▶ePASS FIBEL 2007

INFORMATIONEN ZUM ELEKTRONISCHEN REISEPASS

BUNDESDRUCKEREI

INHALT

SEHR GEEHRTE LESERINNEN UND LESER,

die ePass-Fibel entstand aufgrund der Vielzahl von Anfragen, die in den letzten Jahren an die Bundesdruckerei als Hersteller der deutschen elektronischen Reisepässe aber auch an das Bundesministerium des Innern als verantwortlichem Bundesressort herangetragen wurden. Nach Einführung des ePasses der ersten Generation im November 2005 betraf dies vor allem die konkrete technische Umsetzung der passrechtlichen EG-Verordnung sowie eng damit verknüpfte Themen, beispielsweise die Sicherheitseigenschaften der neuen Dokumente, Datenschutz und Datensicherheit.

Mit der Broschüre liegt nun eine Informationssammlung vor, aus der die organisatorisch-technische Komplexität des ePass-Projekts hervorgeht und die Lösungsansätze zu den damit einhergehenden Fragen: Hierbei hatten wir es mit einem zweistufigen Prozess zu tun, weil nach dem ersten biometrischen Merkmal, dem digitalen Passfoto, ab November dieses Jahres zusätzlich die Fingerabdrücke in ePässen der zweiten Generation gespeichert werden. Zudem wird deutlich, dass parallel zur Vorbereitung der neuen Dokumente eine umfassende Infrastruktur konzipiert und ausgerollt werden musste. Die Qualitätssicherungssoftware für biometrische Daten und Hardware-Komponenten wie die ePass-Leser in Passämtern sind Beispiele dafür. In enger Zusammenarbeit der Bundesdruckerei mit dem Bundesministerium des Innern und seinen spezialisierten Behörden – dem Bundeskriminalamt und dem Bundesamt für Sicherheit in der Informationstechnik – sowie Ländern und Kommunen konnte dieses Großprojekt bewältigt werden. Über vier Millionen elektronische Pässe der ersten Generation wurden bislang in Deutschland ausgegeben.

Die Mitarbeiterinnen und Mitarbeiter in den 6.000 deutschen Passbehörden bereiten sich nun auf die zweite ePass-Generation vor. Mit der Novellierung des deutschen Passgesetzes und den ergänzenden Verordnungen haben wir die Voraussetzungen dafür geschaffen. Auch die Ausstattung der Kommunen mit Fingerabdruck-Scannern und Software für die elektronischen Passantragsverfahren ist bereits erfolgt. Nach Pilotierungen und einem erfolgreichen Feldtest zur Fingerabdruckaufnahme, -qualitätssicherung und -übermittlung bin ich mir sicher, dass auch der 1. November 2007 ein positives Datum für die Dokumentensicherheit und den Innovationsstandort Deutschland sein wird.

Die Bundesdruckerei stellt mit dieser ePass-Fibel umfassende Informationen zum Projekt zur Verfügung. Hierfür sowie für die konstruktive Zusammenarbeit möchte ich mich bedanken.

Ihnen wünsche ich eine anregende Lektüre.

Dr. August Hanning
Staatssekretär im Bundesministerium des Innern

IDENTITÄT SICHER SCHÜTZEN UND BEWAHREN

Ab Herbst dieses Jahres werden in deutschen ePässen erstmalig die Daten von zwei Fingerabdrücken des Dokumenteninhabers im ePass-Chip gespeichert. Über die Möglichkeit eines direkten Abgleichs von Live-Aufnahmen und im Chip gespeicherten ID-Daten wird eine neue Dimension hinsichtlich eindeutiger Verbindung von Dokument und Dokumenteninhaber erreicht und der Schutz der persönlichen Identität der Bürger weiter ausgebaut.

