Bundesamt
für Sicherheit in der
Informationstechnik

Abteilungsleiter 2
Kryptologie und Abhörsicherheit

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63 • 53133 Bonn

Deutscher Bundestag
Innenausschuss
Herrn Dr. Heynckes
Platz der Republik 1
11011 Berlin

Datum: **17. April 2007**
Durchwahl: **(0228) 9582- 5500**
IVBB: **(03018) 9582- 5500**
E-Mail: **Gerhard.Schabhueser@bsi.bund.de**
Internet: **http://www.bsi.bund.de**
Dienstgebäude: **Nr. 2**

GeschäftsZ.: **AL 2 – 433-00-00**

Betr.: Öffentliche Anhörung im Innenausschuss des Deutschen Bundestages; Aufnahme biometrischer Merkmale in den Reisepass - Änderung des PassG;
hier: Stellungnahme zur Anhörungsthematik unter dem Blickwinkel der IT- und Chipsicherheit

Bezug: Schreiben Deutscher Bundestag vom 23. März 2007

Berichterstatter: LRD Dr. Gerhard Schabhüser

1. Einleitung

Der elektronische Reisepass ist mit einem kontaktlosen Chip (Radio-Frequency- oder RF-Chip) ausgestattet. Bei diesem Chip handelt es sich um einen Sicherheitschip mit kryptographischem Koprozessor, auf dem neben den bisher üblichen Passdaten auch biometrische Merkmale gespeichert werden.

Die Verwendung von elektronischen Komponenten und biometrischen Daten in Reisedokumenten dient zwei Zielen:

(1) Die Fälschungssicherheit zu erhöhen
(2) Die Bindung des Passes an den Inhaber zu stärken

Die Einführung elektronischer Komponenten, digitaler Daten und zusätzlicher personenbezogener Daten, hier die biometrischen Daten des Inhabers, bedürfen naturgemäß einer adäquaten Absicherung gegen Missbrauch.

Zur Darstellung des Sachverhaltes wird zunächst ein Überblick über die integrierten Sicherheitsmechanismen für den kontaktlosen Chip im deutschen Reisepass geben. In diesem Überblick werden auch die Risiken und implementierten Gegenmaßnahmen diskutiert und bewertet. Im Anschluss wird auf IT-Sicherheitsrelevanten Aspekte des Entwurfs des PassG sowie der Anträge eingegangen.

2. Darstellung der Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass

2.1 Übersicht

Die grundlegenden technischen Spezifikationen für elektronische Reisedokumente werden von der International Civil Aviation Organization (ICAO) – einer Unterorganisation der Vereinten Nationen – standardisiert[1].

Im Chip werden folgende personenbezogenen Daten gespeichert:
- die personenbezogenen Daten der maschinenlesbaren Zone (MRZ)[2] der Datenseite des Passes
- Gesichtsbilddaten des Inhabers und in Stufe 2
- Fingerabdruckdaten des Inhabers.

Zusätzlich sind die Dokumentennummer des Reisepasses sowie organisatorische Daten zu den auf dem Chip abgelegten Dateien wie die Angaben über die Datengruppen und die Zertifikate sowie Hash-Werte der einzelnen Datengruppen und die elektronische Signatur des Passproduzenten über die gespeicherten Daten im Chip gespeichert.

Die Daten auf dem Chip werden nach den Vorgaben der ICAO in mehreren Datengruppen organisiert (s. Tabelle 1). Nur die Datengruppen DG1 (Personendaten) und DG2 (Gesichtsbild) sind gemäß ICAO verpflichtend, alle weiteren Datengruppen können optional verwendet werden.

Auf den deutschen Reisepass werden von diesen optionalen Datengruppen in der zweiten Ausbaustufe zusätzlich die Datengruppe DG3 (Fingerabdrücke) und DG14 (*Chip Authentication Public Key)* aufgebracht.[3]

Die personenbezogenen Daten werden während der Produktion des Passes auf dem Chip gespeichert und sind danach nicht mehr veränderbar.

