

220209, [REDACTED] b, FIDO2 und der elektronische Personalausweis

noreply@bmi.bund.de

25. März 2022 11:35

An: [REDACTED]

Az: PKII4-12017/1#1 - [REDACTED]

Sehr [REDACTED]

Ihr Schreiben vom 9. Februar 2022 an das Bundesministerium des Innern und für Heimat (BMI), mit dem Sie um Auskunft nach dem Informationsfreiheitsgesetz (IFG) bitten, wurde eingehend in unserem Haus geprüft. Der Sache nach handelt es sich nicht um einen formellen Antrag nach dem IFG, sondern um ein allgemeines Auskunftsverlangen. Daher wurde die Bürgerkommunikation gebeten, Ihnen zur abschließenden Beantwortung Ihrer Zuschrift folgende Hinweise zu übermitteln:

Zur Frage 1: Die Nutzung von Passwörtern als einzige Authentifizierungsart birgt das Risiko für die Bürger und Bürgerinnen, dass das gleiche Passwort bei vielen unterschiedlichen Diensten benutzt wird, erraten, ausgelesen werden könnte oder bei der Übertragung durch ausländische staatliche Stellen in Zusammenarbeit mit Zertifizierungsstellen ausgelesen wird. Auch deshalb empfiehlt das BSI die eine Nutzung einer Zwei-Faktor-Authentisierung, sobald ein Online-Dienst dies ermöglicht.

Würde sich der elektronische Personalausweis mit der Pseudonym-Funktion als Hardware-Token zur Zwei-Faktor-Authentisierung eignen?

Antwort BMI:

Ja, der Personalausweis ist hierfür geeignet. Die pseudonyme Authentisierung wurde hierbei explizit für diesen Anwendungsfall entworfen und erlaubt eine sichere Zwei-Faktor Authentifizierung mit dem Personalausweis als Besitz-Faktor (Hardware-Token) und der PIN als Wissensfaktor. Die PIN wird hierbei durch das PACE-Protokoll unmittelbar durch den Chip des Personalausweises validiert und zu keiner Zeit mit dem Dienstanbieter geteilt.

Mit Hilfe der pseudonymen Authentisierung kann sich der Dokumenteninhaber gegenüber einem Diensteanbieter authentisieren, ohne persönliche Daten freizugeben. Des Weiteren bildet der Chip des Personalausweises für jeden Diensteanbieter ein anderes Pseudonym, so dass das Verbinden von Pseudonymen über Diensteanbiertergrenzen hinweg nicht möglich ist (Nichtverkettbarkeit).

Weitere Informationen zu den Protokollen des Personalausweises können Sie auch in der Technischen Richtlinie TR-03127 des BSI finden:

bsi.bund.de

Frage 2: Wenn dem so wäre, warum wird diese Funktion nicht aktiver beworben und besser erklärt, dass dies ohne Freigabe der eigenen personenbezogenen Daten möglich ist?

Antwort BMI:

Die Pseudonymfunktion wird auf dem Personalausweisportal erläutert, welches als Informationsplattform für die Funktionen des deutschen Personalausweises seitens des Bundesministeriums des Innern und für Heimat betrieben wird. Links:

- <https://www.personalausweisportal.de/Webs/PA/DE/verwaltung/technik/pseudonym/pseudonym-node.html>
- https://www.personalausweisportal.de/SharedDocs/faqs/Webs/PA/DE/Haeufige-Fragen/9_pseudonymfunktion/pseudonymfunktion-liste.html

Frage 3: Warum wurden nicht die Möglichkeit geschaffen, einen zweiten anderen Pin oder keinen Pin nur für diese Funktion zu nutzen? Hätte es dadurch dem Bürger bzw. der Bürgerin verständlicher gemacht werden können, dass wirklich keine auf dem Ausweis personenbezogene Daten bei der Nutzung dieser Funktion ausgegeben werden, sondern vielmehr nur Synonyme?

Antwort BMI:

Die Verwendung einer zweiten PIN würde die Benutzerfreundlichkeit des Systems für den Bürger verschlechtern, ohne einen echten Mehrwert für die Sicherheit der Authentifizierung zu erzielen. Da die PIN ausschließlich durch den Chip des Personalausweises validiert wird, kann diese auch nicht durch mögliche Sicherheitslücken in den Hintergrundsystemen von Diensteanbietern kompromittiert werden.

