

Landeshauptstadt Magdeburg

Stellungnahme der Verwaltung

öffentlich

zum/zur	Stadtamt	Stellungnahme-Nr.	Datum
F0216/07 Fraktion DIE LINKE	FB 32	S0265/07	04.12.2007
Bezeichnung			
Sicherheit für den E-Pass			
Verteiler	Tag		
Der Oberbürgermeister	08.01.2008		

Seit Einführung des ersten biometrischen Merkmals in den Reisepässen der Bundesrepublik Deutschland zum 1.11.2005 wurden durch die Bundesdruckerei bereits mehr als 2 Millionen EU-Reisepässe mit einem RFID-Chip (**R**adio **F**requency **I**dentification, sinngemäß: automatisches Datenerfassungs- und Identifikationssystem mit kontaktloser Datenübermittlung auf der Basis von Hochfrequenztechnologie) gefertigt. Der Einführung des ePasses gingen umfangreiche Untersuchungen u.a. des BSI (Bundesamt für die Sicherheit in der Informationstechnik) voraus. Entsprechende Ausführungen hierzu, sowie weiterführende Studien finden sich auf den Internetseiten des BSI (www.bsi.de). Allgemeine Hinweise zum ePass, u.a. auch zu den zum Einsatz kommenden Sicherheitsstandards finden sich auf der Homepage des Bundesinnenministeriums (BMI) unter www.epass.de.

Veranlasst durch das Vorgehen der Hansestadt Lübeck wandte sich das BMI mit Schreiben vom 23.11.2007 an die Innenministerien der Länder, dessen Inhalt hier auszugsweise nachstehend zitiert wird:

Nach vorliegenden Informationen werden in einer einzelnen Passbehörde Aluminium-Schutzhüllen für den elektronischen Pass zur ergänzenden Sicherung der im Chip gespeicherten biometrischen Merkmale angeboten. Hierzu wird Folgendes angemerkt:

Die im Chip der elektronischen Reisepässe gespeicherten Daten sind durch Sicherheitsmechanismen vor unberechtigtem Zugriff geschützt.

Diese Sicherheitsmechanismen sehen vor, dass ein Lesegerät nur dann die im Chip gespeicherten Informationen lesen kann, wenn es die Daten der auf der Passkarte abgedruckten maschinenlesbaren Zone kennt. Daher setzt jedes Auslesen zunächst generell voraus, dass das Passbuch aufgeschlagen und die auf der Passkarte abgedruckte maschinenlesbare Zone optisch ausgelesen wird. Aus den Daten der maschinenlesbaren Zone berechnet das Lesegerät dann einen Schlüssel, den es an den Chip übermittelt. Nur wenn dem Chip der richtige Schlüssel übermittelt wird, gibt es die in ihm gespeicherten Daten gegenüber dem Lesegerät frei (sog. Basic Access Control).

Für die Fingerabdrücke gibt es darüber hinaus einen zusätzlichen Sicherheitsmechanismus. Nur Lesegeräte, die über Berechtigungszertifikate des den Pass ausstellenden Staates verfügen, können die Fingerabdrücke auslesen (sog. Extended Access Control). ...

Die dargestellten Sicherheitsmechanismen gewährleisten, dass die in den Chips der deutschen Reisepässe gespeicherten Daten hinreichend vor unberechtigtem Zugriff geschützt sind. Es besteht kein Grund, die im Chip gespeicherten Daten durch Alufolie zusätzlich zu schützen. Die in der Öffentlichkeit bekannt gewordene Vorgehensweise einer einzelnen Passbehörde, Alufolien anzubieten, ist ein Alleingang und wird vom Bundesministerium des Innern abgelehnt.

Ich bitte daher, alle Passbehörden auf diese Sachlage hinzuweisen und sie aufzufordern, von einer Verteilung von Alufolien abzusehen, da sie nicht erforderlich sind und zu einer unnötigen Beunruhigung von Passinhabern führen.

Darüber hinaus ist zu beachten, dass die Pässe mit den gespeicherten biometrischen Merkmalen ausschließlich im behördlichen Rechtsverkehr Anwendung finden. Die zum Auslesen Berechtigten (Polizei, Zoll, Pass- und Meldebehörden) benötigen die Daten im Rahmen ihrer hoheitlichen Tätigkeit. In anderen Bereichen, insbesondere im privaten Geschäfts- und Rechtsverkehr finden die elektronisch gespeicherten Daten keine Anwendung. Es ist daher sehr fraglich, welchen „Vorteil“ ein Angreifer sich bei der unrechtmäßigen Datenbeschaffung verschaffen will.

Das Szenario beschreibt der Absatz „Funktionsweise des Zugriffsschutzes“ auf www.epass.de sehr plastisch:

...