Im November 2005 war Deutschland eines der ersten Länder, das gemäß der Empfehlungen der Internationalen Zivilen Luftfahrtorganisation ICAO und der sicherheitstechnischen Anforderungen der EU die Phase 1 des ePass-Projektes, also die Einbindung der Gesichtsbiometrie und den Aufbau der notwendigen technischen Infrastrukturen, in einem integrierten Hochsicherheitssystem verwirklicht hat. Im November dieses Jahres werden wir erneut als einer der ersten Staaten über den erweiterten Zugriffschutz EAC die Fingerabdruckdaten von Bürgern sichern und Phase 2 des ePass-Projektes in der gesamten ID-Prozesskette verankern.

Hervorzuheben ist ganz besonders die Vorreiterrolle des Bundesministerium des Innern (BMI) bei der zügigen Einführung des ePasses sowie bei der Arbeit in den europäischen und internationalen Gremien. Die Experten aus dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie dem Bundeskriminalamt (BKA) haben auf dem Gebiet der ePass-Technik sowie der Standardisierungsfragen wertvolle Grundlagenarbeit geleistet, die maßgebliche Voraussetzung für die erfolgreiche Umsetzung der ePass-Projekte in Deutschland und anderen Staaten war.

Einzellösungen werden den vor uns liegenden Herausforderungen längst nicht mehr gerecht. Hochsicherheitstechnologie bedeutet in interoperablen Systemen zu denken, die von der Datenerfassung über die Herstellung und Personalisierung der Dokumente bis hin zu ihrer Überprüfung bei Zutritts- oder Grenzkontrollen einen in sich geschlossenen und international abgestimmten Sicherheitskreislauf abbilden.

Die Bundesdruckerei trägt mit ihren innovativen Produkten und Lösungen, die über die Arbeit in zahlreichen internationalen Gremien beständig weiter entwickelt werden, dazu bei, die weltweiten Sicherheitsstandards kontinuierlich zu verbessern. Wenn deutsche Bürger im Herbst dieses Jahres erstmalig die Daten ihrer Fingerabdrücke in den Chip der neuen ePässe integriert haben, werden wir eines der anspruchsvollsten Sicherheitskonzepte weltweit realisiert haben.

Mit der vorliegenden „ePass-Fibel" möchten wir Ihnen Einblicke geben in die technischen, rechtlichen und organisatorischen Voraussetzungen, die bis zum November dieses Jahres erfüllt sein werden, um für jeden Bürger in Deutschland einen reibungslosen Beantragungs- und Ausgabeprozess sicher zu stellen. Damit leisten wir unseren Beitrag, um eine deutlich verbesserte Identitätssicherheit zu verwirklichen. An dieser Stelle bedanken wir uns bei unseren Partnern Infineon Technologies AG und NXP Semiconductors Germany GmbH für die überaus konstruktiven Beiträge zur Entstehung dieser Fibel.

Berlin, im Oktober 2007
Ulrich Hamann
Vorsitzender der Geschäftsführung der Bundesdruckerei GmbH

Quelle: Bundesministerium des Innern

1. DER ePASS – EIN REISEDOKUMENT MIT KONTAKTLOSEM CHIP

▶ Mit Einführung elektronischer Reisepässe, kurz ePässe, wurde eine neue Dimension der Dokumentensicherheit und des Identitätsschutzes erreicht, indem die persönlichen Daten und das Gesichtsbild des Passinhabers in einem integrierten elektronischen Chip gespeichert werden. In Deutschland wurde die erste Phase zur Einführung moderner ePässe am 1. November 2005 gestartet und erfolgreich umgesetzt.

Ab dem 1. November 2007 sollen die kontaktlosen Chips auch die Daten von zwei Fingerabdrücken deutscher Bürger aufnehmen.

Die rechtlichen, politischen und technischen Voraussetzungen zur Entwicklung moderner ePass-Systeme wurden in den vergangenen Jahren in zahlreichen internationalen Gremien und Fachausschüssen vorbereitet und in den Entwicklungsabteilungen der führenden Anbieter von Hochsicherheitstechnologien umgesetzt. ◀

1.1 Die Empfehlungen der International Civil Aviation Organization (ICAO)

▶ Der internationale Einsatz von Reisedokumenten erfordert Interoperabilität zwischen den beteiligten Systemen. Diese kann nur über eine entsprechende Standardisierung der verwendeten Systeme und Dokumente erreicht werden.

