

08. Juli 2005

Anfrage

**der Abgeordneten Mag. Maier, Parnigoni, Kaipel, Ulrike
Königsberger-Ludwig
und GenossInnen
an die Bundesministerin für Inneres
betreffend „Biometrie – Hochsicherheitspässe: Einführung –
Sicherheit – Datenschutz – Kosten – Nutzen?“**

Der Rat der Europäischen Union hat bereits am 13. Dezember 2004 die EU-Verordnung EG 2252/2004 http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32004R2_252:EN:HTML verabschiedet und die Aufnahme eines digitalen Gesichtsbildes und Fingerabdrücke als biometrische Merkmale in europäischen Reisepässen ab 2006 bzw. 2008 beschlossen. Gem. Art 6 der VO 2252/04 sind die Mitgliedsstaaten zur Integration von biometrischen Merkmalen binnen einer 18- und 36 Monatsfrist nach Notifizierung der technischen Spezifikationen durch die Europäische Kommission verpflichtet. Die biometrischen Merkmale sollen auf einem kontaktlosen Chip gespeichert werden. Vorerst soll das Bild des Passinhabers und der maschinenlesbare Teil (MRZ) gespeichert werden, Fingerabdrücke sollen in der EU später hinzukommen. Weltweit ist nur das Passbild notwendig, um die Interoperabilität zu gewährleisten (Digitalisierung mit jpeg). Das Bild wird digital gespeichert und durch eine digitale Signatur verschlüsselt.

Öffentliche Diskussionen darüber fanden in den EU-Mitgliedstaaten bzw. in deren nationalen Parlamenten zur Einführung der Hochsicherheitspässe - insbesondere zur Kosten-Nutzen Frage – bislang kaum statt!

Trotz technischer Mängel und ungeklärter datenschutzrechtlicher Probleme beabsichtigt die österreichische Bundesregierung allerdings noch in

diesem Jahr Reisepässe mit biometrischen Daten (vorerst ohne digitalem Fingerabdruck) einzuführen. Es fehlen aber beispielsweise weiterhin zuverlässige Sicherheitsstandards für biometrische Daten im Pass. Bei einer zehnjährigen Gültigkeit von Reisepässen kann überdies heute niemand ernsthaft ausschließen, dass die Daten durch Sensoren unbemerkt gelesen, kopiert oder verändert sowie missbräuchlich verwendet werden. Das ist auch Teil des Ergebnisses einer kürzlich vorgelegten Studie des „Bundesamtes für Sicherheit in der Informationstechnik“, immerhin eine nachgeordnete Behörde des deutschen Bundesinnenministeriums.

Auch die damit verbundenen finanziellen Belastungen für den Bund, die einzelnen Passbehörden und die PasswerberInnen sind nicht geklärt. Zu befürchten ist, dass die Passbehörden und die PasswerberInnen die dadurch entstehenden Systemkosten und Mehrkosten zu tragen haben.

In der Parlamentarischen Anfrage vom 18.06.2003 betreffend „Bürgerfreundliche Verwaltung contra Zentralisierungstendenzen des Bundes“ wurde u.a. auch die Einführung der sog. Hochsicherheitspässe angesprochen und einige Problemstellungen aufgezeigt. Sie war damals u.a. wie folgt begründet:

„Reisepässe – Vollziehung des Passgesetzes

Ähnliches ist durch die Einführung des Hochsicherheitspasses etwa ab 2005 oder 2006 zu befürchten. Bekanntlich stellt das zu Jahresbeginn 2003 bei der Stadt in Betrieb genommene Passamt neue Reisepässe innerhalb von 15 Minuten aus. Die „Pass-Rohlinge“ stammen von der Staatsdruckerei. Gleichzeitig mit der von der EU bis 2006 terminisierten Einführung des „Hochsicherheitspasses“ will der Bund die Herstellung der Reisedokumente bei der Staatsdruckerei zentralisieren. Das wird für die KundInnen und Kunden des Salzburger Passamtes bedeuten

