

Beschluss des ASJ-Bundesvorstands vom 7. Januar 2023:

Personalausweis mit USB-Schnittstelle - Recht auf Pseudonymisierung

Die Bundesregierung, die Bundesinnenministerin, die SPD-Bundestagsfraktion werden aufgefordert,

1. den Personalausweis nebst der darin schon jetzt enthaltenen Vorrichtung zum digitalen Identitätsnachweis und zum digitalen Signieren mit einer qualifizierten elektronischen Signatur (QES) gemäß § 126a BGB mit einer einfachen Chipkarten-Schnittstelle zu versehen, die mit einem bei der Aushändigung des Personalausweises mit zu überreichenden einfachen Chipkartenlesegerät mit einer USB-Schnittstelle (oder Thunderbold) verbunden werden kann.
2. Mit dieser Schnittstelle soll die Identifikation und die QES ohne weitere Vorrichtungen an einem PC oder an einem möglichst beliebigen Mobilgerät ermöglicht werden, an dem der Personalausweis angeschlossen ist. Weitere Geräte sollen - abgesehen von der Wahl einer 2. Faktoridentifikation (siehe unten) - nicht erforderlich sein, insbesondere nicht gesonderte Tastaturen zur PIN-Eingabe.
3. Die bisher schon bestehende NFC-Funkschnittstelle des Personalausweises soll auch für das digitale Signieren mit einer QES verwendet werden können.
4. Die QES-Funktion bedarf vor der ersten Benutzung der Freischaltung durch die Ausweisinhaberin oder den Ausweisinhaber.
5. Sofern der Ausweisinhaber nichts anderes bestimmt, soll die QES als offline-Signatur funktionieren. Alternativ dazu soll die Ausweisinhaberin oder der Ausweisinhaber wählen können, die QES kostenfrei online zu nutzen.
6. Zumindest im Falle der Wahl einer Online-Funktion ist den Ausweisinhabern und den Ausweisinhabern anzubieten, die Nutzung des digitalen Identitätsnachweises und der QES neben der einzugebenden PIN zusätzlich von einer weiteren Authentifizierung entsprechend der vom Online-Banking bekannten 2-Faktor-Authentifizierung abhängig zu machen, bei der zur Nutzung zusätzlich ein Einmalkennwort (TAN) über ein anderes Gerät einzugeben ist.

7. Die Nutzung der oben geforderten Dienste erfolgt für die Ausweisinhaberinnen und Ausweisinhaber als auch für die öffentlichen und nichtöffentlichen Stellen, denen gegenüber die Nutzung erfolgt, ohne zusätzliche Kosten. Die Gebühren für den Personalausweises dürfen nicht wegen ihrer digitalen Funktionen höher bemessen werden. Sofern die digitale Funktion eines Personalausweises während seiner Gültigkeitsdauer defekt wird und hierfür keine grobe Fahrlässigkeit zu erkennen ist, soll ein Ersatz kostenfrei oder mit Gebühren höchstens im einstelligen Euro-Bereich gestellt werden.
8. Die Ausweisinhaberin und der Ausweisinhaber haben das Recht bei der Nutzung dieser digitalen Funktionen zertifizierte Pseudonyme zu verwenden, die ihnen von öffentlich-rechtlichen Datentreuhändern kostenfrei zur Verfügung gestellt werden. Per Rechtsverordnung können nicht-öffentliche und öffentliche Stellen allgemein bestimmt werden, denen gegenüber keine Pseudonyme verwendet werden dürfen. Gleiches kann aufgrund einer - kostenpflichtigen - Einzelfallprüfung für andere Stellen unter Bestimmung der konkreten Szenarien bestimmt werden. Zur Nutzung der Pseudonyme verweisen wir auf den Beschluss der ASJ-Bundeskonferenz 2021 - Datenpolitik für alle - Regelungen mit Bezug auf Private Nr. 5.
9. Ausländischen Mitbürgerinnen und Mitbürgern sind ab einer bestimmten Aufenthaltsdauer entsprechende digitale Identifikationsnachweise und QES ggf. unter Bestimmung weiterer Voraussetzungen zur Verfügung zu stellen.

