Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Passgesetzes und weiterer Vorschriften

Christoph Busch (Fraunhofer IGD / Hochschule Darmstadt)

1. Sicherheitsziele in der Begründung des Gesetzes

Das Passgesetz verweist auf Gemeinschaftsrecht. Dennoch sollte die Begründung für das Gesetz deutlich formuliert werden und in diesem Zusammenhang die in der EG Verordnung Nr. 2252/2004 des Rates vom 13. Dezember 2004 vorliegende Begründung aus nationaler Perspektive und heutiger Sicht diskutiert werden.

1.1. Bewertung der Sicherheitsziele

1.1.1. Enrolment

Von den Zielen, die von der ICAO bei der Passbeantragung / -ausgabe angestrebt werden (siehe ICAO-Ziele EP-1 bis EP-3 in Anhang A / Enrolment-Prozess) wird in Europa derzeit kein Ziel umgesetzt. Ein Gewinn an Sicherheit könnte vor allem mit EP-1 erzielt werden. Aus gutem Grund sieht der Passgesetzentwurf (PassG-E) keine zentralen Datenbanken vor.

Bewertung:

Um die über Jahrzehnte gewachsene Datenschutzkultur nicht zu gefährden, gibt es dazu kurzfristig keine Alternative.

1.1.2. Grenzkontrolle

Das wesentliche Sicherheitsziel, das mit dem biometrischen ePass erreicht werden kann, ist die Bindung zwischen ePass und dem Inhaber des Personaldokumentes. Dies kann bei der Grenzkontrolle genutzt werden, um Personen zu detektieren, die mit einem nicht für sie selbst ausgestellten Dokument die Grenze passieren wollen – der sogenannte „look-alike-fraud“. (Dies korrespondiert zu den ICAO-Zielen BC-1 und BC-2 in Anhang A)

Empfehlung:

In die Begründung des Gesetzes sollte die Information aufgenommen werden, mit welcher statistischen Häufigkeit ein solcher Angriff in der Vergangenheit ausgeübt wurde, sofern diese Information verfügbar ist. Gegebenenfalls kann auf die Ergebnisse des VISA-Lagos Pilotprojektes verwiesen werden.

Die Entscheidung, zusätzlich zu dem von der ICAO als obligatorisch spezifiziertem Lichtbild zwei Fingerbilder in den ePass zu integrieren, ist damit begründbar, dass durch die Auswertung einer Zwei-Finger-Präsentation eine gegenüber einem einfachen 2D-Lichtbild höhere Erkennungsleistung erzielt werden kann.

Sofern jedoch die biometrisch gestützten Grenzkontrollen an den EU-Außengrenzen allein auf der Zwei-Finger-Präsentation basieren sollte, würde die Europäische Union quasi zu einer „biometrischen Insel“: Die Prüfung der Bindung von biometrischer Charakteristik zum ePass könnte lediglich für EU-Bürger vorgenommen werden, da Bürger anderer Herkunft keine entsprechenden Referenzen in ihren Pässen vorweisen könnten. Darüber hinaus könnte die Möglichkeit eines Ersatzverfahrens,

die sich mit der Aufnahme einer zweiten biometrischen Charakteristik ergibt, nicht genutzt werden.

Empfehlung:
Beim Ausbau der biometrischen Grenzkontrolle sollte die Verifikation mit 2D-Lichtbildern und die Verifikation mit Fingerbildern in gleichem Umfang betrieben werden.

1.2. Mögliche ergänzende Ziele

Als weiteres Ziel in der Diskussion um den ePass wird die Beschleunigung der Passagierabfertigung insbesondere an den Grenzkontrollen der Flughäfen genannt.
Bewertung:
Obwohl Pilotversuche wie SmartGate (Australien), Privium (Amsterdam) und die Installation bei einer Privatbank in der Schweiz zeigen, dass Zugangskontrollen grundsätzlich durch den Einsatz biometrischer Verfahren beschleunigt werden können, wurde im Pilot BioP II deutlich, dass dieser Vorteil nur den „Viel-Nutzern" (Frequent-Traveller) zu Gute kommt. Im Allgemeinen ist für die Grenzkontrolle an den EU-Außengrenzen von einer Zunahme der Transaktionszeit auszugehen.