[1] ICAO; *Machine Readable Documents –PKI for Machine Readable Travel Documents Offering ICC Read-Only Access;* Version 1.1; Oktober 2004
[2] Bestehend aus: Dokumenttyp, ausstellender Staat (oder Behörde), Name, Dokumentennummer, Nationalität, Geburtsdatum, Geschlecht, Ablaufdatum, optionale Daten und Prüfsummen.
[3] EU Kommission; *Spezifikationen für EU-Pässe – Anhang zur Entscheidung 28/VI/2006 der Kommission K(2006)2909*

DG1	Stufe 1	Maschinenlesbare Zone
DG2	Stufe 1	Gesichtsbild
DG3	Stufe 2	Fingerabdrücke
DG14	Stufe 2	Chip Authentication Public Key
DG15	Stufe 1, optional	Active Authentication Public Key
Document Security Object	Stufe 1	Hashwerte aller Datengruppen sowie die elektronische Signatur über diese Hashwerte.

Tabelle 1: Logische Datenstruktur des EU-Reisepasses

2.2 Schutz gegen unberechtigte Benutzung

Durch die Integration von biometrischen Merkmalen in den Chip wird die Bindung eines Reisedokumentes an den legitimen Inhaber gestärkt und der unberechtigten Nutzung von Pässen anderer, ähnlich aussehender, Personen (*look-alike fraud*) entgegengewirkt, indem für den Kontrollprozess die Möglichkeit eröffnet wird, die biometrischen Daten (Gesichtsbild, Fingerabdruck) durch Software-Systeme zusätzlich bewerten zu können. Auf den Chips können die relativ großen Datenmengen biometrischer Merkmale leicht gespeichert werden, während gleichzeitig die Möglichkeit besteht, mit Hilfe von kryptographischen Mechanismen die Authentizität der Daten zu garantieren sowie den unerlaubten Zugriff zu verhindern.

2.3 Fälschungssicherheit

Die Fälschungssicherheit des ePasses wird durch das Zusammenspiel der physikalischen Sicherheitsmerkmale des klassischen Passes, der Sicherheitseigenschaften des Chips und den implementierten kryptographischen Verfahren auf ein völlig neues Niveau gehoben.

2.3.1 Passive Authentisierung

Die Authentizität der im Chip gespeicherten Datengruppen wird über eine elektronische Signatur gesichert, die vom Lesegerät während des Kontrollvorganges verifiziert wird. Diese Signatur kann ausschließlich mit dem privaten Schlüssel des Passproduzenten generiert werden. Eine Manipulation der Daten würde daher beim Kontrollvorgang auffallen. Dadurch kann überprüft werden, dass die signierten Daten von einer berechtigten Stelle erzeugt und seit der Erzeugung nicht mehr verändert wurden.

Zum Signieren und Überprüfen der gespeicherten Daten wird eine global interoperable Public-Key-Infrastruktur (PKI) benötigt. Jedes teilnehmende Land baut dazu eine zweistufige PKI auf, die aus einer *Country Signing Certification Authority* (CSCA) und mindestens einem *Document Signer* (DS) besteht. Die CSCA ist im Kontext der Reisepässe die oberste Zertifizierungsstelle eines Landes[4].

Die CSCA signiert mit ihrem privaten Schlüssel ausschließlich DS-Zertifikate, Passdaten werden von ihr nicht signiert. Entsprechend der Gültigkeitsdauer der Reisepässe (10 Jahre) und der festgelegten Verwendungsdauer des privaten CSCA-Schlüssels (3 bis 5 Jahre) muss der zugehörige öffentliche Schlüssel daher zwischen 13 und 15 Jahren gültig sein.

[4] In Deutschland wird die CSCA vom Bundesamt für Sicherheit in der Informationstechnik (BSI) betrieben

Die *Document Signer* sind zum Signieren der digitalen Daten des Passes berechtigte Stellen, im Normalfall sind das die Passproduzenten. Jeder *Document Signer* besitzt mindestens ein eigenes Schlüsselpaar. Der private Schlüssel wird ausschließlich zum Signieren der digitalen Dokumente verwendet, der zugehörige öffentliche Schlüssel muss von der nationalen CSCA zertifiziert werden. Entsprechend der maximalen Verwendungsdauer von 3 Monaten für einen privaten DS-Schlüssel muss der zugehörige öffentliche Schlüssel zehn Jahre und drei Monate gültig sein. Aufgrund der relativ langen Gültigkeit müssen sehr starke Schlüssel verwendet werden. Als Signaturverfahren sind international RSA, DSA und ECDSA (*Elliptic Curve Digital Signature Algorithm*) zugelassen, für den deutschen Reisepass wird ECDSA verwendet. Die empfohlenen Schlüssellängen sind in Tabelle 2 dargestellt.