- Kein one-stop Verfahren*
- Lange Wartezeiten*

- *Druckmonopol bei einem zentralen Konsortium privater bzw. privatisierter Unternehmer*
- *Die Städte und Gemeinden müssen einen Vertrag zwischen Innenministerium und der Staatsdruckerei erfüllen, den sie nicht kennen und auf den sie keinerlei Einfluss haben.*
- *Zahlen müssen die Städte und Gemeinden, leiden müssen die BürgerInnen*

Der Bund begründet die Einführung des neuen Passes in erster Linie mit Sicherheits- bzw. mit technischen Argumenten. Tatsächlich wurden aber bei der Privatisierung der Staatsdruckerei Überkapazitäten geschaffen, die jetzt auf Kosten der Städte und Gemeinden offensichtlich gefüllt werden müssen. Auch unter Beachtung der erhöhten Sicherheitsstandards müsste auch künftig eine dezentrale Pass-Herstellung möglich sein."

Beantwortet werden konnten diese Fragen damals noch nicht.

Die Budgetanfrage von Abg. Mag. Johann Maier nach den Mehrkosten wurde von Ihnen am 21. März 2005 wie folgt beantwortet:

„Es sind mit Mehrkosten für das Passbuch, die Integration des Chips und die Einbringung der Daten des Antragstellers in das Passbuch sowie auf den Chip zu rechnen.

Diese Kosten wirken sich auf den von den Passbehörden zu entrichtenden Preis des Passes aus."

Zur Zeit nimmt international die Kritik an der kurzfristig beabsichtigten Einführung dieser sogenannten Hochsicherheitspässen mit biometrischen Merkmalen zu. Neben der generellen Sinnhaftigkeit von derartigen Hochsicherheitspässen wurden in den letzten Wochen und Monaten u.a. allfällige Risiken, RFID-Chip, Fälschungssicherheit, Datenintegrität, Datenverknüpfung, Gültigkeitsdauer, Kosten und Wartefristen für Passausstellung diskutiert. Die Erfassung und Verwendung biometrischer Daten muss in Österreich überdies auch im Zusammenhang mit dem

„Erkennungsdienst Neu“ des BMI gesehen werden (Erkennungsdienstliche Datenbank sowie Digitale Lichtdatenbank).

Der deutsche Bundesbeauftragte für Datenschutz, Peter Schaar, hat daher mehr Zurückhaltung bei der Speicherung von Daten gefordert. Angesichts rasanter technologischer Entwicklungen und zunehmender Regeln zum Schutz der inneren Sicherheit äußerte Schaar am 19.04.2005 den Wunsch, „dass der Datenschutz ernster genommen wird“. Er forderte ein Moratorium, die Einführung von Hochsicherheitspässen soll in Deutschland um ein Jahr verschoben werden. So könnte die Zeit genützt werden, an der Ausreifung der Technik zu arbeiten, die oft nicht so zuverlässig funktioniere wie angenommen, so Schaar. Es müsse zu einer transparenten Abwägung von Kosten und Nutzen biometrischer Systeme kommen.

Besonders kritisch wird von Konsumenten- und DatenschützerInnen der Einsatz von RFID-Chip´s gesehen. Laut der zitierten EU-Verordnung sollen die europäischen Reisepässe und Dokumente als Speichermedium einen RFID-Chip enthalten. RFID-Systeme bergen aber derzeit noch eine Vielzahl ungelöster Risiken (Verfälschen der Daten, Abhören der Funksignale, Störung des Datenaustausches etc.). Dies ergibt sich auch aus der inneramerikanischen Diskussion. Bürgerrechtsgruppen, High-Tech-Firmen und die Reisebranche haben Bedenken gegen Teile dieser Technologie, vor allem gegen RFID. Die Funktechnik gilt als unsicher. Dieser Chip ermöglicht ein berührungsloses Lesen der Reisepassinformation und möglicherweise damit auch eine flächendeckende Überwachung von PassnutzerInnen. Wer über entsprechende Lesegeräte verfügt kann damit einerseits öffentliche wie private Räume überwachen, andererseits aber auch die Menschen selbst. Die informationelle Selbstbestimmung ist damit am Ende.