2. Diskussion möglicher Risiken

In den folgenden Abschnitten werden die in der Debatte um den ePass genannten Risiken betrachtet.

2.1. Klonen des ePasses

Die Möglichkeit der identischen Reproduktion eines ePasses erscheint schon durch die in der Datenseite eingebauten physikalischen Sicherheitsmerkmale unwahrscheinlich. Auch bei einer exakten Reproduktion des RFID Chips [gru2006] und seiner logischen Datenstruktur ist der Gewinn für einen Angreifer gering. Durch die elektronische Signatur über die Hashwerte der einzelnen Datengruppen ist ein Austausch der biometrischen Daten nicht möglich. Für den Fall, ein geklontes Dokument würde zum Lichtbild eines „look-alike" passen, wäre eine Detektion durch einen Abgleich der Fingerbilder möglich. Zudem: Ohne den technischen Aufwand des Klonens ließe sich – bei Vortäuschung des Passverlustes – ein Pass-Duplikat auf dem Antragswege besorgen.
Bewertung:
unkritisch

2.2. Antragsprozess zum Erhalt eines ePass

Das Antragsverfahren und die Passausgabe erfolgt offensichtlich nicht in allen EU-Ländern mit der notwendigen Sorgfalt. Sollten sich die Experimente einer BBC-Reporterin bewahrheiten, die in 20 EU-Ländern einen ePass unter beliebigen Identitäten kaufen konnte [bbc2006], so ist mit einem „Schwarzmarkt für Pässe" eine kritische Situation entstanden. Diese Situation ist jedoch nicht direkt mit dem Übergang auf den ePass zusammenhängend.
Bewertung:
möglicherweise kritisch – Handlungsbedarf!

2.3. Unberechtigtes Öffnen des ePasses

Diese Möglichkeit kann insbesondere nach der Diskussion über die tatsächliche Entropie der Information in der MRZ nicht prinzipiell ausgeschlossen werden. In einem auf den ersten Blick nahe liegenden Vergleich mit der Sicherheit der DES-Chiffre erscheint selbst der Schlüsselraum 2^{56} heute nicht mehr sicher genug. Im ePass-Szenario liegt jedoch die minimale Transaktionzeit (für das Austesten *eines* von 2^{56} möglichen Schlüsseln) in der Größenordnung von einer Sekunde.
Durch die Randbedingungen der Proximity-Cards (max. 25 cm) und die selbst bei einer Reduktion auf nur noch 2^{20} Schlüssel (ca. 6 Ziffern) abgeschätzte Dauer von 12 Tagen [küg2007] erscheint der Angriff von geringer praktischer Relevanz.
Der Zugriff auf das Gesichtsbild (DG2) ist kein wirklicher Gewinn – ein Foto des ePass-Trägers ließe sich in geringer Zeit anfertigen. Die Rezeption eines Hotels, die den Pass über Nacht behält, kann die Information der DG1 (Name, Geburtsdatum etc.) ohnehin aus der Datenseite entnehmen
Bewertung:
unkritisch.

2.4. Unberechtigtes Mitlesen der Kommunikation des ePasses

Nach Kügler/Naumann [küg2007] ergibt sich aus den Ergebnissen der Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) „MARS“ [bsi2007], dass ein Mitlesen der Kommunikation nur bis zu einer Entfernung von 2,7m möglich ist. Im Folgeschritt wäre noch die mit dem Sitzungsschlüssel chiffrierte Information zu dechiffrieren.
Bewertung:
relativ unkritisch.

2.4.1. Unberechtigtes Sammeln von Passagierdaten

Dabei handelt es sich um ein dem o.g, nachgeordnetes Risiko. Würde die benötigte Dauer zum Öffnen eines ePasses deutlich unterschritten bzw. wäre ein unberechtigtes Mitlesen erfolgreich, wäre es z.B. an Flughäfen bei der Grenzkontrolle oder ähnlichen Personen-Schleusen möglich, Listen von Passanten aufzustellen.
Bewertung:
unkritisch – Dieses Szenario ist bisher auch durch verdeckte Observation des Check-In-Schalters oder durch einen Angriff (z.B. mittels Trojaner) auf die Rechnerinfrastruktur der Grenzkontrolle (elektronische Datenverarbeitung der MRZ-Information) machbar.