Algorithmus	CSCA [Bit]	DS [Bit]	AA [Bit]
RSA / DSA	3072	2048	1024
ECDSA	256	224	160

Tabelle 2: Empfohlene Schlüssellängen

2.3.2 Aktive Authentisierung und Chip-Authentisierung

Die passive Authentisierung garantiert die Authentizität der gespeicherten Daten. Darüber hinaus kann durch einen zusätzlichen Mechanismus auch die Authentizität des Chips selbst sichergestellt werden. Dazu muss der Chip dem Lesegerät gegenüber seine Echtheit beweisen.

Um diesen Nachweis zu erbringen, stehen zurzeit zwei verschiedene Verfahren zur Verfügung:

- die von der ICAO standardisierte aktive Authentisierung (*Active Authentication*) und
- die im Rahmen der *Extended Access Control* (EAC)[5] entwickelte Chip-Authentisierung.

Beide Verfahren basieren darauf, dass in einem sicheren, nicht auslesbaren Bereich des Chips ein Pass-individueller privater Schlüssel gespeichert wird. Der zugehörige öffentliche Schlüssel wird hingegen in einer durch passive Authentisierung geschützten Datengruppe verfügbar gemacht. Der private Schlüssel kann somit vom Chip für die Authentisierung verwendet werden, aber im Gegensatz zu den restlichen Daten nicht kopiert werden.

Im Folgenden werden die beiden Verfahren beschrieben:

- Bei der aktiven Authentisierung erfolgt der Nachweis über die Kenntnis des privaten Schlüssels über ein Challenge-Response-Protokoll, wobei der Chip eine vom Lesegerät gewählte Zufallszahl signieren muss. Der zugehörige öffentliche Schlüssel wird in Datengruppe DG15 angegeben. Als Signaturverfahren sind wiederum RSA, DSA und ECDSA zugelassen, die (relativ kurzen) empfohlenen Schlüssellängen sind in Tabelle 2 unter AA dargestellt.

- Bei der Chip-Authentisierung wird der Nachweis über die Kenntnis des privaten Schlüssels indirekt über den Aufbau eines stark verschlüsselten und integritätsgesicherten Kanal erbracht. Der dabei ausgehandelte starke Sitzungsschlüssel dient der Absicherung der anschließenden Kommunikation. Als

[5] BSI; *Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.0;* Technische Richtlinie TR-03110; 2006

Schlüsseleinigungsverfahren sind DH und ECDH ((*Elliptic Curve) Diffie-Hellman*) zugelassen. Der öffentliche Schlüssel befindet sich in Datengruppe DG14.

Beim deutschen Reisepass wird die Chip-Authentisierung mit ECDH und einer Schlüssellänge von 224 Bit Schlüsseln eingesetzt werden. Die Verwendung dieses Verfahrens ist mit der Einführung der zweiten Stufe des EU-Reisepasses verpflichtend, während die Verwendung der aktiven Authentisierung optional bleibt und im deutschen Pass aus Datenschutzgründen nicht umgesetzt wird:

Durch die Nutzung eines digitalen Signaturverfahrens im Rahmen der aktiven Authentisierung wäre es denkbar, dem Chip Daten zum Signieren „unterzuschieben". Anstelle der im regulären Protokollablauf vorgesehenen „echten" Zufallszahl könnte ein für diesen Zweck präpariertes Lesegerät eine aus Uhrzeit, Ort etc. durch eine Hasfunktion abgeleitete Zahl zum signieren präsentieren. Mit der dann vom Chip signierten Zahl könnte der Lesegerätebetreiber Dritten gegenüber den Beweis über den Zugriff auf den Pass und damit z.B. den Nachweis des Grenzübertrittes führen.