Vorerst kam zur Einführung von Hochsicherheitspässen viel Druck auch von den USA (Patriot act):

Seit 26.Juni 2005 gelten neue Einreisebestimmungen in den USA, grundsätzlich wird nun ein maschinenlesbarer Pass benötigt. Nach der ursprünglichen US-Vorgabe hätten nach dem 26.Oktober 2005 ohne Visum nur die Person in die USA reisen dürfen, die über einen maschinenlesbaren Pass mit einem biometrischen Kennzeichen verfügen. Der von der EU angestrebten Fristverlängerung bis Ende August 2006 wurde nun durch die amerikanische Administration zugestimmt. Nur wer einen so genannten Hochsicherheitspass besitzt, darf nach dem 31.Oktober 2006 ohne Visum in die USA einreisen. Verlangt wird dafür ein maschinenlesbarer Pass mit biometrischen Daten (Visa-Waiver-Programm). Mit Stichtag 1.September 2006 sollen Pässe mit einem biometrischen Kennzeichen in allen Mitgliedsstaaten der EU eingeführt werden. Eine frühere Einführung obliegt den Mitgliedsstaaten. Die USA selbst planen die Einführung von Pässen mit nur einem biometrischen Merkmal (Gesichtsfeld) nicht vor 2007!

Mit entscheidend ist, ob diese so genannten Hochsicherheitspässe auch fälschungssicher sind. Bei den aktuellen Pässen dürfte dies europaweit nicht der Fall sein. Daher werden in Österreich durch das BMI auch so genannte „Dokumentenberater“ in anderen Staaten eingesetzt.

„Schlepperorganisationen versuchen vermehrt, Personen mit ge- oder verfälschte Reisedokumenten per Flugzeug illegal in den Schengen-Raum zu schleusen. Deshalb sind seit November 2003 speziell geschulte ExekutivbeamtInnen und -beamte als Dokumentenberater im Ausland im Einsatz.

Sie informieren das Personal von Fluglinien, Bedienstete von Einwanderungsbehörden und mit der Visa-Ausstellung befasste Personen österreichischer Vertretungsbehörden über Trends und Entwicklungen bei Dokumentfälschungsdelikten und helfen bei der Erkennung gefälschter Reisedokumente. Die neuen Dokumentenberater sollen ab Herbst 2005 in

Moskau, Skopje, Sarajewo und New Delhi eingesetzt werden." (BMI – Aktuell 20.05.2005)

Die unterzeichneten Abgeordneten richten daher an die Bundesministerin für Inneres nachstehende

Anfrage:

1. Sind Sie bereit, einem Moratorium – d.h. einem Aufschub der Einführung der sogenannten Hochsicherheitspässe in Österreich bis zumindest 2006 – zuzustimmen? Wenn nein, warum nicht?
2. Ab welchem Zeitpunkt soll es aus Sicht Ihres Ressorts diese sog. Hochsicherheitspässe mit beiden biometrischen Merkmalen in Österreich geben?
3. Hält das Innenministerium an dem Ziel fest, im Jahr 2005 (Oktober?) die neuen sog. Hochsicherheitspässe mit dem RFID-Chip auf dem das digitale Passbild gespeichert ist, einzuführen? Wenn ja, mit welcher Begründung?
4. Sind in Österreich Großversuche (bzw. zumindest ein Probelauf wie bei der e-card) zur Zuverlässigkeit und Fehleranfälligkeit biometrischer Systeme vor der Einführung von biometrischen Hochsicherheitspässen geplant? Wenn nein, warum nicht?
5. Halten Sie die derzeit in Anwendung befindlichen biometrische (Kontroll)Verfahren zu Hundertprozent einsatzbereit?
6. Ist es richtig, dass mit Beginn des Jahres 2008 EU-weit auch die Speicherung von Fingerabdrücken in den sogenannten Hochsicherheitspässen auf einem RFID-Chip erfolgen soll?

Wie viele und welche Fingerabdrücke sollen dabei abgenommen werden?