Zudem muss gemäß PAuswG der Nutzer bei jedem Identifizierungs-/Authentifizierungs-Vorgang die erwünschten Zugriffsrechte einsehen können. Diese werden dem Nutzer durch den lokal ausgeführten eID-Client (z.B. die AusweisApp2) bei jedem Vorgang präsentiert, so dass dem Nutzer jederzeit erkenntlich ist, ob und welche Identitätsdaten abgefragt werden, oder ob ausschließlich die Pseudonymfunktion verwendet werden soll. Der Benutzer hat zudem die Möglichkeit, die vom Diensteanbieter erbetenen Zugriffsrechte weiter einzuschränken.

Der Wegfall der PIN wurde nicht in Erwägung gezogen, da in diesem Fall keine Zwei-Faktor-Authentifizierung mehr gewährleistet wäre.

Frage 4: Es gibt den Standard FIDO2 der von allen großen digitalen Playern unterstützt wird. Warum wird dieser Standard nicht einfach von der AusweisApp2 mit unterstützt und angeboten?

Antwort BMI:

Es ist richtig, dass die Pseudonymfunktion des Personalausweises und die FIDO-Standards vergleichbare Ziele verfolgen, insbesondere die Authentifizierung ohne Preisgabe von Identitätsdaten, sowie die Nichtverfolgbarkeit über Diensteanbiertergrenzen hinweg.

Der elektronische Personalausweis wurde allerdings bereits erstmalig im Jahr 2010 ausgegeben. Zu diesem Zeitpunkt waren die FIDO-Allianz, sowie deren Standards noch nicht existent und konnten folglich bei der Entwicklung des Personalausweises nicht betrachtet werden.

Eine nachträgliche Einbindung der Standards in die AusweisApp2 ist leider nicht ohne weiteres möglich, da die kryptographischen Protokolle technisch nicht kompatibel mit der Pseudonymfunktion des Personalausweises sind. In beiden Verfahren müssen wesentliche kryptographische Funktionen in einem Hardware-Token des Nutzers ausgeführt werden. Folglich kann eine Unterstützung von FIDO-Standards nicht alleine durch eine Anpassung der AusweisApp2 realisiert werden, sondern müsste durch eine Änderung an der Funktionalität des Ausweis-Chips umgesetzt werden.

Frage 5: Um diesen Standard dennoch nutzen zu können, muss auf Browsererweiterungen von Privatmenschen zurückgegriffen werden.

(<https://addons.mozilla.org/de/firefox/addon/webauthn-eid-for-firefox>) Was sind die Gründe, dass Sie nicht selbst so eine Lösung (als Open Source) entwickeln und anbieten? Inwieweit ergeben sich daraus Haftungsfragen für Sie, wenn Sie die Entwicklung an unbezahlte Entwickler auslagern? Könnten davon Ihre Schutzpflichten gegenüber den Bürgerinnen und Bürger betroffen sein?

Antwort BMI:

Die genannte Browsererweiterung wurde im Rahmen eines Forschungs-projekts des BSI entwickelt (Projekt FIDELIO). Dieses diente der Erprobung der Pseudonymfunktion als Authentifizierungsmittel bei Diensten, welche die Authentifizierung anhand der FIDO-Protokolle unterstützen.

Hierzu wurde ein Dienst geschaffen werden, welcher zwischen der eID-Online-Authentisierung und der FIDO-Authentisierung vermittelt. Dieser Dienst authentisiert den Nutzer zunächst anhand seines Personalausweises, um ihn anschließend darauf aufbauend gegenüber einem FIDO-Dienst zu authentisieren. Dieser Dienst, besteht dabei aus einem standardkonformen eID-Server und einem neu entwickelten Service, dem sog.

FIDELIO eService. Der eService leitet bei jeder Authentisierung aus dem Pseudonym des Nutzers dienst-spezifische asymmetrische Schlüsselpaare ab, welche für das FIDO-Protokoll benötigt werden. Mit diesem Schlüsselpaar werden die für das FIDO-Protokoll notwendigen kryptographischen Operationen durchgeführt. Im Anschluss werden diese Schlüssel wieder vernichtet. Auf diese Weise müssen keine personenbezogenen Daten auf dem FIDELIO eService gespeichert werden.