Für ein unerlaubtes, heimliches Auslesen der Daten (z.B. aus dem geschlossenen Pass in der Jackentasche) müssen dem „Angreifer“ ebenfalls diese drei Angaben vorab bekannt sein. Nur dann kann er den notwendigen Schlüssel generieren und so den Chip dazu bewegen, die Daten frei zu geben. Für die Praxis bedeutet das: Wenn man das Geburtsdatum einer Person, ihre Passnummer und das Ablaufdatum des Passes kennt, nahe genug (d.h. auf 20 cm) an die Person herankommt (dann kennt man in der Regel auch das Gesicht) und zudem weiß, wo sich der ePass befindet (z.B. in der Reisetasche oder im Sakko), kann man mit einem Lesegerät den Chip auslesen. Vorausgesetzt, die Person bewegt sich mehrere Sekunden nicht von der Stelle. Dieses Szenario ist offensichtlich sehr unwahrscheinlich.

Und selbst wenn ein solcher Spionage-Versuch gelänge: Welchen Informationsgewinn hätte der „Angreifer“? Bekannt waren ihm vorab bereits Passnummer, Geburtsdatum und Ablaufdatum. Neu ermittelt wurden nur Name und Vorname, Geschlecht, Staatsangehörigkeit sowie das Passfoto. Vor- und Nachname, Geschlecht und Staatsangehörigkeit wird der „Angreifer“ aber vorher gewusst haben. Schließlich hatte er bereits Passnummer, Geburtsdatum und Ablaufdatum des Passes herausgefunden. Bleibt als „Gewinn“ nur das digitale Passfoto aus dem Chip. Dieses wäre aber bei Vorliegen krimineller Energie weitaus einfacher und unauffälliger zu bekommen: Mit einer leistungsfähigen Digitalkamera müsste sich ein Datenspion nicht auf 20 cm der Zielperson nähern.

Unabhängig von der Frage des eigentlichen Informationsgewinns sind dem „Angreifer“ auch technische Grenzen für die Weiterverwendung der ausspionierten Daten gesetzt:

Erstens sind die ausgelesenen Daten durch eine elektronische Signatur geschützt und können daher nicht geändert und in geänderter Form in neue Chips/Pässe gebracht werden. Die Signatur schützt die Daten gegen nachträgliches Ändern.

Zweitens wird es nicht gelingen, einen Klon-Chip in ein anderes Passdokument einzubringen und auf diese Weise einen Klon-Pass herzustellen. Denn dann müssten auch sämtliche weitere

Sicherheitsmerkmale der Pässe (Hologramme, Sicherheitsschriften etc.) gefälscht werden, was eine praktisch unüberwindbare Hürde für Fälscher darstellt. Deutsche Pässe gehören anerkanntermaßen zu den sichersten weltweit. ...

Beim ePass der zweiten Generation kommt dieser zusätzliche Zugriffsschutz zum Tragen: Nur Staaten, die von Deutschland spezielle Zugriffsberechtigungen erhalten, können auf die Fingerabdrücke im Chip zugreifen.

Zu den Alu-Hüllen sei angemerkt, dass sich hierzu bereits Hinweise aus dem Jahr 2006, evtl. auch früher, finden (bspw. www.heise.de/newsticker/meldung/print/69366 und www.golem.de/0602/43215.html). Hier sollten allerdings nicht nur Personaldokumente sondern auch gleich noch die RFID-Chips der Fußball-WM-Tickets mit geschützt werden. Der Preis beträgt seit dieser Zeit 6 EUR. Gerechnet auf die Ausstellungszahlen der Vorjahre, ergäbe sich hier ein ansehnlicher Markt, von ca. 6 Mio EUR jährlich.

Für Magdeburg würde dies bedeuten, dass im Jahr 2008 auf der Basis der geplanten 6.800 Reisepässe ein finanzieller Mehrbedarf in Höhe von 40.800 EUR entstehen würde. Diese Mittel sind nicht im Haushalt vorgesehen.

Nach Überzeugung der Magdeburger Passbehörde sind die umfangreichen Sicherheitsvorkehrungen zum Schutz der elektronisch gespeicherten, personenbezogenen Daten als absolut ausreichend anzusehen. Die Ausreichung zusätzlicher Schutzhüllen wird als nicht notwendig und vor dem Hintergrund der Haushaltskonsolidierung auch nicht für vertretbar angesehen. Aus den selben Gründen ist auch nicht beabsichtigt, durch ein Merkblatt auf einen zusätzlichen Schutzbedarf durch Hüllen o.ä. hinzuweisen.

In diesem Zusammenhang sei darauf hingewiesen, dass allein in Magdeburg jährlich ca. 3.500 Dokumente als verloren/gestohlen gemeldet werden. Das sich ergebende Missbrauchspotenzial dürfte um ein Vielfaches höher liegen, als die sehr abstrakte Gefährdung durch die Manipulation einer „elektronischen Identität“.

Holger Platz