7. Welche Stellungnahmen wurden von Österreich zur Einführung von sogenannten Hochsicherheitspässen auf europäischer Ebene (z.B. EU-Ministerrat) hinsichtlich der Technik, Datenschutz, rechtliche Fragen etc. abgegeben?
8. Die USA werden voraussichtlich auf die Speicherung von Fingerabdrücken in Pässen verzichten. Mit welcher konkreten Begründung wurde in der EU die digitale Speicherung von Fingerabdrücken verlangt?
9. Welche konkrete Schlüsseltechnik wurde auf EU-Ebene für Hochsicherheitspässe festgelegt (technische Spezifikationen)? Was bedeutet dies beispielsweise für die Herstellung von den sogenannten Hochsicherheitspässen in Österreich?
10. Welche technischen Spezifikationen wurden für das digitale Passbild festgelegt?
11. Welche technischen Spezifikationen wurden für die Fingerabdrücke festgelegt?
12. Falls noch keine technischen Spezifikationen festgelegt wurden: Wann wird voraussichtlich eine Entscheidung darüber getroffen werden?
13. Welche konkrete Sicherheits- oder Schlüsseltechnik kommt in den österreichischen Hochsicherheitspässen zur Anwendung, damit die digitalen Passdaten weder gelesen noch manipuliert werden können?

14. Wie wird die (technische) Kompatibilität der Infrastruktur zwischen den EU-Mitgliedstaaten gesichert?
15. Was wird nach allgemeiner Schätzung innerhalb der EU d.h. bei allen Mitgliedsstaaten die Einführung dieser sogenannten Hochsicherheitspässe (z.B. technische Infrastruktur) kosten?
16. Bis zum heutigen Tage gibt es von Seiten des Innenministeriums auch keinerlei konkreten Aussagen hinsichtlich der Kosten von Pässen mit biometrischen Merkmalen: Mit welchen geschätzten Mehrkosten haben bei der Einführung dieser sog. Hochsicherheitspässe aus Sicht des BMI die einzelnen Passbehörden in den Bundesländern zu rechnen (ersuche am Darstellung der Kostenhöhe)?
17. Werden diese vom Bund übernommen? Wenn nein, warum nicht?
18. Welche zusätzliche technische Ausstattung (Infrastrukturgeräte) ist für die einzelnen Passbehörden notwendig, um Anträge auf Ausstellung von sog. Hochsicherheitspässen entgegennehmen und bearbeiten zu können?
19. Welche Software ist zur Ersterfassung und Verarbeitung biometrischer Daten in den zuständigen Passämtern notwendig? Wie hoch werden die Lizenzgebühren sein?
20. Wie hoch werden die dadurch entstehenden jährlichen (laufenden) Betriebskosten für die einzelnen Passbehörden durch das BMI geschätzt?

21. In welchen Ländern werden die in Österreich zur Verwendung gelangenden Passbücher, RFID-Chips, Betriebssysteme, Lesegeräte, Kontrollgeräte etc. sowie Software produziert (Aufschlüsselung auf EU-Mitgliedsländer)? Welche Unternehmen stellen diese Produkte her (ersuche um namentliche Bekanntgabe der Unternehmen)?

22. Erfolgt in Österreich bereits die notwendigen Ausschreibungen (für Infrastruktur, Geräte, Software sowie sonstige Leistungen) durch die Bundesbeschaffungsgesellschaft (BBG)? Wenn nein, wann soll diese erfolgen?

23. Schreibt die BBG aus? Wenn nein, wer schreibt dann diese Bestellungen bzw. Leistungen aus?

24. Wenn ja, wann erfolgte die Ausschreibung? Wie erfolgte diese Ausschreibung? Wie lautet die Ausschreibung im Wortlaut? Welche Geräte und Leistungen wurden konkret ausgeschrieben? Welche Vergabekriterien werden angewendet?

25. Wie ist der Stand des/der Vergabeverfahren(s)? Wann wird/werden diese abgeschlossen sein und die Vergabe durchgeführt?

26. Mit welchen zusätzlichen Kosten für den Bund ist mit der Einführung der sog. Hochsicherheitspässe aus Sicht des BMI zu rechnen (z.B. Technische Infrastruktur im BMI bzw. an den Grenzkontrollstellen sowie Software)?