2.3.3 Logische Bindung zwischen Chip und Pass

Ein weiterer Schutz gegen das sogenannte Klonen wird über die logische Verknüpfung dieser Daten mit der zugehörigen Datenseite des Reisepasses erreicht. Die wichtigsten personenbezogenen Daten sind sowohl auf dem Chip (in der Datengruppe DG1) manipulationssicher gespeichert als auch auf der Datenseite in maschinenlesbarer Form in der MRZ durch physikalische Sicherheitsmerkmale fälschungssicher abgedruckt. Durch den automatischen Abgleich dieser Daten miteinander würde ein geklonter Chip in einem nicht ebenfalls gefälschtem Pass im Rahmen des Kontrollvorgangs detektiert. Ein „Klonen" deutscher Reisepässe (auch die der Stufe 1) ist daher ausgeschlossen.

2.4 Zugriffschutz

Die Zugriffschutzmechanismen des deutschen Reisepasses dienen der Vermeidung unautorisierten Auslesens der Daten aus dem Chip. Der Begriff „unautorisiert" muss hierbei genauer differenziert werden: Primär ist darunter der Zugriff auf die Daten eines Passbuches im zugeklappten Zustand zu verstehen, also z.B. während sich der Pass in einer Reisetasche oder Geldbörse befindet (*Basic Access Control*).
Für das Auslesen der Fingerabdruckdaten aus Reisepässen der zweiten Stufe wird diese Anforderung dahingehend erweitert, dass lediglich durch *berechtigte* Lesegeräte ein Zugriff erfolgen kann (*Extended Access Control*).

2.4.1 Basic Access Control

Bereits vor der Einführung des elektronischen Reisepasses waren die personenbezogenen Daten in maschinenlesbarer Form in der MRZ auf der Datenseite des Reisepasses enthalten (mit Ausnahme des Gesichtsbilds, welches zwar auf der Datenseite abgedruckt, jedoch nur bedingt maschinenlesbar durch „scannen" ist). Diese Daten sind jedoch nur mit der Einwilligung des Passinhabers lesbar – nur wer Zugriff auf den Reisepass hat, kann auch den Inhalt der Datenseite lesen. Solange der Reisepass geschlossen verwahrt wird, sind die aufgedruckten Informationen vor „unberechtigtem Zugriff" geschützt. Im Rahmen einer Grenzkontrolle wird der Reisepass an einen Beamten übergeben. Durch diese Übergabe stimmt der Reisende einer Überprüfung seiner personenbezogenen Daten zu.
Der grundlegende Zugriffschutz soll für die im Chip abgelegten Daten genau die Eigenschaften des bisherigen Reisepasses nachbilden: Um auf die im Chip gespeicherten Daten zugreifen zu können, muss das Lesegerät die Daten der MRZ

kennen. Diese werden durch optischen Zugriff auf die Datenseite des Reisepasses gewonnen.
Die technische Umsetzung erfordert, dass sich das Lesegerät gegenüber dem Chip authentisieren muss. Für diese Authentisierung benötigt das Lesegerät einen Zugriffschlüssel, der sich aus den Daten der MRZ des Reisepasses ableitet. Das Lesegerät liest also erst die MRZ optisch, berechnet daraus den Zugriffschlüssel und kann sich dann gegenüber dem Chip authentisieren.
In die Berechnung des Zugriffschlüssels gehen die Passnummer, das Geburtsdatum des Inhabers und das Ablaufdatum des Reisepasses ein. Daraus wird ein Hash-Wert berechnet, aus dem die initialen Schlüssel für die Verschlüsselung und die Integritätssicherung abgeleitet werden. Diese werden dann für das Aushandeln der dynamischen 112 Bit langen Sitzungsschlüssel verwendet.

Um das unberechtigte Auslesen des Reisepasses („aktives Auslesen“) zu verhindern, ist die Stärke des Mechanismus ausreichend, da das Ausprobieren aller Schlüssel in kurzer Zeit unmöglich ist – selbst wenn der Angreifer Zusatzinformationen hat, wie Zusammenhänge zwischen Passnummer und Ablaufdatum. Denn der komplette Ablauf einer einzelnen BAC-Authentisierung benötigt bereits ca. 1 Sekunde an Berechnungs- und Kommunikationszeiten. Wie in Tabelle 3 dargestellt, resultieren aus bereits sehr kleinen effektiven Schlüssellängen sehr große Zeiten. Wie sich zeigt, ist ein aktives Auslesen praktisch unmöglich.