Das Projekt wird zurzeit leider nicht aktiv weiterentwickelt, da das Projekt gegenwärtig nicht die gewünschte Nutzerfreundlichkeit bei der Integration in Browser oder Mobil-Betriebssystem erreichen kann. Hierfür ist eine Integrationstiefe in diese notwendig, welche mit den zur Verfügung stehenden Plugin/Addon-Schnittstellen der Browser nicht (mehr) realisierbar ist und eine Mitwirkung der Hersteller erfordern würde, welche aber nicht gegeben ist.

Die Projektergebnisse sind unter einer Open-Source-Lizenz unter folgendem Link verfügbar:

gitlab.com

Der für das Projekt notwendige Web-Dienst wird auch weiterhin durch die adesso SE betrieben.

Frage 6: Mit Ablauf der Gültigkeit des Ausweises wird die Online-Ausweis-Funktion auch deaktiviert. Dadurch ist keine Anmeldung mehr bei eID-Service-Provider oder Online-Dienst möglich. Auch bei einer fristgemäßen Neubeantragung des Ausweises ist eine Anmeldung nicht mehr möglich, weil eine Übertragung der Pseudonym zwischen den Ausweisen nicht vorgesehen ist oder sehe ich das falsch?

Warum wurde keine Kulanz-Zeitraum von ca. zwei Monaten eingeführt, in dem die Bürger und Bürgerinnen beide Ausweise besitzen und den neue beantragten Personalausweis bei den genutzten eID-Service-Provider oder Online-Dienst neu hinterlegen können, um dann später mit endgültigen Ablauf den alten Ausweis zu löschen? Welche Strategien gibt es sonst zum Wechsel des Personalausweises oder wie soll vorgegangen werden?

Antwort BMI:

Es ist richtig, dass das Pseudonym für jede Ausweiskarte individuell ist und folglich bei einem Wechsel des Ausweises nicht mehr mit dem vorherigen übereinstimmt und auch eine Übertragung nicht möglich ist. Die Bereitstellung eines dauerhaften Pseudonym ist nicht möglich, da hierdurch die Schaffung einer staatlich vergebenen Personenkennziffer vermutet werden könnte, welche nach aktueller Rechtsprechung nicht gesetzeskonform wäre.

Ein Kulanzzeitraum von zwei Monaten ist ebenfalls nicht möglich, da gemäß § 4 Absatz 1 des Personalausweisgesetzes eine Person nur einen gültigen Personalausweis der Bundesrepublik Deutschland ausgestellt erhalten darf.

In der FAQ des Personalausweisportals werden Möglichkeiten für Diensteanbieter beschreiben, welche Möglichkeiten bestehen, um den Zugang zum Kundenkonto nach einem Ausweiswechsel über eine pseudonyme Wiedererkennung weiterhin zu ermöglichen. Link:

personalausweisportal.de

Das entsprechende Fachreferat wurde hinsichtlich der Fehlermeldung im Nutzerkonto id.bund.de durch mich informiert.

Mit freundlichen Grüßen
im Auftrag

[REDACTED]
Bürgerkommunikation
im Bundesministerium des Innern und für Heimat

Graurheindorfer Str. 198
53117 Bonn
Telefon: +49 30 186810
E-Mail: Buergerkommunikation@bmi.bund.de
Internet: www.bmi.bund.de
www.g7germany.de

Zusammen gegen Corona

Die Ständige Impfkommission (STIKO) empfiehlt allen Personen ab 18 Jahren eine Auffrischungsimpfung gegen COVID-19, deren zweite Impfung etwa sechs Monate zurückliegt. Seit September wurden bestimmten Personengruppen bereits priorisiert Auffrischungsimpfungen angeboten. Alle Informationen zu diesen Impfungen finden Sie [hier](#).

Schützen Sie sich und andere!

Bei der Bearbeitung Ihres Anliegens wurden bzw. werden von Ihnen personenbezogene Daten verarbeitet.

Welche Daten zu welchem Zweck und auf welcher Grundlage verarbeitet werden, ist abhängig von Ihrem Anliegen und den konkreten Umständen.

Weitere Informationen hierzu und über Ihre Betroffenenrechte finden Sie in der Datenschutzerklärung auf der Internetseite des Bundesministerium des Innern und für Heimat unter: https://www.bmi.bund.de/DE/service/datenschutz/datenschutz_node.html
