Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)845 A

AKDB | Postfach 150 140 | 80042 München

Anstalt des öffentlichen Rechts
Hansastraße 12-16
80686 München

Vorstand
vorstand@akdb.de
Telefon 089 5903 1547

An den

Innenausschuss des Deutschen Bundestages

14. Mai 2021

Stellungnahme für die Sachverständigen-Anhörung

zum

Gesetz zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät (Drucksache 19/28169)

sowie zum

Änderungsantrag der Fraktionen der CDU/CSU und der SPD

im Innenausschuss des Deutschen Bundestages

Management Summary

Der Gesetzentwurf ist zu begrüßen, da er potenziell die Anwenderbasis des neuen Personalausweises (nPA) bzw. des elektronischen Aufenthaltstitels (eAT) und der elektronischen Identität (eID) erhöht. Soweit der Änderungsantrag der Fraktionen der CDU/CSU und der SPD berücksichtigt wird, ergibt sich zudem eine für die (kommunale) Verwaltungsdigitalisierung sinnvolle und notwendige Erleichterung bei der Abfrage von Lichtbild und Unterschrift, soweit die Länder von der Regelungsbefugnis Gebrauch machen.

Bedeutung einer sicheren und nutzerfreundlichen Identifizierungslösung für die OZG-Umsetzung

Eine wesentliche Herausforderung für eine gelungene Verwaltungsdigitalisierung, also auch für die Umsetzung des OZG, ist die breitflächige Nutzung und Akzeptanz der Angebote durch Bürgerinnen, Bürger und Unternehmen. Hierfür unerlässlich ist das Vertrauen durch sichere Identitäten. Die Übertragung des nPA/eAT auf das Smartphone entspricht der Lebenswirklichkeit im Privaten wie in der Wirtschaft und ist deshalb uneingeschränkt zu begrüßen.

Anwendungen außerhalb der Verwaltung

Jede praxis- und bürgernahe Form einer elektronischen Identität hilft der Verwaltung wie der Privatwirtschaft, sichere und personenbezogene Angebote umzusetzen. Eine Lösung wie der nPA/eAT auf dem Smartphone kann durch eine erhöhte Akzeptanz die notwendigen Netzwerkeffekte für eine breitflächige Nutzung entfalten. Wichtig wäre allerdings, dass eine Ausgewogenheit zwischen eIDAS-Vertrauensniveau (möglichst Stufe "hoch" auch für den nPA/eAT auf dem Smartphone) und dem Verzicht auf überschießende Sicherheitsanforderungen (Hardware Secure Element) gewahrt wird. Eine softwareseitige Absicherung, in Abstimmung mit den Betriebssystem-Herstellern der Smartphones, wäre nach unserer Einschätzung zielführend.

Grundsätzlich schließen wir uns hierzu den in der Stellungnahme des Bundesbeauftragten für Datenschutz und Informationssicherheit, Prof. Ulrich Kelber, vom 12. Februar 2021 dargelegten Anpassungsvorschlägen zum eID-Gesetz an und unterstützen diese ausdrücklich.

Änderungsantrag

Der Änderungsantrag soll es den Ländern ermöglichen, eigene Passregister zu führen, aus denen dann in einem automatisierten Verfahren Lichtbild und Unterschrift (z.B. für Sicherheitsbehörden) extrahiert werden können.

Bezüglich einer zentralen Speicherung von Passbildern in zentralen Registern der Länder ist auf die positiven Erfahrungen mit den Landesmelderegistern im Rahmen der melderechtlichen Behördenauskunft zu verweisen. Diese wird in allen Flächenländern (außer Nordrhein-Westfalen) erfolgreich praktiziert. Zu den Vorteilen eines landesweiten Pass-/Ausweisregisters zählen

- die sehr hohe Verfügbarkeit solcher Register,
- die zentrale Benutzer-/Rechte-Steuerung für alle Anfragen an einer Stelle,
- die Nutzung vorhandener Infrastrukturen in analoger Anwendung der Struktur der Landesmelderegister,
- die nur einmalige Investition für die Schaffung solcher Register je Bundesland, im Gegensatz zu den andernfalls jeweils lokal notwendigen Investitionen auf Seiten der Kommunen für den Zugriff, die Infrastruktur, den Betrieb, die Sicherstellung der Verfügbarkeit sowie die Updates dezentraler Pass-/Ausweisregister.

Insgesamt ist davon auszugehen, dass eine dezentrale Ausgestaltung für die Kommunen deutliche Mehrkosten gegenüber zentraler Passregister auf Landesebene nach sich zieht. Letztere gehen zudem für die zuständigen Sicherheitsbehörden mit erleichterten Kommunikationsszenarien einher, da weniger Kommunikationspartner involviert sind. Auch die Anforderungen an die IT-Sicherheit zur Absicherung des Zugriffs auf die Register sind so deutlich einfacher umzusetzen. Dies gilt umso mehr, als eine Nutzung etwa im Rahmen des § 22a Abs. 2 Satz 6

PaßG bzw. § 25 Abs. 2 Satz 5 PAuswG mit Einwilligung der antragstellenden Person dann erheblich weniger technische Komplexität aufweist.

Mit freundlichen Grüßen

[redacted]

Rudolf Schleyer
Vorstandsvorsitzender