27. Wo sind die Mehrkosten für diese sog. Hochsicherheitspässe im Budget 2006 ausgewiesen (Ersuche um Bekanntgabe der Budgetpositionen)?
28. Wie erfolgt zur Zeit die Aufteilung der Passgebühren zwischen Bund und den Bundesländern? Wie soll die Aufteilung der Passgebühren mit Einführung der sogenannten Hochsicherheitspässe geändert werden?
29. Was kostet derzeit ein Passbuch?
30. Was wird mit Einführung dieser so genannten Hochsicherheitspässe ein Passbuch kosten?
31. Was kostet ein dafür notwendige Chip (Einkaufskosten mit Mehrwertsteuer)?
32. Mit welchen Mehrkosten haben nach dem derzeitigen Informationsstand bei Einführung der so genannten Hochsicherheitspässe die PasswerberInnen zu rechnen? Was wird voraussichtlich ein sog. Hochsicherheitspass die einzelnen PasswerberInnen kosten?
33. Wird es für Familien mit Minderjährigen (d.h. Kindern) so wie in anderen EU-Mitgliedsstaaten reduzierte – familienfreundliche - Passgebühren geben? Wenn nein, warum nicht?
34. Welche Kosten erwarten Sie für die Bereitstellung der notwendigen technischen Infrastruktur für die Kontrolle von Pässen mit biometrischen Merkmalen an Grenzkontrollstellen oder Flughäfen?

35. Ist es richtig, dass die digitalen Passbilder für die sogenannten Hochsicherheitspässe vom Photographen über das Internet online an die befassete Passamtbehörde übermittelt werden sollen?
36. Wenn ja, wie wird bei dieser Übermittlung die Datensicherheit (Datenintegrität) gewährleistet?
37. Ist es richtig, dass die MitarbeiterInnen der einzelnen Passämter mit Einführung der sog. Hochsicherheitspässe (2. Phase) die Fingerabdrücke abnehmen werden?
Wenn nicht, wer dann?
38. Ist es richtig, dass die so genannten Hochsicherheitspässe zentral in der ÖSD produziert werden? Warum ist eine dezentrale Herstellung bei den einzelnen Passbehörden (z.B. Stadt Salzburg) nicht mehr möglich?
39. Ist es richtig, dass die so genannten Hochsicherheitspässe in Zukunft von der ÖSD mit der Post den PasswerberInnen zugestellt werden?
Wenn ja, wie wird damit – ohne Identitätskontrolle - die Zustellung an den tatsächlichen Antragsteller sichergestellt?
40. Wie lange wird die Ausstellung von den sogenannten Hochsicherheitspässen dauern? Ist es richtig, dass die Wartefrist für PasswerberInnen mindestens 5 Tage beträgt?
41. Wenn ja, wird es für Notfälle eine Express-Ausstellung und Express-Zustellung geben? Wenn nein, warum nicht?

42. Wie erklären Sie den österreichischen StaatsbürgerInnen die damit verbundenen Verzögerungen bei der Ausstellung bzw. Zustellung eines Passes?
43. Ist es richtig, dass in den sogenannten Hochsicherheitspässen ein kontaktloser RFID-Chip (Funk-Chip) eingesetzt wird?
44. Ist es richtig, dass ein digitales Gesichtsbild (und später auch Fingerabdrücke) als biometrische Kennzeichen auf einem RFID-Chip (Funkchip) gespeichert werden sollen? Wenn nicht, wo dann?
45. Ist es richtig, dass der Chip so gebaut sein muss, dass ein drittes biometrisches Merkmal (z.B. Iris) gespeichert werden kann?
46. Wie ist die langfristige Haltbarkeit (Lebensdauer) des Datenchips (bei einer Gültigkeitsdauer der Pässe von derzeit 10 Jahren) zu bewerten?
47. Wie begründen Sie die Ver- bzw. Anwendung von biometrischen Merkmalen (Daten) in den sog. Hochsicherheitspässen?
Worin besteht der zusätzliche Sicherheitsnutzen von biometrischen Merkmalen bei der Einreise bzw. Personenkontrolle?
48. Besteht durch die Möglichkeit des kontaktlosen Auslesens tatsächlich ein Sicherheitsgewinn oder sind hiermit nicht tatsächliche neue Risiken des unbefugten Aus- bzw. Mitlesens zu befürchten? Wie verhalten sich diese Risiken zum Grundrecht auf informationelle Selbstbestimmung?