Die Internationale Zivile Luftfahrtorganisation ICAO übernimmt als Unterorganisation der Vereinten Nationen (UN) seit Jahrzehnten die Aufgabe, über die Vereinheitlichung und Absicherung international gültiger Reisedokumente den weltweiten Reiseverkehr zu erleichtern und nachhaltig abzusichern. Sie ist gleichzeitig die zentrale Institution, die sich über die Entwicklung international abgestimmter Standards mit neuen Sicherheitstechnologien und biometrischen Verfahren für Reisedokumente beschäftigt und Empfehlungen für die optimale Abwicklung, Sicherheit und Umweltverträglichkeit in der zivilen Luftfahrt ausspricht. Bereits in den 1990er Jahren wurde von der ICAO der maschinenlesbare Pass (MRP) standardisiert.

Seit Juli 2005 liegt einer der Arbeitsschwerpunkte der ICAO in der Standardisierung elektronischer Komponenten für internationale Reisedokumente, die im Standard 9303 definiert sind. Hierin werden sowohl die technischen Spezifikationen des Chips und die auf dem Chip enthaltenen Datenstrukturen als auch die Verfahren zur Speicherung von Gesichtsbildern und Fingerabdrücken und die Verfahren zur Erzeugung elektronischer Schlüssel umfassend beschrieben. Als Basishardware für elektronische Pässe ist entsprechend der ICAO-Vorgaben ein kontaktloser Prozessorchip vorgesehen.

Im Jahr 2001 legte die ICAO als international gültiges Standardverfahren zur Steigerung der Sicherheit im grenzüberschreitenden Reiseverkehr die Einführung elektronischer Reisepässe mit Gesichtsbiometrie fest.

Derzeit folgen rund 110 UN-Mitgliedsstaaten den Empfehlungen der International Civil Aviation Organization und geben an ihre Bürger ICAO-konforme maschinenlesbare Reisedokumente aus. Alle übrigen Mitgliedsstaaten haben sich über entsprechende Absichtserklärungen dazu verpflichtet, bis spätestens zum April 2010 ihre Pässe auf das von der ICAO vorgegebene Sicherheitsniveau anzuheben.

Damit werden in absehbarer Zeit in allen ICAO-konformen Reisepässen auf der so genannten Datenseite die Identitätsdaten, ein Foto oder digitales Bild des Dokumenteninhabers und eine zweizeilige maschinenlesbare Zone (MRZ) integriert sein. Über optische Verfahren können die Daten auf Basis der MRZ von autorisierten Instanzen computergestützt ausgewertet und bei der Grenzkontrolle entsprechend der gesetzlichen Bestimmungen des Einreiselandes mit vorhandenen Datenbanken abgeglichen werden. ◄

1.2 Die Politik als Impulsgeber und Treiber der ePass-Entwicklung

► Neue Ausprägungen des internationalen Terrorismus, der grenzüberschreitenden Kriminalität und des Identitätsdiebstahls haben die Nutzung aller Mittel und Möglichkeiten, die die Informationstechnologie zum Schutz der Identität jedes Bürgers bietet, zwingend erforderlich gemacht.

Die Forderung nach elektronischen Reisedokumenten mit integrierten biometrischen Merkmalen – spätestens nach dem 11. September 2001 von der internationalen Staatengemeinschaft nachdrücklich unterstrichen – hat die Entwicklung entsprechender Technologien nachhaltig vorangetrieben. Über neue Gesetze, wie den „US Enhanced Border Security and Visa Reform Act of 2002", das die 27 Mitgliedsstaaten des VISA-Waiver-Programms seit Oktober 2004 dazu verpflichtet, durch die Einführung von ePässen einen erleichterten visumfreien Reiseverkehr in die USA zu ermöglichen, entstanden weltweit neue politische Vorzeichen.

