**Deutscher Bundestag**
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)845 B

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

Innenausschuss des
Deutschen Bundestages

**nur per E-Mail**

**Betr.:** Öffentliche Anhörung zum Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät“

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur öffentlichen Anhörung. Gern übersende ich Ihnen vorab meine Stellungnahme in schriftlicher Form.

Der auf dem Personalausweis, dem Aufenthaltstitel und der eID-Karte umgesetzte Identitätsnachweis (Online-Ausweisfunktion) wurde 2010 eingeführt. Bürger*innen können sich damit sicher und datenschutzfreundlich gegenüber Dienstanbietern authentisieren. Die wesentlichen Grundideen der Online-Ausweisfunktion sind:

1) Umsetzung einer Zwei-Faktor-Authentisierung, die auf Wissen (eine sechsstellige PIN) und Besitz (Ausweiskarte) basiert

2) Dienstanbieter erhalten nur diejenigen personenbezogenen Daten, die sie für ihren Dienst benötigen (umgesetzt über Berechtigungszertifikate, die vom Bundesverwaltungsamt ausgegeben werden) und

3) Bürgerinnen und Bürger wissen, wem gegenüber sie sich authentisieren (ebenfalls umgesetzt über Berechtigungszertifikate)

Dem Gesetzentwurf ist zu entnehmen, dass der geplante elektronische Identitätsnachweis mit einem mobilen Endgerät diese Technik übernimmt, d.h. sowohl eine Zwei-Faktor-Authentisierung als auch über Berechtigungszertifikate die Authentisierung datenschutzfreundlich umsetzt. Die Sicherheit hängt von der konkreten Ausgestaltung ab, die naturgemäß dem Gesetzesentwurf nicht vollständig zu entnehmen ist, sondern vielmehr, wie schon bei der kartenbasierten Lösung, über Technische Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geregelt wird. Das BSI hat hier schon Vorarbeiten geleistet und z.B. in der

Technischen Richtlinie TR-03159 Anforderungen für Identitätsnachweise auf mobilen Endgeräten formuliert, mit denen ein eIDAS-Sicherheitsniveau von subtantiell erreicht wird, welches für die meisten Anwendungsfälle ausreichend ist. Insbesondere müssen hierfür sogenannte Sicherheitselemente eingesetzt werden, die kryptographisches Schlüsselmaterial sicher speichern und es ermöglichen, kryptographische Algorithmen sicher durchführen zu können. Es kann also davon ausgegangen werden, dass die Lösung sicher umgesetzt wird.

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 Identitätsnachweise schwächen. Dies betrifft nicht nur Sicherheitslücken des eingesetzten Sicherheitselements (inklusive der hierauf laufenden Software), sondern auch Sicherheitslücken des verwendeten Betriebssystems des mobilen Endgerätes. So könnte z.B. eine Angreifer*in bei entsprechender Sicherheitslücke eine Schadsoftware auf dem mobilen Endgerät installieren, welche es ihr ermöglicht, den Identitätsnachweis aus der Ferne wie die reguläre Nutzer*in zu verwenden. Es sollte daher ein Schwachstellenmanagement für diese Geräte aufgebaut werden, das es der Betreiberin des Gesamtsystems (Bundesdruckerei im Auftrag der Bundesregierung) 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).

**Fazit:** Den elektronischen Identitätsnachweis für mobile Endgerät umzusetzen birgt das Potential, die Nutzungsreichweite deutlich zu erhöhen und damit die Digitalisierung sicher voranzutreiben. Vorrausetzung hierfür ist jedoch die sichere Umsetzung der Lösung, ein transparentes Handeln und die Einbindung der Zivilgesellschaft. Auch wenn Anfangs nur eine sehr eingeschränkte Auswahl von Geräten auf Grund fehlender Sicherheitsnachweise genutzt werden können, wird sich dies meines Erachtens zukünftig positiv verändern.

Mit freundlichen Grüßen

[redacted]

Prof. Dr. Marian Margraf