Begründung:

Mit zunehmender Digitalisierung aller Lebensabläufe soll der Personalausweis seine Funktionen zur Identifizierung und Authentifizierung auch auf digitalem Weg erfüllen. Damit die Digitalisierung der Gesellschaft voranschreiten kann, müssen technische und praktische Hürden so weit und so gut es geht aus dem Weg geräumt werden. Der Personalausweis muss aus sich heraus auch digital funktionieren. Weder dürfen der Ausweisinhaberin und dem Ausweisinhaber zusätzliche Kosten noch ein zusätzlicher Beschaffungsaufwand für besondere Geräte auferlegt werden. Dem Datenschutz ist durch ein reguliertes Recht auf Pseudonymisierung Rechnung zu tragen.

zu 1.- 3.: Der Personalausweis dient der. Bisher erreicht der Personalausweis die Identifizierung einer Person, damit diese die ihr zustehenden Rechte wahrnehmen

kann, und deren Authentifizierung, damit diese nachweisbar Verpflichtungs- und Bekundungstatbestände schaffen kann, auf manuellem Wege durch Vergleich von Bild und Unterschrift mit den entsprechenden Merkmalen des Ausweisinhabers.

Für die digitale Welt können diese Funktionen über digitale Zertifikate erzielt werden, die den Ausweisinhaber zuverlässig einer bestimmten Person zuordnen und das digitale Signieren von Dokumenten bzw. deren Hash-Werten ermöglichen.

Die hierfür erforderliche Verbindung des Personalausweises mit einem Computer funktioniert derzeit nur mit einer beschränkten Anzahl von Mobiltelefonen, über bestimmte Kartenleser am PC und im Übrigen auf Umwegen (NFC-fähiges Mobiltelefon mit modernem Betriebssystem muss im selben WLAN mit einem PC verknüpft sein). Die Kartenleser kosten etwa 30 €. Für eine QES ist derzeit ein besonderer Kartenleser erforderlich, der 60 € kostet; ein Mobiltelefon kann dafür in Deutschland nicht verwendet werden. Da derzeit kein Kartenleser der die QES des Personalausweises nutzen kann, bedarf es für eine QES gesonderter Karten, die mindestens weitere 40 € kosten. Dies ist in mehrfacher Hinsicht zu umständlich und ein wesentlicher Grund für die geringe Digitalisierung von privatrechtlichen und Verwaltungsabläufen.

Um diesem Missstand zu begegnen, müssen die Bürgerinnen und Bürger mit dem Personalausweis ein Mittel in die Hand bekommen, das sie ohne die Anschaffung weiterer Zusatzgeräte und ohne zusätzliche Kosten unmittelbar an ihren Computern verwenden und insbesondere mit diesen verbinden können. Dafür ist die USB-Schnittstelle die am weitesten verbreitete Schnittstelle.

Estland zeigt mit seinem Personalausweis, der zugleich eine digitale ID-Karte mit QES-Funktion ist, dass ein solcher Ausweis wie nachfolgend abgebildet mit einer von Bank- und Chipkarten bekannten elektrisch leitenden Kontaktzone zur

Signalübertragung ausgestattet werden kann (siehe rechte Abbildung für die Rückseite, dort links das Kontaktfeld).



Für einen Kontakt mit einem PC oder einem Mobilgerät bedarf es dann lediglich noch eines Kartenlesers, dessen Endpreis für den Endverbraucher in Estland im Laden derzeit rund 5 € beträgt und beispielsweise wie folgt aussieht:



Um dem Ausweisinhaber auch die Kosten- und Beschaffungshürde für den Kartenleser zu nehmen, soll ihm ein solches Gerät kostenlos mit dem deutschen Personalausweis ausgehändigt werden; die damit für den Staat verbundenen Kosten im Großeinkauf würden dabei auf einen - im Verhältnis zu den Vorteilen vernachlässigbaren - Bruchteil sinken. Für Nutzer von Geräten anderer Hersteller ohne USB-Buchse wie z.B. Apple-Geräten sollen solche Kartenleser mit den entsprechenden Steckern (z.B. Thunderbolt und Lightning) ausgestattet sein.