2.5. Automatische Bomben

Möglicherweise werden von Terroristen Bomben automatisch gezündet.

2.5.1. Spezialisierte Bomben

Zündung einer Bombe, sobald ein ePass mit einer "Deutschen Chip-ID" detektiert wird. Das Risiko bestünde, wenn Seriennummern systematisch für nationale Kontingente von ePässen vergeben werden. Das Risiko entfällt bei Verwendung von Chips mit zufälliger Unique ID (UID).
Bewertung:
unkritisch.

2.5.2. Personalisierte Bomben

Bei bekannter MRZ einer VIP-Person (z.B. Szenario „Kennedy-Mord“) kann eine Bombe genau dann gezündet werden, sobald der zur bekannten MRZ passende ePass in der Nähe detektiert wird. Der Abstand muss jedoch in der Größenordnung des Proximity-Chips liegen (kleiner 25 Zentimeter).

Bewertung:

möglicher Angriff – Das Risiko ist jedoch durch physikalisches Shielding, d.h. eine abstrahlsichere Tüte (Pass-Booklet, mit Alu-Folie gefütterte Brieftasche etc.) mit geringen Kosten zu kontrollieren [shi2007].

2.6. Haltbarkeit der RFID

Die Hersteller prognostizieren eine Haltbarkeit, die der Gültigkeit der Pässe (10 Jahre) entspricht. Es ist jedoch davon auszugehen, dass das Nutzerverhalten zu sehr unterschiedlichen Gebrauchsspuren an den Dokumenten führen wird. Bei der zu erwartenden physikalischen Belastung ist es nicht unwahrscheinlich, dass ein Anteil der verarbeiteten Chips in den ausgegebenen Pässen **keine** 10 Jahre halten wird.

Bewertung:

möglicherweise kritisch – Wenn die Statistik zu Chip-Lesefehlern an der Grenzkontrolle eine in der Praxis niedrigere Chip-Lebensdauer zeigen sollte, müsste die Gültigkeit auf 5 Jahre angepasst werden können.

2.7. Unzureichende Qualität der biometrischen Charakteristika der Datensubjekte

Durch Umweltbedingungen, handwerkliche Tätigkeit oder auch durch (Haut-) Krankheiten kann die Abbildung der biometrischen Charakteristik „Papillar-Leisten“ nicht in für die Fingerbilderkennung ausreichender Qualität erfolgen. Der Anteil der Bevölkerung, der bespielsweise durch Hautkrankheiten – temporär oder dauerhaft – keine Fingerbilder in ausreichender Qualität liefern kann, wird von Hautärzten auf 3% bis zu 11% geschätzt. Gesicherte Erkenntnisse oder diesbezügliche Statistiken liegen noch nicht vor. Eine realistische Einschätzung der Bedeutung dieses Risikos lässt sich vermutlich nach der gegenwärtigen Erprobungsphase und Fingerbild-Erfassung nach §23a PassG abgeben.

Bewertung:

möglicherweise kritisch – insbesondere bei zivilisationsbedingter Zunahme von Allergien. Die praktischen Auswirkungen lassen sich durch ein etabliertes Ersatzverfahren auch in der Grenzkontrolle (d.h. Gesichtserkennung) minimieren.

2.8. Alterung der Referenzdaten

Der biometrische Vergleich mit einem zehn Jahre alten Fingerbild wird noch einen guten Vergleichswert erbringen.

Der biometrische Vergleich mit einem zehn Jahre alten Gesichtsbild ist bereits heute bei der manuellen Inspektion durch den Grenzbeamten gegebenenfalls schwierig. Im gleichen Umfang ist zu erwarten, dass eine automatische biometrische Gesichtsbild-Erkennung beim Vergleich der Bilder gegebenenfalls keinen guten Vergleichswert liefern wird. Gesicherte Erkenntnisse oder diesbezügliche Statistiken liegen noch nicht vor. Dies bedeutet jedoch nicht notwendiger Weise eine Verschlechterung gegenüber dem bisherigen Kontrollprozess.

Bewertung:
möglicherweise kritisch – Wenn die Statistik zu Falsch-Rückweisungsraten an der Grenzkontrolle einen überproportionalen Anstieg bei hohem Alter der Referenzdaten zeigen sollte, müsste die Gültigkeit des ePasses auf 5 Jahre angepasst werden können.

