ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

An
den Ausschuss für Inneres und Heimat des
Deutschen Bundestages

Stellungnahme zum Gesetzentwurf zur Stärkung der Sicherheit im Pass-, Ausweis und ausländerrechtlichen Dokumentenwesen BT-Drucksachen 19/21986 und 19/22783

Nationales Forschungszentrum für angewandte Cybersicherheit

Prof. Dr. Christoph Busch

Hochschule Darmstadt
Haardtring 100
64293 Darmstadt
Tel. +49-6151-16-30090

christoph.busch@h-da.de

2020-10-23

Sehr geehrte Damen und Herren,

ich danke für die Einladung zur Anhörung am kommenden Montag und übersende Ihnen vorab meine Stellungnahme zum Gesetzentwurf.

Ich bin weitestgehend zufrieden mit dem Entwurf des Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen (Drucksache 19/21986) vom 31.08.2020 und freue mich über die Änderungen, die gegenüber der Vorversion vom 09.12.2019 umgesetzt wurden.

Der Entwurf ist in seinem Wesen richtig und wichtig und wird ermöglichen, dass Deutschland zu den Europäischen Vorreitern im Live-Enrolment (Schweden und Norwegen) endlich aufschließen kann.

zur Technik:
Ich kann Ihre Annahme bestätigen, dass derzeit nach meinem Wissen alle Produkte zur automatisierten Gesichtserkennung durch Morphing-Angriffe verwundbar sind. Es ergeben sich hohe Übereinstimmungswerte für beide im Lichtbild „enthaltenen“ Personen, die denen von unveränderten Lichtbildern entsprechen. Das bedeutet, dass Personaldokumente Ihren eigentlichen Wert verlieren, da die biometrische Bindung an den Inhaber nicht mehr gewährleistet ist.

Es gibt zwei Alternativen zur Prävention vor Morphing-Angriffen:

1.) Live-Enrolment in Deutschland und allen anderen EU-Ländern
2.) Elektronische Übertragung von digital signierten Lichtbildern direkt von autorisierten Photographen (Dienstleistern) an die Passbehörde (ebenfalls in allen EU-Ländern)

zu 1.): das ist die langfristig sinnvollste Lösung, die in Deutschland und allen EU-Mitgliedsstaaten umgesetzt werden sollte. Jedoch bleiben auch damit die Morphing-Angriffe von Drittstaatlern weiterhin möglich.

zu 2.): dies könnte z.B. durch De-Mail realisiert werden, wie es nun in Abschnitt E.2 in der Drucksache 19/21986 diskutiert wird. Damit sollten die vorgetragenen Bedenken der Photographen ausreichend berücksichtigt sein. Forderungen zur Beibehaltung der Verwendung ausgedruckter Lichtbilder sind nicht mehr zeitgemäß und bei Kenntnis der Morphing-Angriffe nicht zu verantworten. Zudem werden meines Wissens die Digitalisierungs-Bemühungen der Bundesregierung ja auch von den Oppositionsparteien getragen. Warum sollte man hier eine Ausnahme machen?

Im direkten Vergleich ist die Alternative 1.) klar zu favorisieren. Erstens aus Gründen der Sicherheit des Verarbeitungsprozesses, da Alternative 2.) möglicherweise Einbringpunkte für manipulierte/gemorphte Lichtbilder zulassen würde. Zweitens sind bei Alternative 2.) Kosten und logistischer Aufwand bei der Registrierung der Dienstleister anzunehmen.

Unabhängig von 1.) und 2.) ist es notwendig, Morphing-Attack-Detection (MAD) Verfahren zu entwickeln, die für den Einsatz an der Grenze zur Detektion von Pässen mit gemorphten Lichtbildern z.B. aus Drittstaaten geeignet sind. siehe:
https://christoph-busch.de/projects-mad.html

Es gibt mittlerweile etliche Forschungsaktivitäten, um gemorphte Lichtbilder zu erkennen. Die Detektionsleistung und insbesondere die Falschalarmraten solcher MAD-Verfahren sind derzeit ungenügend und für den operativen Einsatz noch nicht geeignet. siehe:
https://pages.nist.gov/frvt/html/frvt_morph.html
Dabei sei betont, dass die Alterung von biometrischen Referenzdaten im Verlauf der 10 jährigen Gültigkeitsdauer des Ausweises, in Verbindung mit einem Morphing-Angriff, die Chancen zur Detektion von gemorphten Lichtbildern weiter schmälern.