Zusätzlich soll der Ausweisinhaber natürlich auch weiterhin eine NFC-Verbindung nutzen können, um sich kabellos mit einem Mobiltelefon oder einem entsprechenden (eigenen) Kartenleser mit einem PC verbinden zu können. Estland und Österreich, wo ähnliches mit einer Bürgerkarte bereitgestellt wird, zeigen, dass es auch für die QES keines besonderen, mit einer Tastatur ausgestatteten Kartenlesers bedarf. Eine spezielle Tastatur auf dem Kartenleser, wie es derzeit für digitale Signaturkarten in

Deutschland erforderlich ist, um die PIN zur Nutzung der QES eingeben zu können, ist nach der eIDAS-Verordnung (EU-VO 910/2014) nicht erforderlich.

Wichtig ist es, dem Bürger auch einen Kartenleser zur Anbindung an den eigenen PC per USB an die Hand zu geben. Viele Vorgänge wie beispielsweise eine Steuererklärung oder komplizierte Antragsverfahren lassen sich nicht gut an einem Mobiltelefon vornehmen. Hierfür wird der PC gebraucht. Aber auch schon so einfache Angelegenheiten wie der Blick in das zentrale Fahrerlaubnisregister oder das Grundbuch für das eigene Grundstück lassen sich leichter am PC als an einem Mobiltelefon erledigen. Manche, insbesondere ältere Mobiltelefone sind zu einer Verbindung per NFC schon gar nicht in der Lage.

Mit einer solchen digitalen Ausrüstung des Personalausweises sollen den Bestrebungen der Europäischen Union zur Einführung eines eID-Systems für eine EU-eID-Wallet-App auf einem Mobiltelefon nicht die Relevanz genommen werden. Der digitale Personalausweis soll seine Funktionen ggf. zusätzlich zu einer solchen App entfalten können, auch und gerade weil seine Funktionen nicht zwingend auf ein Mobiltelefon angewiesen sein sollen.

zu 4.: Die entsprechende Ausgestaltung des Personalausweises und die Zurverfügungstellung eines einfachen Kartenlesers, wie oben dargestellt, sollen dem Bürger eine Identifikation und insbesondere eine QES nur ermöglichen. Insbesondere die QES soll von ihm freigeschaltet werden müssen, um selbst bestimmen zu können, ob diese Funktion mit seinem Personalausweis möglich ist oder nicht.

zu 5.+6.: Es ist bekannt, dass die QES offline von der Signaturkarte selbst erzeugt, alternativ dazu aber auch im online-Verfahren mit Hilfe eines zertifizierten Rechenzentrums bewirkt werden kann. Die dabei zu Buche schlagenden Kostenunterschiede dürften letztlich nicht relevant sein. Entscheidend ist, dass die Bürgerinnen und Bürger größeres Vertrauen in eine Offline-Signatur setzen werden und dass diese für den konkreten Signaturvorgang keiner Internetverbindung bedarf. Deshalb soll das offline Verfahren als Standard vorgesehen sein.

Gleichwohl soll der Ausweisinhaber aber auch eine QES wählen können, die im online-Verfahren signiert. Diese Alternative soll bereits deshalb zur Wahl stehen, weil insbesondere dann auch eine Verknüpfung mit einem weiteren

Authentifizierungsverfahren möglich wird, wie es von der 2-Faktor-Authentifizierung im Online-Banking bekannt ist. Damit kann ein noch höheres Maß an Sicherheit vor unechten digitalen Signaturen gewährleistet werden.

zu 7.: Entscheidend für eine erfolgreiche und breite Verwendung der digitalen Identifizierung und der QES dürfte das Ausbleiben zusätzlicher Kosten für die Bürgerinnen und Bürger sowie die (kostenlose) Bereitstellung aller erforderlichen Mittel, um diese Funktionen an einem eigenen Gerät wie dem eigenen PC oder dem eigenen Mobiltelefon (auch älterer Bauart) nutzen zu können. Die Erfahrungen des Bildschirmtextes in Frankreich (dort: "Minitel") in den 80er und 90er Jahren im Vergleich zu Deutschland zeigen, dass solche Innovationen sich nur durchsetzen, wenn sie flächendeckend wirken. Frankreich hatte damit im Gegensatz zu Deutschland Erfolg, weil die erforderlichen Geräte kostenlos zur Verfügung gestellt wurden.