2.9. Fehlendes Vertrauen der Bürger in den ePass

Bei fehlendem Vertrauen der Bürger in den ePass und die damit zusammenhängenden Prozesse besteht die Gefahr, dass ein hoher Anteil von Bürgern den Pass zerstören könnte.
Bewertung:
möglicherweise kritisch

3. Detail-Kommentare zum PassG-Entwurf

zu Artikel 1 (PassG)
S.7 zu Nr. 1 (§1 Abs. 1): Die Formulierung „*Passpflicht bei Geltungsbereich*“ könnte auf die Schengen-Außengrenzen angepasst werden.
S.9 zu Nr. 3c (§4 Abs. 3): Die Formulierung „*Eine bundesweite Datenbank der biometrischen Daten ...*“ schließt regionale Datenbanken nicht ausdrücklich aus. Nach Einschätzung von Alexander Roßnagel sind vernetzte dezentrale Datenbanken mit einer bundesweiten Datenbank in rechtlicher Hinsicht gleichzusetzen [ros2006]. Damit würde sich ein Widerspruch zu §22a ergeben, da Lichtbilder als biometrische Daten zu betrachten sind (§22a bedingt die Existenz von Lichtbildarchiven in den Meldebehörden oder an anderen Orten)
S.10 zu Nr. 4 (§5 Abs. 1): Es könnte erforderlich werden, die Gültigkeit von 10 Jahren an einen kürzeren Zeitraum anzupassen.
S.14 zu Nr. 9aa (§16 Abs. 2): Die Formulierung „*Biometrische Merkmale*“ sollte durch „*Biometrische Daten*“ ersetzt werden.

zu Artikel 4 (AsylverfahrensG)
S.21 zu Nr. 2b (§16 Abs. 1a): Die Formulierung „*und die Iris*.“ sollte durch *„und das Irisbild.*“ ersetzt werden.

zu Artikel 6 (AufenthaltG)
S.23 zu Nr. 3b (§49 Abs. 1): Die Formulierung „*und die Iris*.“ sollte durch *„und das Irisbild.*“ ersetzt werden.

zu Artikel FreizügigkeitsG
S.26 zu Nr. 1b (§8 Abs. 2): Die Formulierung „*und die Iris*.“ sollte durch *„und das Irisbild.*“ ersetzt werden.

4. Kommentare zur Stellungnahme des Bundesrates

zu Nr. 2: Eine Speicherung des Doktorgrades im Pass / Personalausweis ist nicht wirklich erforderlich.
zu Nr. 5: Die Formulierung zu §16a Satz 5-neu gibt nicht das in der Begründung genannte Ziel wieder.

5. Kommentare zur Drucksache 16/3046 Keine Einführung des elektronischen Personalausweises

Die Aufnahme biometrischer Daten in den elektronischen Personalausweis ist nicht unmittelbarer Bestandteil des vorliegenden Gesetzentwurfes, wird aber gleichwohl im Zusammenhang diskutiert.

Die Aufnahme der ICOA-9303-kompatiblen Logischen Daten Struktur (LDS) in den ePA ist erforderlich, wenn das Dokument nach §1 Abs. 2 des PassG zum Verlassen des Geltungsbereiches des Grundgesetzes über eine Auslandsgrenze berechtigen soll und diese Auslandsgrenze zugleich Außengrenze des Schengen-Raumes ist. Der Anteil der Bürger, die dazu nicht den Pass selbst einsetzen, ist vermutlich gering.

Es sollte aber die Chance genutzt werden, mit dem ePA ein Personaldokument in Umlauf zu bringen, das dem Bürger optional auch die Nutzung der biometrischen Authentisierung in nicht-hoheitlichen Anwendungsfällen ermöglicht (wenn der Bürger dies wünscht). Die Daten könnten bei ausreichender Chip-Kapazität in einer getrennten logischen Datenstruktur abgelegt werden, gegebenenfalls unter Einsatz einer Match-on-Card Lösung. Dabei könnte auf die ISO-Standards 19794-2 oder 19794-8 zurückgegriffen werden.
Dies wäre insbesondere im Bereich eBanking langfristig ein Sicherheitsgewinn und mit der Zunahme der Phishing-Problematik auch hinreichend begründet. Der Verfügungsrahmen könnte dann sinnvoll gestaffelt werden, zum Beispiel:
1.) bis 400 EURO Transaktion bei Einsatz von PIN/TAN
2.) bis 4.000 EURO Transaktion bei Authentisierung mittels ePA
3.) bis 8.000 EURO Transaktion bei Authentisierung mittels ePA plus Fingerabdruck
4.) bis 40.000 EURO Transaktion bei Authentisierung mittels ePA plus nicht-flüchtiger biometrischer Charakteristik (z.B. 3D-Gesichtsmodell, Fingervenenbild)