49. Aus welchen Gründen wurde gerade diese Form der Datenübertragung gewählt?
50. Wie wird bei dem nun verwendeten biometrischen Erkennungsverfahren die Datensicherheit garantiert?
51. Wie soll sichergestellt werden, dass nur berechnigte Stellen und zwar mit Zustimmung des Inhabers des Passes auf die Daten zugreifen können, wenn es doch nur eine Frage der Zeit ist, wann der entsprechende Code „gehackt“ werden kann?
52. Welche Gutachten und Beweise liegen Ihnen vor, dass der „Chip“ tatsächlich erst mit dem Einlesen der maschinenlesbaren Teile aktiviert wird?
53. Sehen Sie den Chip als Sicherheitsmerkmal?
Wenn ja, ist dieser fälschungssicher?
54. Welche sonstigen Sicherheitsmerkmale sollen diese sogenannten Hochsicherheitspässe in Österreich enthalten?
55. Ist es richtig, dass die bisher im Pass aufgedruckten Informationen, wie beispielsweise Name, Geburtsdaten, Gültigkeitsdauer und Passnummer zusätzlich auch im Chip gespeichert sind?
56. Wenn ja, sind diese verschlüsselt gespeichert?

57. Die neuen sogenannten Hochsicherheitspässe sollen angeblich fälschungssicherer sein, was vor einigen Jahren auch von den Euroscheinen behauptet wurde. Nun wissen wir, dass dies nie stimmt:

Welche Garantie können Sie abgeben, dass diese sogenannten Hochsicherheitspässe mit Verwendung der beiden biometrischen Kennzeichen tatsächlich fälschungssicher sind und damit ihrem auch Namen gerecht werden?

58. Welche technische Sicherheitsinfrastruktur ist vorgesehen?

Wie bewertet das Innenministerium den hierzu notwendigen Forschungsbedarf, um etwa kryptographische Sicherheitsmethoden auf Basis kostengünstiger passiver RFID-Chips zu implementieren?

59. Wie groß ist die Speicherkapazität des vorgesehenen RFID-Chip? Was passiert bei einer fehlerhaften Datenübertragung oder Zurückweisung?

60. Wer haftet für den entstandenen Schaden (z.B. Urlaub) bei einer Zurückweisung an einer Grenzkontrollstelle, die auf einen technischen Mangel (z.B. Lesegerät) zurückgeführt ist? Sollen in derartigen Fällen Schadenersatzansprüche gestellt werden können? Wenn nein, warum nicht?

61. Wie und wodurch wird der in den sogenannten

Hochsicherheitspässen verwendete Chip vor unberechtigtem Auslesen ohne Zustimmung und Wissen geschützt (Skimming)?

62. Selbst wenn nach derzeitigem Stand der Technik ein unberechtigtes Mit- bzw. Auslesen nicht möglich sein sollte: Wie ist die langfristige informationstechnische Sicherheit der hierzu eingesetzten Verschlüsselungsverfahren zu bewerten?
63. Können Sie ausschließen, dass die Kommunikation zwischen dem RFID-Chip und dem Lesegerät (z.B. am Flughafen) durch Dritte abgehört werden kann?
64. Können Sie ausschließen, dass mit RFID-Chip´s in sogenannten Hochsicherheitspässen Bewegungsprofile von Passinhabern durch Dritte erstellt werden?
65. Wie sicher sind RFID-Chips gegenüber externer Störquellen? Wie wird technisch sichergestellt, dass Störsender (z.B. an Grenzkontrollstellen) das Auslesen der im Chip enthaltenen Daten verhindern?
66. Werden in Zukunft zur Passkontrolle (Personenkontrolle) für die Fremden und/oder ÖsterreicherInnen durch die Fremden- oder Sicherheitsbehörden auch mobile Lesegeräte eingesetzt?
67. Wie soll die Kontrolle am Flughafen oder sonstigen Grenzkontrollstellen bei der Einreise in ein EU-Land erfolgen? Kommt es zu einem 1:1 Abgleich (Vergleich der Eingangsdaten mit den für die Person gespeicherten Referenzdaten)?