Dabei ist der zusätzliche Kostenaufwand für die oben dargestellten Forderungen äußerst gering, jedenfalls wenn man sie ins Verhältnis zu den Aufwendungen stellt, die Frankreich mit Minitel hatte. Der Personalausweis weist jetzt schon die erforderlichen Prozessoren auf, um einen digitalen Identitätsnachweis und ein QES zu ermöglichen. Eine zusätzliche elektrische Kontaktfläche, wie sie der estnische Personalausweis zeigt, dürfte nur wenige Cent mehr kosten. Gleiches gilt letzten Endes für den Kartenleser, wenn er in entsprechender Stückzahl angeschafft werden muss.

Die vermehrte Nutzung der digitalen Funktionen eines Personalausweises kann über seine gesamte Gültigkeitsdauer hinweg auch mit einem erhöhten Verschleiß einhergehen. Das damit verbundene Risiko eines vorzeitigen Defektes soll nicht der Bürger tragen müssen. Sofern keine mutwilligen Beschädigungen zu erkennen sind, soll der Bürgerin und dem Bürger in diesem Fall ein Ersatz kostenlos oder nur gegen eine geringe Schutzgebühr zur Verfügung gestellt werden.

zu 8.: Die breite und flächendeckende Nutzung eines digitalen Identifikationsnachweises birgt indessen eine neue Gefahr in sich: die Überidentifikation ("overidentification"). Wenn es zu einfach wird, zuverlässig die Personendaten eines Individuums digital im Geschäftsverkehr und bei der Nutzung digitaler Medien zu erfassen, kann dies dazu führen, dass solche Daten übermäßig erfasst, gespeichert und schließlich anhand der zuverlässigen Datenkonsistenz miteinander verknüpft werden.

Dem kann und muss mit Hilfe von elektronischen Pseudonymen begegnet werden, die von einem öffentlich-rechtlich getragenen Datentreuhänder zertifiziert sind. Geschäftliche und kommunikative Kontakte, die in der analogen Welt ohne verlässlichen Identifikationsnachweis stattfinden, wie der Kauf einer beliebigen Ware oder die Beteiligung an einer öffentlichen Diskussion, müssen auch in der digitalen Welt ohne die zuverlässige und sofortige Erfassung der echten Klarnamen stattfinden können. Im Konfliktfall kann auch in der analogen Welt dieser Klarnamen mit einem gewissen Rechercheaufwand ermittelt werden (Frage an andere Diskussionsteilnehmer: Kennst du den, der diese Verleumdung geäußert hat?). Übertragen auf die digitale Welt folgt daraus, dass ein Nutzer sich zunächst quasi anonym eine Ware kaufen und an einer Diskussion teilnehmen kann, aber im Konfliktfall über ein zu verwendendes, zertifiziertes Pseudonym ermittelt werden kann, wenn der Diensteanbieter ein solches Pseudonym verlangt. Der das Pseudonym zertifizierende Datentreuhänder kann dann in einem Konfliktfall unter klar definierten Voraussetzungen (z.B. gerichtliche Auseinandersetzung) den Klarnamen mitteilen.

Hierfür muss festgeschrieben werden, dass für die Vielzahl der zivilrechtlichen und auch einige der öffentlich-rechtlichen digitalen Kontakte das Recht besteht, nur ein von einem öffentlich-rechtlichen Datentreuhänder zertifiziertes Pseudonym zu verwenden. Im Wege einer Positivliste wären die Fälle zu bestimmen, in denen zwingend Klarnamen von Beginn an verwendet werden müssen (z.B. Bankgeschäfte, Gerichtskontakte, Behördenkontakte mit Bedeutung für die Finanzen eines Individuums). Für alle anderen Kontakte würde das Recht auf Pseudonymität gelten, wobei zusätzlich eine Einzelfallprüfung vorzusehen wäre, in begründeten Ausnahmefällen dennoch einen Klarnamen über den digitalen Identitätsnachweis verlangen zu können. Der digitale Identitätsnachweis im Personalausweis müsste darauf zugeschnitten sein, für die Stellen, denen kein Klarnamen zwingend mitzuteilen ist, ein Pseudonym übermitteln zu können.

zu 9: Wenn der digitale Identitätsnachweis und die QES weite Verbreitung gefunden haben, dürfen ausländische Mitbürger nicht dadurch benachteiligt werden, dass sie keinen deutschen Personalausweis erhalten. Entsprechend der bereits heute geltenden Regelung in Estland sollen ausländische Mitbürger deshalb eine gesonderte Karte für einen digitalen Identitätsnachweis und eine QES erhalten können.