Es wäre sinnvoll, zum Lesen der Datenstruktur auch in diesem Falle zur ICAO-Spezifikation vergleichbare Sicherheitsstandards zu verlangen.

zu Nr. 2:
Grundsätzlich kann eine biometrische Referenz aus einem oder mehreren gespeicherten biometrischen Samples (Lichtbilder, Fingerbilder, Irisbilder), biometrischen Templates (Menge von gespeicherten Merkmalen z.B. Minutien) oder biometrischen Modellen (z.B. Hidden Markov Modell) gebildet werden (Definitionen nach ISO/IEC JTC1 SC37 SD2v6 Harmonized Biometric Vocabulary [iso2006]).

Ein biometrisches Sample (z.B. das Papillar-Linienbild / Fingerbild) als analoge oder digitale Repräsentation biometrischer Charakteristika (z.B. der Papillar-Leisten) vor dem Prozess der biometrischen Merkmalsextraktion bietet die größtmögliche Interoperabilität und wurde unter anderem deshalb von der ICAO als Speicherformat für die biometrischen Referenzen im ePass gewählt. Die EG Verordnung Nr. 2252/2004 des Rates vom 13. Dezember 2004 und insbesondere die Entscheidung der Kommission vom 28. Juni 2006 über die technischen Spezifikationen der Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten legen Gesichtsbilder und Fingerbilder für den ePass fest.
Es ist unklar, welche Grundlage und Bedeutung die Formulierung *„die derzeit*

bestehenden Regelungen erlauben eine Speicherung der biometrischen Merkmale ausschließlich als Template“ hat?
Für die biometrischen Daten des Fingers gibt es mit den ISO-Standards 19794-2 oder 19794-8 geeignete Template-Datenformate – nicht jedoch für biometrische Daten des Gesichtes!

zu Nr. 4:
Der Bericht zur Untersuchung BioP II zeigt höhere Fehlerraten einerseits bei nicht ausgereiften Mensch-Maschine-Schnittstellen und andererseits bei nicht trainierten Nutzern. Daraus lässt sich jedoch nicht schließen, dass biometrische Erkennungsverfahren grundsätzlich noch keinen brauchbaren Reifegrad erreicht hätten.
Zur Bewertung des Leistungspotenzials sollten die Erfahrungen mit dem AFIS-System des BKA und die Testberichte des National Institute of Standards and Technology (NIST) berücksichtigt werden [nist2006] und [nist2007].

zu Nr. 5 und Nr.7:
Die Formulierungen legen den Eindruck nahe, eine Nutzung biometrischer Daten bei der Authentisierung in privaten Onlinegeschäften würde die Weitergabe biometrischer Daten an den Dienste-Anbieter notwendig machen.

Dies ist nicht der Fall.

Es lassen sich durchaus alternative Konzepte (z.B. Match-on-Card oder auch Renewable Biometrics) zur biometrischen Authentisierung realisieren, ohne das Recht auf informationelle Selbstbestimmung einzuschränken [bus2006 und vee2006].

6. Referenzen

[bbc2006] http://news.bbc.co.uk/2/hi/programmes/panorama/6158927.stm

[bla1996] M. Blaze et. al, Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security, Jan 1996, verfügbar unter: http://theory.lcs.mit.edu/~rivest/bsa-final-report.ps

[bsi2007] BSI: Messung der Abstrahleigenschaften von RFID-Systemen (MARS): Teilbericht zu den Möglichkeiten des passiven Mitlesens einer RFID-Kommunikation, zu Veröffentlichung anstehend 2007

[bus2006] C. Busch, Biometrische Verfahren – Chancen, Stolpersteine und Perspektiven, in Biometrie und Datenschutz – Der vermessene Mensch, Tagungsband zum Symposium des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am 27. Juni 2006, S. 28-53, (2006)

[des1999] http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/

[gru2006] http://www.heise.de/newsticker/meldung/76379

[icao2004a] International Civil Aviation Organization, MRTD/NTWG. Biometrics Deployment of Machine Readable Travel Documents, Version 2.0. ICAO, Mai 2004.

