Deutscher Bundestag **Drucksache 16/12582**

16. Wahlperiode 08. 04. 2009

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Dr. Max Stadler, Christian Ahrendt, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 16/12493 –

Technische Schwierigkeiten mit dem elektronischen Pass und dem elektronischen Personalausweis

Vorbemerkung der Fragesteller

In neuen Reisepässen und demnächst auch Personalausweisen werden RFID-Chips (RFID – Radio Frequency Identification) verwendet, auf denen biometrische Daten gespeichert und mittels derer personenbezogene Daten elektronisch ausgelesen werden können.

Problematisch ist hierbei jedoch, dass die Datenerhebung und Datenübertragung von biometrischen Informationen mit der vorhandenen Infrastruktur nicht ausreichend entwickelt ist, um vor unautorisierter Entschlüsselung zu schützen. Die Entschlüsselung der Daten auf Reisepässen, bei denen der Chip mit demselben Sicherheitssystem „Basic Access Control“ geschützt wird, wie das bei den elektronischen Personalausweisen der Fall ist, ist bereits mehrfach verschiedenen Experten gelungen. So haben Spezialisten der Sicherheitsfirma Riscure aus Delft, Niederlande, bereits im Frühjahr 2006 in einer Demonstration die Verschlüsselung dieser Ausweispapiere innerhalb von zwei Stunden nach Aufzeichnung des Codes entschlüsselt. Danach lagen Geburtsdatum, Foto und Fingerabdruck des Passbesitzers im Klartext vor. Der Computerexperte Jeroen van Beek von der Universität Amsterdam entschlüsselte im August 2008 den Chip. Innerhalb einer Stunde wurde auf dem Pass eines Jungen der manipulierte RFID-Chip mit dem Foto eines palästinensischen Selbstmordattentäters aufgebracht. Der Pass wurde von einem Lesegerät akzeptiert, das mit der Software arbeitet, die von der Zivilluftfahrt-Organisation als Standard empfohlen wird. Für die Fälschung wurden lediglich ein öffentlich verfügbares Programm, ein Card-Reader und günstige RFID-Chips benötigt. Es ist deshalb davon auszugehen, dass elektronische Schutzvorrichtungen immer nur einen begrenzten, deutlich unter der vorgesehenen Nutzungszeit des Personalausweises von zehn Jahren liegenden Zeitraum zuverlässigen Schutz vor Datendiebstahl gewährleisten. Mangels Möglichkeiten zu Sicherheits-Updates ist zu befürchten, dass die Ausweise hinsichtlich Angriffen auf ihren Datenbestand sehr bald auch gegenüber Laien nicht mehr ausreichend geschützt sein werden.

Sowohl der Personalausweis als auch der im November 2005 eingeführte elektronische Reisepass haben in der Regel eine Gültigkeit von zehn Jahren. Es ist

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 7. April 2009 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

damit zu rechnen, dass mit der Zunahme der Rechenleistung von Computerchips und der weiteren Softwareentwicklung die Entschlüsselung eines veralteten Sicherheitssystems mit fortschreitender Zeit immer einfacher wird.

Der elektronische Personalausweis soll unter anderem auch zur Nutzung von elektronischer Kommunikation mit Behörden zum Einsatz kommen und wird mithin künftig Voraussetzung zur Teilnahme an E-Government-Anwendungen. Auch im elektronischen Geschäftsverkehr soll der elektronische Personalausweis zur Identifikation und sicheren Kommunikation genutzt werden können. Gerade im Hinblick auf diese Anwendungen ist die Möglichkeit eines Identitätsdiebstahls durch unberechtigtes Auslesen oder Manipulation des Chips mit gravierenden Gefahren nicht nur für das Persönlichkeitsrecht, sondern auch im Hinblick auf wirtschaftliche Schädigungen der Betroffenen verbunden.