Art des Suchraums	Mögliche Schlüssel	Maximale Dauer
Voller Suchraum	2^{56}	2 Milliarden Jahre
Reduzierter Suchraum	2^{40}	35000 Jahre
Stark reduzierter Suchraum[6]	2^{30}	34 Jahre
Überwiegend bekannter Suchraum	2^{20}	12 Tage

Tabelle 3: Zeiten für das unberechtigte aktive Auslesen

Selbst bei einer sehr unwahrscheinlichen Reduzierung des Suchraums auf nur noch 2^{20} Schlüssel (ca. 6 Ziffern) dauert der Angriff noch bis zu 12 Tagen. Hierbei müsste ständiger und direkter Kontakt zur Zielperson bestehen, um im Ergebnis die unbekannten 6 Ziffern in Erfahrung zu bringen. Dies dürfte jedoch mit einfacheren Mitteln (z.B. durch sogenanntes *„social engineering“*) und in kürzerer Zeit in Erfahrung zu bringen sein.

Zu beachten ist auch Reichweite, über die ein aktives Auslesen überhaupt ermöglicht werden kann. Nach den Ergebnissen einer vom BSI beauftragten Studie[7] ist ein aktives Auslesen eines ISO 14443 konformen Chips im ePass nur in einer maximalen Reichweite von ca. 15-25 cm möglich (unter der Voraussetzung einer bekannten MRZ!).

2.4.2 Extended Access Control

Mit der Einführung der zweiten Stufe des elektronischen Reisepasses werden nach Vorgaben der EU die Fingerabdrücke des Passinhabers auf dem Chip gespeichert.

[6] Dieser stark reduzierte Suchraum setzt bereits Detailwissen (z.B. das exakte Geburtsdatum und eine starke Einschränkung der Behördenkennziffer) über die Zielperson voraus.
[7] BSI; *Messung der Abstrahleigenschaften von RFID-Systemen (MARS); Teilbericht zu den Möglichkeiten des passiven Mitlesens einer RFID-Kommunikation*; zur Veröffentlichung anstehend.

Sensitive personenbezogene Daten wie Fingerabdrücke bedürfen eines besonders starken Schutzes und vor allem der Vorgabe einer engen Zweckbindung. Innerhalb der Arbeitsgruppe zur technischen Standardisierung des EU-Reisepasses wurde daher basierend auf einer Technischen Richtlinie des BSI die Spezifikation eines erweiterten Zugriffschutzes ausgearbeitet, des so genannten *Extended Access Control* (EAC). Das Ziel dieses erweiterten Zugriffschutzes ist es, die im Chip abgespeicherten Fingerabdruckdaten ausschließlich Lesegeräten zugänglich zu machen, die von der Pass-ausstellenden Nation autorisiert wurden.

Funktionsweise des erweiterten Zugriffschutzes
Der Chip zwingt jedes Lesegerät, sich gegenüber dem Chip als berechtigt „auszuweisen", bevor es Zugriff auf die Fingerabdruckdaten erhält. Das Verfahren wird Terminal-Authentisierung genannt und basiert auf einer PKI für Lesegeräte, die im Folgenden näher beschrieben wird. Der Terminal-Authentisierung ist die Chip-Authentisierung vorgeschaltet, die neben der Echtheitsüberprüfung des Chips auch eine stark verschlüsselte Kommunikation zwischen Lesegerät und Chip aufbaut. Dadurch ist garantiert, dass alle nachfolgend übertragenen Daten, insbesondere die Fingerabdruckdaten, stark verschlüsselt werden und nicht unberechtigt abgehört werden können.