[iso2006] ISO SC37 Harmonized Biometric Vocabulary (Standing Document Version 6 – vom 31.08.2006) http://www.3dface.org/media/vocabulary.html

[küg2007] D. Kügler und I. Naumann, Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass, in DuD 3/2007, S. 176-180, März 2007

[nist2006] National Institute of Standards and Technology: "MINEX – Performance and Interoperability of the INCITS 378 Fingerprint Template", Testbericht, (2006)

[nist2007] National Institute of Standards and Technology: "FRVT 2006 and ICE 2006 Large-Scale Results March 2007", Testbericht, (2007)

[ros2006] A. Roßnagel, Biometrie – Schutz und Gefährdung von Grundrechten, in Biometrie und Datenschutz – Der vermessene Mensch, Tagungsband zum Symposium des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am 27. Juni 2006, S. 56-76, (2006)

[shi2007] RFID-Shielding, http://www.rfid-shield.com/products.php

[vee2006] M. van der Veen et al., Face Biometrics with Renewable Templates, SPIE Conference, 2006

Anhang A

Auszug aus dem Deployment-Report der ICAO [icao2004]:

"There are several typical applications for biometrics during the enrolment process of applying for a passport or visa:
EP-1. The applicant's biometric template(s) generated by the enrolment process can be searched against one or more biometric databases (identification) to determine whether the applicant is known to any of the corresponding systems (for example, holding a passport under a different identity, criminal record, holding a passport from another state).
EP-2. When the applicant collects the passport or visa (or presents themselves for any step in the issuance process after the initial application is made and the biometric data is captured) their biometric data can be taken again and verified against the initially captured template
EP-3. The identities of the staff undertaking the enrolment can be verified to confirm they have the authority to perform their assigned tasks. This may include biometric authentication to initiate digital signature of audit logs of various steps in the issuance process, allowing biometrics to link the staff members to those actions for which they are responsible.

There are also several typical applications for biometrics at the border:
BC-1. Each time travellers (ie MRTD holders) enter or exit a State, their identities can be verified against the images or templates created at the time their travel documents were issued. This will ensure that the holder of a document is the legitimate person to whom it was issued and will enhance the effectiveness of any Advance Passenger Information (API) system. Ideally, the biometric template or templates should be stored on the travel document along with the image, so that travellers' identities can be verified in locations where access to the central database is unavailable or for jurisdictions where permanent centralized storage of biometric data is unacceptable.
BC-2. Two-way check - The traveller's current captured biometric image data, and the biometric template from their travel document (or from a central database), can be matched to confirm that the travel document has not been altered.
BC-3. Three-way check - The traveller's current biometric image data, the image from their travel document, and the image stored in a central database can be matched (via constructing biometric templates of each) to confirm that the travel document has not been altered. This technique matches the person, with their passport, with the database recording the data that was put in that passport at the time it was issued.
BC-4. Four-way check - A fourth confirmatory check, albeit not an electronic one, is visually matching the results of the 3-way check with the digitised photograph on the Data Page of the traveller's passport.

Besides the enrolment and border security applications of biometrics as manifested in one-to-one and one-to-many matching, States should also have regard to, and set their own criteria, in regard to:
SC-1. Accuracy of the biometric matching functions of the system. Issuing States must encode one or more facial, fingerprint or iris biometrics on the MRTD as per LDS standards (or on a database accessible to the Receiving State). Given an ICAO-

standardised biometric image and/or template, Receiving States must select their own biometric verification software, and determine their own biometric scoring thresholds for identity verification acceptance rates – and referral of imposters.
SC-2. Throughput (eg travellers per minute) of either the biometric system or the border crossing system as a whole.
SC-3. Suitability of a particular biometric technology (finger or face or eye) to the border crossing application.