Fingerbilder im Dokumentenwesen:
Die „Zufallsfunde“ von gemorphten Pässen in polizeilichen Ermittlungen oder bei der Kontrolle an den Grenzen sind in der Regel auf andere Indizien als die Lichtbild-Analyse zurückzuführen. Selbst bei einer anzunehmenden Leistungssteigerung der MAD-Verfahren in den kommenden Jahren bleibt zum sicheren Nachweis der biometrischen Verbindung von Personaldokumenten zum Passinhaber (d.h. ein Pass = ein und **nur ein** Nutzer) bis auf Weiteres nur der biometrische Vergleich der beiden Fingerbilder aus dem Pass mit den Fingerabdrücken des Reisenden. Dieser Fingerbild-Vergleich dient somit der Zielerreichung einer sicheren

Identitätsfeststellung. Der Vergleich gehört derzeit nicht zum Standardprozess in der Grenzkontrolle, könnte jedoch in Zukunft die bisherigen Kontrollschritte im Verdachtsfall (z.B. bei Alarm eines MAD-Verfahrens) oder bei sonstigen Auffälligkeiten ergänzen. Damit ergibt sich die technische Notwendigkeit, die Fingerbilder beizubehalten – unabhängig vom rechtlichen Rahmen, der durch die EU-Verordnungen 2252/2004 und 2019/1157 ohnehin vorgegeben ist. Eine Diskussion um den etwaigen Verzicht von Fingerbildern im Pass- und Personalausweis ist meines Erachtens nicht erforderlich.

Die Sorge von Kollege Weichert, dass Fingerbilder als nationale Kennziffern genutzt werden können teile ich nicht, da eine nachhaltige Speicherung ja nur im Ausweisdokument erfolgt, die biometrischen Referenzdaten sich somit unter der vollständigen Kontrolle des Bürgers selbst befinden. Es muss sichergestellt bleiben – und darauf vertraue ich – dass weder die Passbehörden noch die Bundesdruckerei bei der Ausstellung des Ausweises eine Kopie der biometrischen Bilder erstellt. Ein nationales Register von Fingerbildern der Bundesbürger sollte es in Deutschland auch weiterhin nicht geben.

Auch die Sorge, dass Fingerbilder von Deutschen Bürgern durch Unberechtigte ausgelesen werden können, ist nicht begründet, da die Fingerbilder durch Extended Access Control (EAC) ausreichend geschützt sind.
https://www.icao.int/Security/FAL/PKD/BVRT/Pages/Document-readers.aspx

Der Vorschlag von Kollege Weichert, statt der Indexfinger den/die Ringfinger oder kleine Finger zu erfassen, ist meines Erachtens nicht im Einklang mit der EU-Verordnung 2019/1157. Auch wenn dort nicht explizit der Index-Finger gefordert wird, ist doch die Intention der Verordnung erkennbar: Auf dem Personalausweis (Identity cards of Union citizens) soll die gleiche ICAO 9303 logische Datenstruktur gespeichert werden, wie sie auch nach EU-Verordnungen 2252/2004 in den Reisepässen Verwendung findet. Wären nur in Deutschen Personalausweisen die kleinen Finger gespeichert, jedoch in allen anderen Ländern die Zeigefinger (wie erwartet), wäre die Identitätsfeststellung im Ausland zumindest behindert. Auch aus technischer Sicht, ist ein Wechsel auf den kleinen Finger nicht sinnvoll: Die Fingerabdruckfläche wäre kleiner, und lieferte weniger Minutien. Je kleiner die Fingerabdruckfläche, desto weniger Gewissheit bietet der biometrische Vergleich. Zudem ist die biometrische Erfassung der Zeigefinger durch die anatomischen Gegebenheiten wesentlich einfacher als beim Ringfinger oder beim kleinen Finger.

Alternativen und Anforderungen an den Anbieter:
Ein noch kontrovers diskutiertes Element im Gesetzentwurf ist die Regelung in Artikel 1 betreffend Passgesetz §1 (5), wonach das Gesetz genau *einen* Anbieter als Lieferanten vorsieht, wobei in E.3 explizit die Bundesdruckerei genannt ist.