Für die Durchführung der Terminal-Authentisierung muss das Lesegerät mit einem Schlüsselpaar und einer vom Chip verifizierbaren Zertifikatskette ausgestattet werden. In diesen Zertifikaten sind die Rechte des Lesegeräts exakt festgelegt. Dabei bestimmt immer das Land, das den Reisepass herausgegeben hat, auf welche Daten ein (ausländisches) Lesegerät zugreifen kann. Durch dieses Vorgehen ist sichergestellt, dass Lesegeräte nur auf die Daten zugreifen können, für die sie auch legitimiert wurden.
Die Zertifikate der Lesegeräte werden von einem *Document Verifier* (DV) ausgestellt. Ein DV verwaltet eine Reihe von Lesegeräten, z.B. die Lesegeräte, die im Rahmen der Grenzkontrolle verwendet werden. Die DV-Zertifikate werden wiederum von einer nationalen Wurzelinstanz herausgegeben, der *Country Verifying Certification Authority* (CVCA). Der öffentliche Schlüssel der nationalen CVCA wird auf dem Chip gespeichert und stellt eine Art Vertrauensanker dar. Ein berechtigtes Lesegerät muss sich also mithilfe eines privaten Schlüssels und einer Zertifikatskette gegenüber dem Chip authentisieren, wobei die Zertifikatskette mit dem auf dem Chip gespeicherten öffentlichen Schlüssel der nationalen Wurzelinstanz enden muss.
Sollen ausländische (d.h. EU und Drittstaaten) Lesegeräte zum Zugriff auf die gespeicherten Fingerabdruckdaten berechtigt werden, muss daher die nationale CVCA für den entsprechenden ausländischen DV ein Zertifikat ausstellen.

2.5 Abhören der Kommunikation

Neben dem aktiven Auslesen ist grundsätzlich auch das passive Mitlesen einer Pass-Leser-Kommunikation und nachträgliche Entziffern als Angriff denkbar. Dieser Angriff ist aus rein kryptographischer Sicht bei Pass-Leser-Kommunikationen erfolgversprechend, wenn ausschließlich das Basic Access Protokoll eingesetzt wird und setzt eine fehlerfreie Aufzeichnung des Schlüsseleinigungsverfahren durch den Angreifer voraus[8]. Nach aktuellen Ergebnissen einer BSI-Studie[9] ist das fehlerfreie Mitlesen bis zu einer Entfernung von 2 m möglich. Ab einer Entfernung von 2,7 m konnte die Kommunikation jedoch nicht mehr erfolgreich mitgelesen werden.

[8] Treten Messfehler auf, so steigt durch die Fehlervervielfältigung der Entschlüsselung der Aufwand exponetiell an.
[9] BSI; *Messung der Abstrahleigenschaften von RFID-Systemen (MARS); Teilbericht zu den Möglichkeiten des passiven Mitlesens einer RFID-Kommunikation*; zur Veröffentlichung anstehend.

Die Praxisrelevanz dieses Angriffes ist nach hiesiger Einschätzung gering, da die durch einen solchen Angriff kompromittierbare Information (Inhalt der MRZ und ein digitales Photo des Passinhabers) mit weniger aufwendigen Methoden zu gewinnen sind.

Wird jedoch die Chip-Authentisierung durchgeführt, die innerhalb Europas für alle Lesegeräte (sofern vom Chip unterstützt) verpflichtend ist, auch wenn kein Zugriff auf die Fingerabdrücke erfolgt, werden alle personenbezogenen Daten grundsätzlich stark verschlüsselt übertragen. In dem Fall ist das nachträgliche Entziffern einer mitgelesenen Pass-Leser-Kommunikation nicht möglich.

2.6 Chip-Sicherheit

Die im Pass integrierten RF-Chips sind Sicherheitschips, deren Sicherheitseigenschaften im Rahmen eines Evaluierungs- und Zertifizierungsverfahrens nachgewiesen wird bzw. wurde. Die Sicherheitsanforderungen sind in spezifischen, vom BSI entwickelten Protection Profiles[10] festgelegt. Es handelt sich hierbei um „State of the Art“ Sicherheitstechnologie, in dem Deutschland (zusammen mit Frankreich) die Technologieführerschaft inne hat.

