Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)58

4.07.2022

Innenausschuss des Deutschen Bundestages

nur per E-Mail

Freie Universität Berlin

Fachbereich Mathematik und Informatik
ID-Management

Prof. Dr. Marian Margraf
Takustraße 9
14195 Berlin

+49 30 838 75-245
marian.margraf@fu-berlin.de

01.07.2022

Betr.: Öffentliche Anhörung digitale Identitäten des Digitalausschusses am 04. Juli 2022

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur öffentlichen Anhörung. Gern übersende ich Ihnen vorab meine Stellungnahme in schriftlicher Form. Leider kann ich auf Grund der kurzen Frist aber nicht alle Fragen im Detail beantworten.

Meines Erachtens werden Bürger*innen digitale Identitäten nutzen, wenn sich dadurch für sie Prozesse deutlich vereinfachen. Hierzu ist es aber erforderlich, dass auch eine große Anzahl von Services bereitstehen. Ein Treiber hierfür könnte das Online-Zugangsgesetz sein, das Bund, Länder und Kommunen verpflichtet, ihre Verwaltungsleistungen auch digital anzubieten, auch wenn die Umsetzung sich deutlich verzögert. Dies zeigen auch unsere Untersuchungen in diesem Bereich. Bürger*innen stehen digitalen Identitäten sehr positiv gegenüber, kritisieren aber die wenigen Anwendungsfälle.

Eine weitere notwendige Voraussetzung ist die Harmonisierung regulatorischer Anforderungen an digitale Identitäten für verschiedene Sektoren, z.B. Gesundheits-, Versicherungs- und Finanzsektor und öffentliche Verwaltung. Nur so lassen sich mit einer bestimmten digitalen Identität sehr viele Services nutzen. Die Harmonisierung betrifft auch die eindeutige Interpretation von Attributen. So ist z.B. die gegenseitige Anerkennung von notifizierten digitalen Identitäten über die eIDAS VO für alle Mitgliedsstaaten rechtsverbindlich. Für semantische Definitionen einzelner Attribute sind Datenbanken vorgesehen. Dies sollte nicht nur für notifizierte digitale Identitäten umgesetzt werden, sondern für alle digitalen Identitäten und zusätzlich auch für Beglaubigungen, die z.B. im SSI-Kontext eingesetzt werden (z.B. über eine freiwillige Selbstverpflichtung der Anbieter von Lösungen).

Grundsätzlich halte ich die Umsetzung der SSI-Prinzipien (Teilnahme, Barrierefreiheit, Transparenz, Sicherheit, Datenschutz und minimale Offenlegung usw.) für digitale

Identitäten und Beglaubigungen für wünschenswert. Allerdings sind die derzeit umgesetzten Lösungen sicherheitstechnisch noch nicht ausgereift.

Ein wesentlicher Kritikpunkt ist, dass bei der Umsetzung nicht zwischen digitalen Identitäten und Beglaubigungen (z.B. Abschlusszeugnissen) unterschieden wird. Mit einer digitalen Identität kann ich nachweisen, Marian Margraf zu sein, mit meiner Diplomurkunde lediglich, dass Marian Margraf ein Diplom hat. Die sicherheitstechnischen Anforderungen sind aber unterschiedlich. So dürfen z.B. Beglaubigungen vom Holder durchaus kopiert werden, für digitale Identitäten, die ja an die jeweilige Person gebunden ist, muss dies technisch verhindert werden.

Außerdem halte ich die einseitige Fokussierung auf Blockchain-Technologien für nicht zielführend. SSI sollte technologieoffen erforscht und entwickelt werden.

Weitere berechtigte Kritikpunkte an heutigen SSI-Lösungen sind, dass

a) keine Sicherheitsbeweise für die verwendeten kryptographischen Protokolle existieren,

b) sich Verifier nicht gegenüber Holdern authentisieren müssen,

c) Verifier Daten inklusive Zusatzinformationen erhalten, so dass auch gegenüber Dritten nachgewiesen werden kann, dass die Daten echt sind und

d) bisher keine technische Lösung für die Umsetzung digitaler Identitäten auf Smartphones existiert, die die sicherheitstechnische Anforderung Gerätebindung (um das Kopieren von digitalen Identitäten zu verhindern) umsetzt, ohne ein eindeutiges Merkmal (einen öffentlichen Schlüssel) zu verwenden, der Verifiern immer übertragen wird.

Über dieses eindeutige Merkmal kann aber der Holder über verschiedene Verifier hinweg nachverfolgt werden, auch wenn bei Anbieter A z.B. nur eine Altersverifikation durchgeführt wird, bei Anbieter B andere Identitätsdaten wie Name und Adresse übermittelt werden. Dies hebelt das Prinzip Datenschutz und minimale Offenlegung aus.

Die oben genannten Probleme bestehen für die im Jahr 2010 eingeführte Online-Ausweisfunktion im Übrigen nicht.