Hier sind die Vor- und Nachteile für die Festlegung
auf nur einen Anbieter abzuwägen:

a) Für einen Anbieter (d.h. die Bundesdruckerei) spricht

- Es ist leichter zu erreichen, dass in der technischen Umsetzung im Detail einheitliche Lösungen zum Einsatz kommen. Die zu verwendende Technik wird einmalig geprüft, zertifiziert und dann installiert.
- Gegebenenfalls notwendige Updates zum Schließen von Sicherheitslücken, werden von der aufdeckenden Institution an *einen* Ansprechpartner weitergeleitet und hoffentlich zeitnah verteilt.
- Sofern eine einheitliche Lösung zum einheitlichen Preis für alle Passbehörden festgelegt wird, kommt es nicht zu höheren Kosten für den ländlichen Raum (in dem weniger Umsatz zu erwarten ist, als bei einer Passbehörde in einem Ballungszentrum).
- Auch in anderen föderal organisierten EU-Ländern wurde diese Option gewählt.

b) Für viele Anbieter spricht

- Während die Passproduktion selbst eindeutig eine sicherheitskritische Aufgabe ist, genügt bei der Aufnahme der Lichtbilder und Fingerbilder die Sorgfalt und der Nachweis, dass jegliche Manipulation der erfassten biometrischen Bilder ausgeschlossen werden kann. Dies lässt sich dadurch erreichen, dass die Eignung der Erfassungsgeräte durch eine Zertifizierung der Geräte eingefordert wird.
- Die Grundlage für eine solche Zertifizierung besteht bereits durch die Technische Richtlinie BSI TR-03121-3.2. Siehe:
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03121/tr-03121.html
  Einige Systemanbieter von Erfassungsgeräten wurden bereits nach BSI TR-03121 zertifiziert und sind auf der Homepage des BSI gelistet:
  https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachTR/ZertifizierteProdukte/Enrolment_Stations/Enrolment_Stations_node.html

Mit dieser Liste erfüllt das BSI schon in der aktuellen Fassung des Passgesetzes die Aufgabe nach §6a (3), nämlich die Einhaltung der Anforderungen an Geräte zur Erfassung des Lichtbildes und der Fingerabdrücke festzustellen.

- Es könnten *mehrere* Lieferanten / Betreiber unter Einsatz von verschiedenen Produkten zum Einsatz kommen, wenn diese Produkte nach TR-03121 zertifiziert wurden. Die beste Technologie kann sich im freien Wettbewerb durchsetzen.
- Das Sicherheitsniveau der Technologie verschiedener Anbieter wird immer noch höher sein als die Übermittlung von Lichtbildern durch Dienstleister nach Alternative 2.), wie oben diskutiert.

Diese Abwägung ist nach meinem Eindruck die entscheidende Frage in der Anhörung am 26. Oktober, zu der es verständlicher Weise kontroverse Meinungen gibt.

Ich kann die operativen Gründe für Option a) nachvollziehen. Aus meiner Sicht wird diese Option a) jedoch weder eine höhere biometrische Qualität von Lichtbildern oder Fingerbildern bedeuten noch eine Erhöhung der Sicherheit gegenüber Option b). Zudem ist zu bedenken, dass auch Option b) in jedem Fall eine höhere Sicherheit zur Alternative 2.) darstellt – also zur Übermittlung der Lichtbilder durch den Dienstleister per De-Mail-Übertragung. Biometrische Qualität und Sicherheit werden nur erreicht, wenn die in den Passbehörden aufgestellten Erfassungsgeräte zwingend zertifiziert sein müssen und beim Auftreten von Sicherheitslücken zur Not abgeschaltet werden, wenn der Lieferant nicht zeitnah ein Update bereitstellen kann. Die Notfallabschaltung könnte einen oder mehrere Lieferanten betreffen und sowohl bei Option a) als auch bei Option b) zum Einsatz kommen. Ersatzweise muss die Passbehörde in einem Fall der Abschaltung dann auf die Dienstleister (d.h. die Photographen) verweisen, mit denen sie (die Passbehörde) nach §6a Absatz 3 ja ohnehin über eine normierte Schnittstelle verbunden ist.