Vorbemerkung der Bundesregierung

Es wird dargestellt, dass das Verfahren „Basic Access Control“, das derzeit für den elektronischen Reisepass verwendet wird, bereits mehrfach gebrochen worden sei und ebenfalls für den elektronischen Personalausweis zum Einsatz kommen soll. Es soll z. B. möglich sein, „Geburtsdatum, Foto und Fingerabdruck des Passbesitzers“ innerhalb von zwei Stunden zu entschlüsseln.

Diese Aussagen sind falsch.

Zum einen sind beim elektronischen Personalausweis alle Daten durch das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte und international als hochsicher geltende Verfahren „Extended Access Control“ geschützt. Das heißt: sämtliche auf dem Ausweis gespeicherten Daten sind auf hohem Niveau gegen unberechtigten Zugriff geschützt. Zum anderen sind die Aussagen selbst in Bezug auf den elektronischen Reisepass nicht richtig, da auch dort dieses Verfahren zum Schutz der Fingerabdrücke bereits zum Einsatz kommt.

Weiterhin wird behauptet, dass der elektronische Reisepass leicht gefälscht werden kann und auf einen Pass-Chip das Foto eines palästinensischen Selbstmordattentäters aufgebracht worden sei. Dieser sei anschließend von einem von der Internationalen Zivilluftfahrtorganisation (ICAO) als Standard empfohlenen Lesegerät akzeptiert worden.

Diese Darstellung ist ebenfalls falsch.

Die auf dem Chip gespeicherten Daten sind durch eine elektronische Signatur gegen Veränderungen geschützt. Diese Signatur wurde in dem beschriebenen Fall nicht überprüft. Bei den in Deutschland für die Identitätskontrolle vorgesehen Geräte ist eine Sicherheitszertifizierung des BSI vorgesehen, die das Vorhandensein der Signaturprüfung im Gerät feststellt.

Wie bei konventionellen Sicherheitsmerkmalen (z. B. Hologrammen) sind daher grundsätzlich auch die neuen elektronischen Sicherheitsmerkmale (z. B. die Signatur) gleichfalls zu überprüfen. Ein Unterlassen der Prüfungen führt – nahe liegend – zum eventuellen „Nicht-Erkennen“ von Fälschungen oder Manipulationen.

1. Aus welchen Gründen geht die Bundesregierung davon aus, dass entgegen der sonst üblichen rasanten technischen Entwicklung bei elektronischen Personalausweisen und Pässen eine Technikfestigkeit für die Gültigkeitsdauer von zehn Jahren gegeben ist?

Elektronische Pässe und Personalausweise sind keine „Consumer-Produkte“ und unterliegen daher nicht der rasanten technischen Entwicklung von Elektronikprodukten. Beide Dokumente sind mit physikalischen und elektronischen

Sicherheitsmerkmalen auf höchstem technologischem Niveau zur Maximierung der technischen Aufwandsschwelle für Fälschungs- und Verfälschungsversuche ausgestattet und sind für eine für ein Reisedokument typische Handhabung und Belastung während der gesamten Gültigkeitsdauer von zehn Jahren ausgelegt. Auf Grundlage internationaler Normen wurde für den elektronischen Reisepass zwischen dem Bundesministerium des Innern (BMI), dem Bundeskriminalamt (BKA), dem BSI und der Bundesdruckerei ein Lastenheft zu systematischen Untersuchungen abgestimmt. Dieses Lastenheft enthält die für die Qualifikation eines geeigneten Inlays und des Dokuments notwendigen Prüfungen, wie zum Beispiel Stempeltests, dynamisches Biegen unter Last, Torsionsprüfungen, Röntgenbelastungen, Klimaprüfungen, chemische Beanspruchungen usw. Qualifizierende Tests finden sowohl bei der Bundesdruckerei als auch bei den Chipzulieferern NXP und Infineon statt. Die vorliegenden Erkenntnisse aus der seit dem 1. November 2005 laufenden Produktion von bisher etwa acht Mio. ePässen lassen keinen Zweifel an der dauerhaften Funktionstüchtigkeit erkennen; der Prozess der Qualitätssicherung wird kontinuierlich sichergestellt. Die diesbezüglichen positiven Erfahrungen werden auf die Produktion des elektronischen Personalausweises übertragen und durch langfristige Lieferverträge sichergestellt.