2.7 Sicherheitsanforderungen an die Lesesysteme

Bei der Bewertung des Sicherheitsniveaus des ePass ist natürlich zu berücksichtigen, dass das Lesesystem die angebotenen Sicherheitsfunktionen korrekt und zuverlässig nutzt. Dazu sind Konformitäts- und Sicherheitsnachweise für die Lesesysteme vorgesehen. Die Anforderungen werden in Form von Technischen Richtlinien und Protection Profiles formuliert.

3. Stellungnahme zum Gesetzentwurf der Bundesregierung zur Änderung des PassG

Aus dem Blickwinkel der IT-Sicherheit ist der Entwurf zur Änderung des PassG nicht zu beanstanden. Dabei haben insbesondere die folgenden Paragraphen Einfluss auf die IT- und Chipsicherheit:

3.1: § 4 , Abs. 2, Nr. 5: Erhöhung der Sicherheit für das Basic Access Protokoll.

Durch die Anforderung, dass die Passnummer keinen erkennbaren Zusammenhang zu den sonstigen Daten der MRZ und damit der BAC-Schlüssel haben darf, wird die Entropie des BAC-Schlüssels erhöht. Dies wird ebenfalls durch die Erweiterung des Zeichensatzes erreicht. Diese Änderung ist im Sinne der IT-Sicherheit zu begrüßen.

3.2: § 4, Abs. 3: Integration des RF-Chips und Anforderungen an die Manipulationssicherheit und Zugriffskontrolle

Über § 4, Abs. 3 wird die EG Verordnung (EG) Nr. 2252/2004 umgesetzt. Dadurch werden automatisch die Sicherheitsmechanismen wie in Kapitel 2 dargestellt verpflichtend.

[10] BSI; *Protection Profile for Machine Readable Travel Document with "ICAO Application", Basic Access Control*; Version 1.0
BSI; *Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control*; Version 1.0

3.3: § 6a: Einführung einer elektronischen Passdatenübertragung und Anforderungen an die einzusetzende Sicherheitstechnik

Durch Abs. (2) und (3) wird sichergestellt, dass die im Rahmen des Antragsprozesses erhobenen Informationen angemessen abgesichert werden. Dazu wurde vom BSI in Zusammenarbeit mit dem BKA eine Technische Richtlinie zu Passdatenübertragung entwickelt, die Bestandteil der in Abs. (3) Rechtsverordnung werden soll.

3.4: § 16a: Prüfberechtigung der biometrischen Daten.

Um das Ziel (2) (siehe Einleitung) zu erreichen, ist das Auslesen der biometrischen Daten und der Abgleich mit einem Live-Bild (bzw. dem gedruckten Gesichtsbild) erforderlich. Hierzu wird hier die Rechtsgrundlage geschaffen. Durch die gemäß § 4, Abs. 3 verpflichtende Zugriffskontrolle auf die Daten des Chips wird hier implizit eine entsprechende Sicherheitsinfrastuktur für die Kontrollebene verpflichtend.

4. Stellungnahme zum Antrag der Fraktion der FDP [BT 16/854]

4.1 Die Aussagen zum aktiven Auslesen und passiven Auslesen können vom BSI so nicht bestätigt werden. Aufgrund einer aktuellen, vom BSI beauftragten Studie[11] ist das aktive Auslesen realistisch bis zu einer Entfernung von ca. 25 cm (siehe 2.4.1) und ein fehlerfreies Mitlesen bis zu einer Entfernung von weniger als 2,7 m (siehe 2.4.4) möglich.

4.2 Die Generierung der Passnummer wird ja durch § 4 Abs 2 Nr. 5 neu geregelt. Die Entropie des BAC-Schlüssels kann realistisch auf ca. 40 Bit geschätzt werden. Für die Sicherheitsziele, die mit dem BAC-Protokoll erreicht werden sollen, ist das nach h. E. ausreichend (siehe 2.4.1 und 2.5).
Für das aktive Auslesen der Fingerabdrücke werden autorisierte Leser benötigt, die im Rahmen des EAC-Protokolls eine starke Verschlüsselung zwischen Leser und Passchip aufbauen. Die Sicherheit ist mit 112 Bit vergleichbar zu der in SSL implementierten.