In diesem Zusammenhang der Zertifizierung finde ich für die anstehende Entscheidung a.) versus b.) drei Sachverhalte interessant:

i) Aktuell sind nach meinem Kenntnisstand ca. 1000 Geräte zur Erfassung von Lichtbildern in den ca. 6115 Pass- und Personalausweisbehörden im Einsatz.

ii) Die Bundesdruckerei hat derzeit 149 Geräte im Einsatz. Das Zertifikat für das Self-Service-Terminal (SST) ist jedoch auf der Website des BSI nicht gelistet.

iii) Ein Mitmarktteilnehmer der Bundesdruckerei hat derzeit 170 Geräte im Einsatz, wobei das von diesem Unternehmen eingesetzte Gerät nach TR-03121 zertifiziert wurde (Zertifizierungs-ID BSI-K-TR-0359-2019)

Sollte die Entscheidung für Option b) fallen, dann müsste §1(5) im Passgesetz NEU lauten:
Das Bundesministerium des Innern, für Bau und Heimat bestimmt den Passhersteller und macht seinen Namen im Bundesanzeiger bekannt. Die eingesetzten Geräte müssen nach der technischen Richtlinie TR-03121 zertifiziert sein. Die Liste der zertifizierten Geräte wird ebenfalls im Bundesanzeiger bekannt gemacht.
Die Änderung im PAuswG müsste analog erfolgen.

Abschließend - die Notwendigkeit des Gesetzes und des Live-Enrolment:
Wie im FAZ-Beitrag "Ein Pass für Zwei" von Piotr Heller am 20.01.2020 berichtet, ergab eine Umfrage unter den Experten auf der Security Printers Konferenz im Oktober 2019, dass eine relevante Anzahl von Pässen mit gemorphten Lichtbildern in den letzten 5 Jahren berichtet wurden. Darüber hinaus gibt es Hinweise auf eine hohe Dunkelziffer. Diese hohe vermutete Dunkelziffer ist auch durch die fehlenden Detektionsmöglichkeiten von gemorphten Lichtbildern zu erklären. Es gibt derzeit keine verlässliche Möglichkeit, ein gemorphtes Bild als solches zweifelsfrei zu erkennen.

Wir reden seit fünf Jahren über Migration. Ich glaube, dass das nur der Anfang von dem ist, was wir in den nächsten Jahrzehnten als Migration erleben werden. Ein Grund ist, dass der Klimawandel in Afrika viele Menschen dazu zwingen wird, ihre Länder zu verlassen.

Die Menschen in Afrika haben Zugang zum Internet. Sie lesen die Nachrichten aus Europa und sie lesen auch unsere Publikationen, die sich im Allgemeinen mit dem Thema Biometrie befassen. Das weiß ich, da ich Fragen zu unseren Publikationen bekomme. Es ist naheliegend, dass Migranten auch über Morphing-Angriffe Bescheid wissen und in Zukunft eine Flugreise (mit entsprechend manipuliertem Pass) einer Schlauchboot-Seereise vorziehen werden.

Aus diesem Grund steht zu recht im Gesetzentwurf: "*Die Funktion des Passes als Dokument zur Identitätskontrolle ist damit im Kern bedroht*." Das ist noch eine vorsichtige Formulierung! Sollte sich die Kenntnis über die Verwundbarkeit der Gesichtserkennung bei Morphing-Angriffen ausbreiten, dann kann man die derzeitigen Prozesse an der Grenze nur noch als "Abschreckung" vor Angriffen, aber nicht mehr als "Kontrolle" und Abweisung von unerlaubten Grenzübertritten bezeichnen.

Vor dem Hintergrund der massiven Verbreitung biometrischer Systeme an den Grenzen müssen Präventionsmaßnahmen gegen Morphing sowohl die Vermeidung des Einbringens von manipulierten Lichtbildern in nationale Personaldokumente (hier: verpflichtende Aufnahme und Speicherung der Lichtbilder ohne Medienbruch *in* den Passbehörden oder bei den Dienstleistern) als auch die sichere Detektion von gemorphten Bildern in Dokumenten aus Drittstaaten (hier: Forschung und Entwicklung) umfassen.

Mit freundlichen Grüßen

Prof. Dr. Christoph Busch