Deutscher Bundestag **Drucksache 16/12493**

16. Wahlperiode 25. 03. 2009

Kleine Anfrage

der Abgeordneten Gisela Piltz, Dr. Max Stadler, Christian Ahrendt, Hartfrid Wolff (Rems-Murr), Jens Ackermann, Dr. Karl Addicks, Rainer Brüderle, Ernst Burgbacher, Patrick Döring, Mechthild Dyckmans, Jörg van Essen, Otto Fricke, Horst Friedrich (Bayreuth), Dr. Edmund Peter Geisen, Hans-Michael Goldmann, Miriam Gruß, Joachim Günther (Plauen), Dr. Christel Happach-Kasan, Heinz-Peter Haustein, Elke Hoff, Birgit Homburger, Dr. Werner Hoyer, Michael Kauch, Hellmut Königshaus, Dr. Heinrich L. Kolb, Gudrun Kopp, Dr. h. c. Jürgen Koppelin, Heinz Lanfermann, Sibylle Laurischk, Harald Leibrecht, Ina Lenke, Sabine Leutheusser-Schnarrenberger, Michael Link (Heilbronn), Markus Löning, Dr. Erwin Lotter, Horst Meierhofer, Patrick Meinhardt, Jan Mücke, Burkhardt Müller-Sönksen, Dirk Niebel, Detlef Parr, Cornelia Pieper, Frank Schäffler, Marina Schuster, Dr. Hermann Otto Solms, Carl-Ludwig Thiele, Florian Toncar, Dr. Daniel Volk, Christoph Waitz, Dr. Claudia Winterstein, Dr. Volker Wissing, Dr. Guido Westerwelle und der Fraktion der FDP

Technische Schwierigkeiten mit dem elektronischen Pass und dem elektronischen Personalausweis

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 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.

Wir fragen die Bundesregierung:

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

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

Berlin, den 25. März 2009

Dr. Guido Westerwelle und Fraktion

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