Die sichere Umsetzung digitaler Identitäten auf Smartphones ist nach wie vor eine große Herausforderung. Zwar hat das Bundesamt für Sicherheit in der Informationstechnik hier schon Vorarbeiten geleistet und z.B. in der Technischen Richtlinie TR-03159 Anforderungen für digitale Identitäten auf mobilen Endgeräten formuliert, mit denen ein eIDAS-Sicherheitsniveau von substantiell erreicht wird, welches für die meisten Anwendungsfälle ausreichend ist. Insbesondere müssen hierfür aber sogenannte Sicherheitselemente eingesetzt werden, die

kryptographisches Schlüsselmaterial sicher speichern und es ermöglichen, kryptographische Algorithmen sicher durchführen zu können. Diese sind zwar in den meisten mittel- bis hochpreisigen Smartphones enthalten und werden, wenn sich entsprechende Geschäftsmodelle für die Smartphone-Hersteller erkennbar werden, auch in niedrigpreisigen Smartphones verbaut werden (Sicherheitselemente selbst sind nicht teuer), allerdings ist derzeit nicht abschätzbar, ob Smartphone-Hersteller tatsächlich eine Nutzung der Sicherheitselemente (dies betrifft auch eSIMs) für digitale Identitäten zulassen. Ich halte es daher auch für sinnvoll, digitale Identitäten auf Basis der auf Smartphones bereitgestellten Sicherheitsfunktionen umzusetzen und hier gemeinsam mit den Herstellern die Funktionalität für die Verwendung digitaler Identitäten zu verbessern. Ein gutes Beispiel hierfür ist die Umsetzung bzw. Implementierung des Standards für mobile Führerscheine (ISO 18013-5) durch Apple und Google in ihren Smartphone-Betrienssystemen.

Darüber hinaus möchte ich noch einmal auf zwei Themen eingehen, die ich bereits in meiner Stellungnahme vom Mai 2021 im Rahmen der Öffentlichen Anhörung zum Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät“ erläutert habe.

Im Gegensatz zu der kartenbasierten Online-Ausweisfunktion, für die nur eine sehr eingeschränkte Anzahl von Sicherheitselementen (mit entsprechendem Betriebssystem und Software) genutzt wird, ist die Anzahl der verwendeten Hard- und Softwareversionen bei mobilen Endgeräten deutlich höher. Dabei ist nicht auszuschließen, dass es zukünftig zu Sicherheitslücken kommt, die auch die Sicherheit der auf den mobilen Endgeräten umgesetzten digitalen Identitäten schwächen. Es sollte daher ein Schwachstellenmanagement für diese Geräte aufgebaut werden, das es der Betreiberin des Gesamtsystems ermöglicht, Sicherheitslücken zu erkennen, zu bewerten und Gegenmaßnahmen, wie z.B. in schweren Fällen einzelne Geräte von der Verwendung auszuschließen, einzuleiten.

Weiter stehen Teile der Zivilgesellschaft großen Digitalisierungsprojekten der Bundesregierung skeptisch gegenüber, auch weil der Staat divergierende Interessen verfolgt. So wurde z.B. die Einführung der Online-Ausweisfunktion im Jahr 2010 vom CCC sehr negativ begleitet. Befürchtet wurde vor allem, dass der Staat über die Online-Ausweisfunktion die Bürgerinnen und Bürger ausspähen kann und nicht in der Lage ist, die Lösung sicher und datenschutzfreundlich zu gestalten. Die kritische Begleitung solcher Projekte sollte aber als Chance begriffen werden, Bürger*innen frühzeitig zu beteiligen, die Lösung zu verbessern und so insgesamt die gesellschaftliche Akzeptanz, gerade mit Blick auf Sicherheits- und Datenschutzfragen zu steigern.

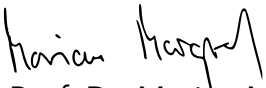
Daher sollte der gesamte Entwicklungsprozess sowie die darauffolgende Pflege und Weiterentwicklung vollständig transparent gestaltet und die Zivilgesellschaft stark eingebunden werden. D.h., alle Umsetzungskonzepte (z.B. Architektur-, Krypto-,

Sicherheitskonzept sowie Richtlinien zur sicheren Softwareentwicklung) müssen schon bei der Erstellung öffentlich zugänglich sein, mit der Öffentlichkeit diskutiert, Änderungsvorschläge bewertet und vor allem eine Ablehnung von Änderungen nachvollziehbar begründet werden. Auch die Softwareentwicklung sollte als Open-Source-Projekt unter einer geeigneten Open-Source-Lizenz gestaltet werden und auch hier die Community aufgerufen werden, daran mitzuwirken. Dies betrifft die im Projekt zu entwickelnden Softwarekomponenten, die Smartphone-Apps und die Secure-Element-Applets.

Hierfür sollte ein Internetportal bereitgestellt werden oder bestehende Services (z.B. GitHub oder GitLab) genutzt werden, auf dem alle Informationen zum Entwicklungsprozess, den Dokumenten und der Software aufgeführt sowie die Mitwirkungsmöglichkeiten dargestellt werden. Ein wesentliches Element des Portals ist die Aufbereitung von Änderungsvorschlägen an Dokumentation und Software durch die Community und deren öffentliche Bewertung durch die Projektleitung und Community (Aufnahme/Ablehnung inklusive Begründung).

Die oben beschriebenen Prozesse, sowie die Open Source Veröffentlichung im generellen, sollten den Standards und Best Practices der Open Source Community entsprechen (siehe hierfür z.B. die Veröffentlichungsstrategie der Corona-Warn App).

Mit freundlichen Grüßen



Prof. Dr. Marian Margraf