Aktueller Begriff

Deutscher Bundestag ■ Wissenschaftliche Dienste

Elektronischer Reisepass (E-Pass)

Der elektronische Reisepass (E-Pass, mitunter auch als ePass bezeichnet) ist ein mit einem Speicherchip ausgestatteter Reisepass, der seit dem 01.11.2005 ausgegeben wird. Der Chip enthält neben den üblichen persönlichen Angaben zum Inhaber auch biometrische – also zur Personenerkennung anhand biologischer Merkmale – verwertbare Daten. Gegenwärtig ist darauf ein digitales Passfoto hinterlegt, ab November 2007 sollen zusätzlich zwei Fingerabdrücke gespeichert werden. Vom 01.03 bis zum 30.06.2007 werden über zwanzig Passbehörden in Deutschland das neue Antragsverfahren für den elektronischen Reisepass der zweiten Generation im Echtbetrieb testen. Für das Jahr 2008 ist zudem ein elektronischer Personalausweis vorgesehen, auf dem ebenfalls biometrische Merkmale gespeichert werden. Auf europäischer Ebene ist die Einführung biometrischer Reisepässe in der EG-Verordnung 2252/2004 vom 13.12.2004 geregelt. Sie greift weitgehend auf technische Vorgaben der International Civil Aviation Organization (ICAO) zurück, einer Unterorganisation der Vereinten Nationen. Bisher wurden insgesamt 2,6 Millionen E-Pässe ausgegeben.

Funktionsweise des E-Passes

Der im E-Pass verwendete „Radio Frequency Identification"-Funkchip (RFID) ist in den Passdeckel integriert. Er kann kontaktlos ausgelesen und batterielos über das Lesegerät mit Strom versorgt werden. Über einen eingebauten Mikroprozessor überwacht er den Zugriff auf die gespeicherten Daten und steuert deren Verschlüsselung. Organisiert sind diese nach einem als „Logical Data Structure" (LDS) bezeichneten Muster, das von der ICAO normiert ist. Neben den bereits gespeicherten Angaben und den Fingerabdruckbildern ist in diesem Schema auch Raum für ein – in Deutschland nicht erfasstes – Irismuster vorgesehen. Ebenfalls angelegt sind optionale Speicherbereiche, unter anderem für Adresse, Telefonnummer und Beruf des Inhabers sowie für zusätzliche Fotos oder einen Nachweis der Staatsbürgerschaft.

Beim Grenzübertritt mit dem E-Pass wird neben der üblichen Sicherheitsprüfung auch der Inhalt des Chips ausgelesen und mit den gedruckten Passdaten abgeglichen. Die biometrischen Merkmale werden nur zur Unterstützung herangezogen. E-Pässe, deren Chip nicht funktioniert, bleiben daher weiter gültig, was allerdings die Funktion des RFIDs als Sicherheitsmerkmal aufhebt. Bei der Überprüfung erfolgt eine Zugangs- und Zugriffskontrolle durch den Chip, außerdem prüft das Lesegerät die Daten auf Manipulationsversuche. Je nach Empfindlichkeit der Daten werden diese durch aufeinander aufbauende Sicherungsmechanismen gesichert: (1) Als weniger empfindlich gelten die personenbezogenen Angaben und das Passfoto. Sie sollen über den grundlegenden Zugriffsmechanismus „Basic Access Control" (BAC) vor unerlaubtem Auslesen geschützt werden. Um Zugriff zu erhalten, errechnet dabei das Lesegerät aus den Angaben auf der Passkarte einen Zugangsschlüssel, mit dem es sich beim Chip ausweist. Damit soll sichergestellt werden, dass nur ein zur Inspektion übergebener, geöffneter E-Pass ausgelesen werden kann. (2) Will ein Inspektionssystem ab November 2007 auf die Fingerabdrücke zugreifen, muss es neben der BAC auch eine erweiterte Zugangskontrolle „Extended Access Control" (EAC) absolvieren. Hierbei weist zuerst der Chip nach, dass er seit Ausgabe des E-Passes nicht ausgetauscht wurde. Danach legt das Lesegerät ein digital signiertes Zertifikat des Landes vor, das den E-Pass ausgestellt hat. An diesem erkennt der E-Pass, auf welche Daten das Lesegerät zugreifen darf. Bei jedem Zugriff (BAC und EAC) überprüft das Lesegerät zudem eine auf dem E-Pass gespeicherte digitale Signatur sowie einen „Fingerabdruck" der hinterlegten Daten. Damit soll sichergestellt werden, dass