68. Oder ist es richtig, dass bei der Einreise an den Grenzkontrollstellen (oder Flughafen) die im Pass (Chip) gespeicherten biometrischen Daten mit denen der einreisenden Person verglichen werden? Wird also nur die Übereinstimmung (Identität) von Pass und Inhaber elektronisch überprüft?
69. Wenn nein, wie erfolgt dann die Kontrolle?
70. Ist es dann richtig, dass für eine Person mit falschen Personendaten aber mit richtigen biometrischen Merkmalen, die im RFID-Chip gespeichert sind, die Passkontrolle ohne Beanstandung verläuft?
71. Wenn ja, bringt dann die Verwendung von biometrischen Daten und dieses Verfahren mehr an Sicherheit und Schutz vor Terrorismus?
72. Wie wird in Österreich bzw. in allen EU-Mitgliedsländern sichergestellt, dass die sogenannten Hochsicherheitspässe mit biometrischen Merkmalen (z.B. Gesichtsbild und/oder Fingerabdrücke) nicht mit falschen Personendaten versehen werden?
73. Wie wird in Österreich bzw. in allen EU-Mitgliedsländern sichergestellt, dass die sogenannten Hochsicherheitspässe mit richtigen Personendaten nicht mit falschen Personendaten versehen werden?
74. Wie können nach Einführung dieser sogenannten Hochsicherheitspässe (mit den beiden biometrischen Merkmalen) Verbrecher oder Terroristen an der Einreise nach Europa oder Österreich gehindert werden?

75. Erfolgt die Fingerabdruckidentifizierung bei diesen Kontrollen (Einreise) zentral beim Bundeskriminalamt (AFIS)? Wenn ja, aufgrund welcher Rechtsgrundlage?
76. Ist auf dem RFID-Chip eine Verschlüsselung der erfassten biometrischen Daten möglich?
77. Wann und unter welchen Voraussetzungen erfolgt eine Aktivierung des RFID-Chips?
Wie und unter welchen Voraussetzungen erfolgt die Deaktivierung?
78. Ist es richtig, dass der Chip nicht lesbar d.h. inaktiv ist, solange die maschinenlesbare Zeile (MRZ) nicht benutzt wird?
79. Ist es richtig, dass der Chip erst durch Auflegen auf ein Lesegerät (10 cm über das Lesegerät) durch das Einlesen der MRZ aktiviert und lesbar wird, da die MRZ einen Schlüssel enthält, der erst den Zugriff ermöglicht wird und erst dann Daten übermittelt werden?
80. Stellt die MRZ eine Erhöhung der Fälschungssicherheit dar, nachdem das Dokument 9303 (das die Gestaltung des Passes, den Aufbau der MRZ und deren Lesbarkeit regelt) allgemein zugänglich ist und sich die Inhalte der MRZ über das Internet abrufen lassen?
81. Ist es richtig, dass es bei der maschinenlesbaren Zeile (MRZ) um eine Beschleunigung der Grenzkontrolle bzw. der Personenabfertigung (Einreise) geht und nicht um mehr Fälschungssicherheit?

82. Können Sie ausschließen, dass durch diese sogenannten Hochsicherheitspässe sowie mit den damit verbundenen zentralen Speichermöglichkeiten und Verknüpfungsmöglichkeiten von biometrischen Daten „Gläserne Bürger“ geschaffen werden können?
83. Werden die an den österreichischen Grenzkontrollstellen und Flughäfen gelesenen Daten gespeichert? Wenn ja, aufgrund welcher Rechtsgrundlage?
84. Werden die an österreichischen Grenzkontrollstellen und Flughäfen gelesenen Daten (biometrische Merkmale) mit den in zentralen Datenbanken gespeicherten Daten des BMI u.a. (Erkennungsdienstliche Datenbank oder digitale Lichtdatenbank) dabei verglichen? Wenn ja, mit welchen zentralen Datenbanken oder Referenzdatenbanken?
85. Wenn nein, wird durch das BMI die Auffassung geteilt, dass aus verfassungsrechtlichen Gründen die biometrischen Daten in der Verfügungsgewalt der PassinhaberInnen verbleiben müssen und daher ausschließlich auf dem Reisepass, nicht aber in zentralen Datenbanken gespeichert werden oder mit Referenzdatenbanken abgeglichen werden dürfen?
86. Können Sie daher einen Abgleich dieser biometrischen Passdaten mit zentralen Dateien ausschließen? Wenn nein, warum nicht?
87. Welche staatlichen Stellen (Behörden) sollen Zugriff auf die für die Hochsicherheitspässe erfassten biometrischen Daten (Lichtbilddatei oder Fingerabdruckdatei) bekommen?

