIs oder digitale Identitäten?

    Wie schätzt die Bundesregierung das Potential von SSIs zur Datenminimierung im Internet ein?

Die sinnvolle Verwendbarkeit von Server Side Includes (SSI) im Kontext sicherer digitaler Identitäten ist ein umfangreicher Themenkomplex, der noch ergebnisoffen diskutiert wird. Dezentral gespeicherte digitale Identitäten sind grundsätzlich dazu geeignet die Menge an Daten in zentralen Registern zu reduzieren. Bei einer solchen Minimierung ist allerdings immer die Qualität des Schutzes der persönlichen Daten zu berücksichtigen. Die Bundesregierung beobachtet die aktuellen Entwicklungen mit Interesse.

Eine im Rahmen des Förderprogramms Smart Data vom Bundesministerium für Wirtschaft und Energie (BMWi) in Auftrag gegebene Studie zum ISÆN Konzept (Individual perSonal data Auditable addrEss Number) weist das Potential der Distributed Ledger Technologie im Bereich selbstverwalteter sicherer Identitäten (Self-Sovereign-Identities) aus. Dennoch bleiben technische und rechtliche Fragen offen, wie beispielsweise die Berücksichtigung rechtlicher Vorgaben der Datenschutzgrundverordnung oder der eIDAS Verordnung. Bei dezentralen bzw. betreiberlosen Blockchains kann nach derzeitiger Rechtslage (z. B. wie in Artikel 24 Absatz 2 Buchstabe c der eIDAS-Verordnung gefordert) keine Haftung durch eine definierte Stelle sichergestellt werden.

11. Bedarf es der Einschätzung der Bundesregierung nach einer Definition von Standards für das Angebot von SSI und digitalen Identitäten?

    Wenn nein, warum nicht?

Die Bundesregierung befürwortet eine internationale, technologieoffene Standardisierung für die Sicherheitsaspekte von digitalen Identitäten, einschließlich SSI. Eine weltweite, international anerkannte Standardisierung etwa im Rahmen des bei der Internationalen Organisation für Normung (ISO) im April 2017 gegründeten neuen technisches Komitee für „Blockchain and distributed ledger technologies“ (ISO/TC 307) erscheint jedoch nur mit einer sehr langfristigen Perspektive realistisch. Deshalb sollte eine Standardisierung innerhalb der Europäischen Union (etwa im Kontext von und aufbauend auf der eIDAS Verordnung oder der CENELEC „Focus Group Blockchain“) erfolgen. Daneben ist in Einzelfällen auch die Mitwirkung in internationalen Industriekonsortien (wie z. B. der FIDO Allianz, Fast IDentity Online) zweckmäßig.

12. Steht die Bundesregierung in Kontakt oder verhandelt bereits über Möglichkeiten, wie Standards zu digitalen Identitäten weltweit untereinander kompatibel ausgestaltet werden können?

Für den digitalen EU-Binnenmarkt ist die gegenseitige Anerkennung der elektronischen Identifizierungsmittel der Mitgliedstaaten auf Basis der eIDAS-Verordnung (Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG) geregelt.

Dabei verfolgt die eIDAS-Verordnung das Ziel der Interoperabilität der nationalen Identifizierungssysteme. Aus Sicht der Bundesregierung ist das Konzept der gegenseitigen Anerkennung als Basis für eine weltweite Kompatibilität nationaler Identitäten grundsätzlich geeignet.

13. Bedarf es der Einschätzung der Bundesregierung nach rechtlicher Neuregelungen, um die im Zusammenhang mit Blockchainanwendungen verwendeten Signaturen und den Beweiswert von Blockchaineinträgen anzuerkennen?

Wenn ja, welche?

Und arbeitet die Bundesregierung bereits an solchen Neuregelungen?

Wenn nein, durch welche rechtlichen Regelungen können in Blockchainanwendungen verwendete Signaturen und der Beweiswert von Blockchaineinträgen heute schon rechtlich anerkannt werden?

14. Bedarf es der Einschätzung der Bundesregierung nach einer neuen rechtlichen Definition von Merkmalen oder Eigenschaften, die geeignet sind, um sich als natürliche oder juristische Person komplett digital auszuweisen?

Die Fragen 13 und 14 werden im Zusammenhang beantwortet.

Die Überprüfung und Anpassung des Rechtsrahmens ist eine Daueraufgabe der Bundesregierung. Ziel der Bundesregierung ist es, einen technologieneutralen, innovations- und investitionsfreundlichen Rechtsrahmen zu gewährleisten. Soweit ein konkreter Rechtsänderungsbedarf erkannt wird, legt die Bundesregierung entsprechende Vorschläge dem Deutschen Bundestag vor.

15. Sieht die Bundesregierung über die Identifizierung von Personen hinaus ein von Staat und Verwaltung verwertbares Potential von SSI und digitalen Identitäten für die Authentifizierung von Geräten oder anderen Sachen im Rechtssinne?

Eine besondere Herausforderung stellt in diesem Bereich das Vordringen des „Internet of Things“ dar. Schon jetzt sind etwa sechs Milliarden Geräte mit dem Internet verbunden, bis zum Jahr 2020 könnte diese Zahl sogar auf 50 Milliarden steigen. „Dinge“ erhalten eigene digitale Identitäten, Nutzer verknüpfen ihre eigene digitale Identität mit den Geräten. Die Identität des Nutzers wird damit zur Massenware.

Hier gilt es, die Einhaltung der datenschutzrechtlichen Vorgaben sicherzustellen, u. a. muss für die Nutzer transparent sein, wo welche Daten auf welcher Grundlage und zu welchen Zwecken gespeichert werden und wer für ein Gerät bzw. die damit verbundene Datenverarbeitung verantwortlich ist. Die Bundesregierung sieht in der Verwendung von SSI ein Potential, diese Probleme in den Griff zu bekommen.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333