4.3 Die Entzifferung einer nur mit BAC-geschützten, vorab fehlerfrei aufgezeichneten Kommunikation ist mit entsprechendem Aufwand, der durch § 4 Abs. 2 Nr 5 deutlich erhöht wird, im Prinzip möglich. Der technische Aufwand des fehlerfreien Mitlesens, der Fehlerkorrektur und der Entzifferung stehen nach h. E. aber in keinem Verhältnis zum erwarteten Informationsgewinn (siehe 2.5).
Durch die Implementierung der Chip-Authenisierung (siehe 2.3.2) kann jedes aktive Lesegerät einen solchen Angriff verhindern, indem es die Chip-Authentisierung durchführt und in diesem Schritt einen nicht entzifferbaren kryptographischen Tunnel erzeugt.

4.4 Die im Rahmen der passiven Authentisierung, der Chip-Authentisierung und des Extended Access Control eingesetzten Algorithmen sind von ihren Schlüssellängen hinreichend dimensioniert. Die Public Key Verfahren werden auch im Bereich des staatlichen Geheimschutzes eingesetzt. Der symmetrische Algorithmus Triple-DES ist nach h. E. langfristig nicht entzifferbar.

[11] BSI; *Messung der Abstrahleigenschaften von RFID-Systemen (MARS); Teilbericht zu den Möglichkeiten des passiven Mitlesens einer RFID-Kommunikation*; zur Veröffentlichung anstehend.

5. Stellungnahme zum Antrag der Fraktion der FDP [BT 16/3946]

5.1 Wie in Kapitel 4 schon erläutert, sind nach h. E. die Schutzmechanismen für die Gültigkeitsdauer des Passes/Personalausweises ausreichend.

5.2 Ziel der Biometriestudie **BIOP II**, die von BSI und BKA durchgeführt wurde, war eine auf Grund wissenschaftlicher Kriterien angelegte Erprobung der drei biometrischen Verfahren (Gesichts-, Fingerabdruck- und Iriserkennung) vor dem Hintergrund der bevorstehenden Anwendung biometrischer Merkmale in Reisedokumenten.

Die in BioP II erreichten Erkennungsleistungen lassen die Eignung biometrischer Systeme für einen Praxiseinsatz erkennen. Die Testteilnehmer bedienten die biometrischen Systeme im Selbstbedienungsmodus. Bei ungeübten Personen führte dies zu einer schlechteren Erkennungsleistung (höhere Falschrückweisungsrate). Für den Echteinsatz biometrischer Verfahren im hoheitlichen Bereich ist die Bedienung der Systeme mit Unterstützung geschulter Personen (Grenzkontrollbeamte) vorgesehen.

5.3 Für die Onlineauthentiserung ist der Rückgriff auf die biometrischen Daten des ePA nicht vorgesehen. Der ePA dient in diesem Fall als Personal Secure Environment und wird durch eine PIN vom Inhaber freigeschaltet.

6. Stellungnahme zum Antrag der Fraktion Bündnis90/Die Grünen [BT 16/4159]

6.1 Die Forderung, die Biometrie-Daten nur für den 1:1 Abgleich einzusetzen ist in §16a PassG vorgesehen.

6.2 Die Forderung international gültige, grundlegende Datenschutzstandards bei der Durchführung biometrischer Grenzkontrollen zu etablieren, wird durch die aktive Mitgestaltung (und teilweise der Federführung Deutschlands) in den relevanten Normungsgremien Rechnung getragen.

7. Stellungnahme zum TA-Bericht „Biometrie und Ausweisdokumente“ [BT 15/4000]

7.1 Die in der EG Verordnung (EG) Nr. 2252/2004 realisierte Lösung entspricht der in der TA-Studie dargestellten Handlungsalternative 2.

7.2 Wie in 6.2 ausgeführt ist Deutschland überaus aktiv eigene Beiträge in die ICAO und EU Gremien einzubringen. Dies entspricht einer der Forderungen der TAB-Autoren im Ausblick. Konkret wurde das BAC auf Drängen Deutschlands in den ICAO-Empfehlungen aufgenommen. Das EAC-Protokoll in der EG-Verordnung wurde maßgeblich von Deutschland mitgestaltet.

elektr. gezeichnet

Dr. Gerhard Schabhüser