2. Welche Erkenntnisse liegen der Bundesregierung zur durchschnittlichen Lebensdauer von RFID-Chips vor?

Die Haltbarkeit von RF-Chips ist im Wesentlichen von dem Einsatzgebiet und der Konstruktion des Kartenkörpers/Inlays abhängig. Entsprechend den spezifischen Anforderungen für den elektronischen Reisepass und den elektronischen Personalausweis werden entsprechende Prüfvorschriften zur Qualifikation des Inlays bzw. Kartenkörpers erstellt, um eine Funktion des RF-Chips über eine Nutzungszeit von zehn Jahren zu gewährleisten (siehe auch Antwort zu Frage 1 zu den etablierten Prüfungen für den elektronischen Reisepass). In keinem Fall können Aussagen über Lebensdauer von RFID-Chips wie sie z. B. im Einzelhandel, im öffentlichen Personennahverkehr (ÖPNV) oder in Zutrittskontrollsystemen Verwendung finden auf die Nutzung im elektronischen Reisepass und elektronischen Personalausweis übertragen werden, da diese konstruktionsbedingt für eine wesentlich kürzere Lebensdauer ausgelegt sind.

3. Welche Erkenntnisse zur Langzeitnutzung von RFID-Chips über zehn Jahre liegen der Bundesregierung vor?

4. Wie hoch schätzt die Bundesregierung die Wahrscheinlichkeit ein, dass ein RFID-Chip in einem elektronischen Pass oder elektronischen Personalausweis vor Ablauf der Gültigkeitsdauer von zehn Jahren nicht mehr funktionsfähig ist?

Siehe Antwort zu Frage 2.

5. Wie hoch schätzt die Bundesregierung die Wahrscheinlichkeit ein, dass die Algorithmen der elektronischen Pässe oder elektronischen Personalausweise vor Ablauf der Gültigkeitsdauer von zehn Jahren nicht mehr sicher sind, weil diese nicht mehr dem Stand von Wissenschaft und Technik entsprechen?

Die Wahrscheinlichkeit, dass die Algorithmen der elektronischen Pässe oder elektronischen Personalausweise vor Ablauf der Gültigkeitsdauer von zehn Jahren nicht mehr sicher sind, ist vernachlässigbar gering. Die eingesetzten Algorithmen und Schlüssellängen für hohen Schutzbedarf (Absicherung gegen

Fälschung und Verfälschung, Schutz von sensitiven Daten gegen unberechtigten Zugriff) sind nach international anerkannten Empfehlungen so gewählt, dass deren Sicherheit aller Voraussicht nach bis mindestens 2030 gegeben ist.

Das BSI führt eine regelmäßige Überprüfung der Sicherheit der eingesetzten Algorithmen und Schlüssellängen durch und gibt die im elektronischen Reisepass und im elektronischen Personalausweis einzusetzenden Algorithmen und Schlüssellängen verbindlich vor.

6. Wie hoch schätzt die Bundesregierung die Wahrscheinlichkeit ein, dass die Algorithmen der elektronischen Pässe oder elektronischen Personalausweise vor Ablauf der Gültigkeitsdauer von zehn Jahren nicht mehr sicher sind, weil diese entschlüsselt bzw. gehackt wurden?

Siehe Antwort zu Frage 5.

7. Welche Möglichkeiten, sich hinsichtlich der Funktionsfähigkeit ihres elektronischen Reisepasses bzw. Personalausweises zu vergewissern, steht den Bürgerinnen und Bürgern zur Verfügung bzw. auf welchem Wege sollen sie über Funktionsmängel oder Sicherheitslücken informiert werden?