88. Soll es mit der Einführung des zweiten biometrischen Merkmales (Fingerabdrücke) eine eigene zentrale Fingerabdruckdatei geben oder werden diese Abdrücke auch im AFIS gespeichert?
89. Wenn ja, wer hat darauf eine Zugriffsmöglichkeit?
90. Ist es geplant, anderen Mitgliedsstaaten der EU oder überhaupt anderen Staaten einen Zugriff auf die für die Hochsicherheitspässe erfassten digitale Gesichtsbilddatei und Fingerabdruckdatei zu gewähren?
91. Wenn ja, aus welchen Gründen und aufgrund welcher Rechtsgrundlage?
92. Werden Sie weiterhin auf europäischer Ebene mit Nachdruck gegen die Einführung einer zentralen europäischen Passdatenbank – die nun auch biometrische Kennzeichen enthält - eintreten?
93. Welche EU-Mitgliedsländer treten zur Zeit für die Einführung einer zentralen europäischen Passdatenbank ein?
94. Welchen konkreten Beitrag können diese geplanten Hochsicherheitspässe mit diesen beiden biometrischen Merkmalen zur Bekämpfung der Kriminalität insbesondere des Terrorismus in Österreich, in der EU bzw. weltweit leisten?
95. Worin liegt der entscheidende – zusätzliche - Sicherheitsgewinn durch die Einführung biometrischer Merkmale durch die Verwendung sogenannter Hochsicherheitspässe?

96. Wie sieht die „Kosten – Nutzenrechnung“ für die Aufnahme und Verwendung dieser beiden biometrischer Daten in den sogenannten Hochsicherheitspässen in Österreich aus?
97. Wie wird das Sicherheitsniveau von Reisepässen, die zur Zeit in anderen Mitgliedsstaaten der EU gelten und ausgestellt werden, durch das BMI beurteilt? Mit welchen Ländern gab es in den letzten 5 Jahren die größten Probleme?
98. Wie wird das Sicherheitsniveau von Reisepässen, die zur Zeit in Drittstaaten gelten und ausgestellt werden, durch das BMI beurteilt? Mit welchen Ländern gab es in den letzten 5 Jahren die größten Probleme?
99. Welche Pässe aus anderen EU-Mitgliedsstaaten und Drittstaaten lassen sich besonders leicht fälschen?
100. Wie viele konkrete ernstzunehmende Fälle von (Ver-)Fälschungen österreichischer Pässe (inkl. der gefälschten Pässe) sind der Bundesregierung seit 2000 im In- oder Ausland bekannt geworden (Aufschlüsselung auf die einzelnen Jahre)?
101. Wie oft wurden in den Jahren 2000, 2001, 2002, 2003 und 2004 in Österreich bei fremdenbehördlichen oder sicherheitsbehördlichen Kontrollen Menschen mit einem gefälschten oder verfälschten nichtösterreichischen Pass(z.B. Griechischer Pass) aufgegriffen (Aufschlüsselung auf Jahre und Passherkunft)?

102. Wie viele Verbrechen nach dem StGB wurden unter Verwendung eines verfälschten oder gefälschten Passes 2000, 2001, 2002, 2003 und 2004 begangen? Welche Delikte betraf dies (Aufschlüsselung der Anzahl auf Delikte und Jahre)?
103. Wie viele Verstöße nach dem Passgesetz gab es 2000, 2001, 2002, 2003 und 2004 in Österreich (Aufschlüsselung auf Jahre)? Um welche Verstöße handelte es sich dabei (Aufschlüsselung der Verstöße auf Jahre)?
104. In wie weit hat die Arbeit der österreichischen Dokumentberater zu deutlichen Erfolgen im Kampf (insb. gegen illegale Migration) auf dem Luftweg geführt?
105. Wann werden Sie dem Parlament eine Novelle des Passgesetzes vorlegen?
Was soll konkret Inhalt dieser Novelle sein?

Ulrich
Krisz
Krisz
Krisz
Krisz