diese nicht manipuliert wurden. Die ICAO schreibt lediglich letztere Echtheitsprüfung vor, die EG verlangt zusätzlich BAC und (wenn Fingerabdrücke gespeichert werden) EAC. Je nachdem, ob BAC oder EAC genutzt wird, erfolgt eine unterschiedlich starke Verschlüsselung der Übertragung.
Zur Überprüfung des E-Passes müssen mehrfach digitale Signaturen geprüft werden. Die dafür nötigen Schlüssel sollen zwischen den Staaten in einem als „Public Key Infrastructure“ (PKI) bezeichneten Netzwerk produziert und ausgetauscht werden. Je nach Art des benötigten Schlüssels erfolgt die Verteilung zwischen den Staaten zentral über die ICAO oder dezentral durch die Staaten selbst. Da innerhalb der PKI auch vor kompromittierten Schlüsseln gewarnt wird, kommt ihr große Bedeutung für das Funktionieren und die Sicherheit des E-Passes zu. Oberste PKI-Institution in Deutschland wird das Bundesamt für Sicherheit in der Informationstechnik (BSI). Es beglaubigt mittelbar die in den Pässen enthaltenen Daten und vergibt die Zugriffszertifikate für ausländische Kontrolleure. Um das Risiko kompromittierter Schlüssel zu senken, wird die Gültigkeitsdauer der verwendeten Zertifikate auf möglichst kurze Zeiträume verringert.

Erwartungen und Einwände

Befürworter des E-Passes verweisen darauf, dass die Bedrohung durch den internationalen Terrorismus eine Aufnahme biometrischer Daten in Ausweisdokumente nötig mache. Der E-Pass ermögliche die eindeutige Identifizierung des Passinhabers anhand biometrischer Kennzeichen. Terroristen fiele es damit schwerer, unerkannt in die Bundesrepublik einzureisen. Mit der neuen Generation deutscher Pässe würde die Sicherheit der Dokumente auf ein neues Niveau gehoben. Aus diesem Grund wird die Nutzung von Biometrie auch als geeignetes Mittel zur Vorbeugung gegen Identitätsdiebstahl bezeichnet. Zusammen mit dem geplanten europäischen Visuminformationssystem und einer biometriegestützten Aufenthaltskarte stellt der E-Pass Teil eines integrierten Konzeptes dar. Auch sei der E-Pass nötig, um einen einheitlichen europäischen Standard für Reisepässe zu schaffen, da die Dokumente anderer Mitgliedsstaaten leicht zu fälschen seien. Vom E-Pass wird zudem erwartet, dass er eine Verwendung gestohlener Papiere erschwert und dass Sicherheitskontrollen (z.B. an Flughäfen) beschleunigt werden können.
Kritiker wenden ein, dass Sicherheitslücken das Risiko eines Identitätsdiebstahls erhöhen. So seien wiederholt Sicherheitsmechanismen des E-Passes umgangen worden; darunter auch Verfahren, die in der EAC verwendet werden. Obwohl die EAC weiter als im Grunde sicher angesehen wird, könne – da die Daten zur Kontrolle zwangsläufig entschlüsselt werden müssen – eine missbräuchliche Speicherung oder Verwendung der Passinhalte durch kontrollierende Staaten nicht verhindert werden. Überdies können Lesegeräte entwendet oder EAC-Zugriffszertifikate unerlaubt weitergegeben werden. Kritiker weisen zudem darauf hin, dass durch Täuschung oder Bestechung echte E-Pässe mit falschen Daten erworben werden können. Daher sei ein Abgleich mit einer Referenzdatenbank nötig. Kritiker sehen daher in einem Referenzabgleich auch ein Datenschutzrisiko, da in diesem Zusammenhang eine umfassende und zukünftig europaweite Sammeldatei entstehen könnte.

Ausgewählte Quellen:

- Beel, Jöran/ Gipp, Bela (2005): E-Pass. Der neue biometrische Reisepass. Herzogenrath. Shaker-Verlag.
- http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Nachrichten/Pressemitteilungen/2007/02/kommunen__epass.html
- http://www.bmi.bund.de/cln_028/nn_1082274/Internet/Content/Themen/PaesseUndAusweise/Einzelseiten/Biometrie__FAQ.html
- http://www.epass.de
- http://www.bsi.de/fachthem/epass/index.htm
- http://www.heise.de/ct/hintergrund/meldung/65898
- http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf
- http://www.bsi.de/fachthem/epass/EACTR03110_v101.pdf
- Strate, Gregor/ Kersten, Jan (2005). Funkchips – „Radio Frequency Identification“ (RFID). DER AKTUELLE BEGRIFF, Nr. 15/2005. (Stand der Internetquellen: 16. März 2007)

Verfasser: Dipl.-Pol. Gregor Strate, Praktikant Thomas Metz, Fachbereich WD 8, Umwelt, Naturschutz, Reaktorsicherheit, Bildung und Forschung