Um die Funktionsfähigkeit des in heute ausgegebenen Reisepässen integrierten Chips zu überprüfen und insbesondere die dort gespeicherten Daten anzuzeigen, wurden allen Passbehörden von der Bundesregierung Lesegeräte zur Verfügung gestellt. Auch für den elektronischen Personalausweis werden Lesegeräte bereitgestellt werden.

Grundsätzlich finden sich Informationen zu Sicherheitslücken, wie zum Beispiel in Softwareprogrammen, aber auch Informationen zu Viren, Würmern, Trojanern, auf den Internetseiten des BSI. Die Bundesregierung geht nicht davon aus, dass es bei elektronischen Ausweisen zu Funktionsmängeln und Sicherheitslücken kommt, siehe dazu auch Antwort zu Frage 5.

8. Welche Möglichkeiten sollen Bürgerinnen und Bürger haben, wenn der RFID-Chip in ihrem elektronischen Reisepass oder elektronischen Personalausweis aufgrund technischer Funktionsverluste oder -ausfälle, aufgrund technischer Weiterentwicklung und Veraltung der Technik oder aufgrund von Sicherheitslücken wegen des unerlaubten Entschlüsselns bzw. Hackens der Algorithmen nicht mehr nutzbar ist?

Zu den Themen Funktionsverlust, Weiterentwicklung und Veralten der Technik und Sicherheitslücken siehe Antworten zu den Fragen 2 und 5.

Sollte es in Einzelfällen zu einem technischem Funktionsverlust bzw. -ausfällen des Chips kommen, können Bürgerinnen und Bürger ihren elektronischen Reisepass bzw. Personalausweis reklamieren. Eine erneute Gebühr fällt, außer wenn der Funktionsverlust durch unsachgemäße Nutzung verursacht wurde, nicht an.

9. Fallen erneut Gebühren an, wenn aus den vorgenannten Gründen ein Pass oder Personalausweis beantragt werden muss?

Siehe Antwort zu Frage 8.

10. Ist es bereits zu Neuausstellungen von Ausweispapieren aus den vorgenannten Gründen gekommen, und falls ja, in wie vielen Fällen, und aus jeweils welchen Gründen?

Von den seit 1. November 2005 ausgegebenen etwa 8,2 Millionen elektronischen Reisepässen kam es bis Februar 2009 zu 68 berechtigten Reklamationen, die auf nicht funktionsfähige Chips zurückgingen. Das ist eine Ausfallquote von lediglich 0,0008 Prozent.

11. Welche Vereinbarungen mit den Herstellern der in den elektronischen Reisepässen bzw. elektronischen Personalausweisen verwendeten RFID-Chips hat die Bundesregierung hinsichtlich von Gewährleistungsrechten und Garantien getroffen?

12. Weichen die Gewährleistungs- oder Garantiefristen von der Gültigkeitsdauer der elektronischen Reisepässe oder elektronischen Personalausweise ab, und welche Unterschiede gibt es?

13. Welche Vereinbarungen mit den Herstellern der in den elektronischen Reisepässen bzw. elektronischen Personalausweisen verwendeten RFID-Chips hat die Bundesregierung hinsichtlich etwaiger Schadensersatzansprüche wegen technischer oder informationstechnischer Mängel getroffen?

Die Bundesregierung hat keine Vereinbarungen mit den Chipherstellern getroffen. Vereinbarungen bestehen mit der Bundesdruckerei GmbH. Diese wie auch die Vereinbarungen der Bundesdruckerei mit den Herstellern der Chips sind Geschäftsgeheimnisse der betroffenen Unternehmen und können nicht offen gelegt werden.

Bürgerinnen und Bürger haben aber die Möglichkeit elektronische Reisepässe (und zukünftig auch Ausweise) zu reklamieren, siehe dazu auch Antwort zu Frage 8.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333