Bereits am 13. Dezember 2004 reagierte die Europäische Union mit der Richtlinie 2252/2004 auf die internationale Sicherheitslage und beschloss verpflichtend für alle EU-Mitgliedsstaaten die Einführung elektronischer Reisepässe mit biometrischen Merkmalen.

In der EU-Richtlinie sind die Standards und technischen Spezifikationen für Material und Drucktechniken sowie für die erforderlichen biometrischen Daten des neuen ePasses festgelegt. Mit einem digitalisierten Bild als Pflichtkriterium legt sie die Gesichtsbiometrie als Standardtechnologie für europäische Reisedokumente fest und definiert Fingerabdrücke als weiteres, in einer zweiten Phase zu integrierendes biometrisches Standardmerkmal.

Mit Ausnahme von Großbritannien und Irland haben sich alle EU-Staaten dazu verpflichtet, das digitale Lichtbild spätestens 18 Monate nach Inkrafttreten der Richtlinien in ihre Reisedokumente aufzunehmen. Drei Jahre nach Verabschiedung der erforderlichen Sicherungsstandards sind auch die Daten von zwei Fingerabdrücken des Dokumenteninhabers im neuen ePass zu integrieren.

Das Bundesministerium des Innern (BMI) und seine nachgeordneten Behörden haben besonderen Anteil an der zügigen Implementierung der ePass-Technologie. Die deutschen Experten leisten in europäischen und internationalen Gremien vor allem auf dem Gebiet der ePass-Technik und bei Standardisierungsfragen wertvolle Arbeit.

Bereits 2004 wurde auf Initiative des BMI, des BSI und deutscher Unternehmen die „Essen-Group" gegründet. Die „Essen Group" ist eine informelle und länderübergreifende Arbeitsgruppe, die sich mit den ePässen der neuen Generation in Europa beschäftigt. Sie gibt Empfehlungen für Experten- und Entscheidungsgremien und war u.a. federführend bei der Entwicklung des „Golden Reader Tools" (Lese-Software für elektronische Dokumente) beteiligt.

Besonders hervorzuheben ist das Engagement der deutschen Politik auch bei der Durchführung des Interoperabilitätstests 2006 in Berlin. Kurz vor Ablauf

des EU-weit verbindlichen Stichtags zur Einführung von ePässen konnte bei der Veranstaltung bewiesen werden, dass die Vorgaben für die Standardisierung der ePässe erfolgreich waren und technisch weltweit wirkungsvoll umgesetzt werden konnten. ◀

1.3 Die deutsche ePass-Einführung in zwei Phasen

▶ Gemäß der bindenden EU-Richtlinie wird der ePass in Deutschland in zwei Stufen eingeführt. Seit dem 1. November 2005 enthalten die neuen deutschen Reisedokumente einen in die vordere Decke des Passbucheinbandes eingebrachten kontaktlosen Chip, in dem neben den personenbezogenen Daten auch das digitale Lichtbild des Passinhabers gespeichert wird. Über das stilisierte Chipsymbol auf der vorderen Deckseite des Passbuches ist das neue Dokument als ePass erkennbar.

1.3.1 Phase 1 – Integration der Gesichtsbiometrie

Das elektronisch gespeicherte digitale Passbild hat bereits in der ersten Einführungsphase die Bindung zwischen Dokument und Dokumenteninhaber sowie die Möglichkeiten zuverlässiger Kontrollverfahren deutlich verstärkt.

Über den Abgleich des auf der Passkarte gedruckten Passbildes mit den im Chip gespeicherten Bilddaten konnte bereits Ende 2005 ein deutlicher Zugewinn an Dokumentensicherheit erreicht werden. Durch den zusätzlich möglichen 1:1-Vergleich der gespeicherten Informationen mit live aufgenommenen Kamerabildern wurde zudem der Einstieg in die computergestützte Identitätsverifikation ermöglicht.

ePass-Symbol auf dem deutschen Reispass

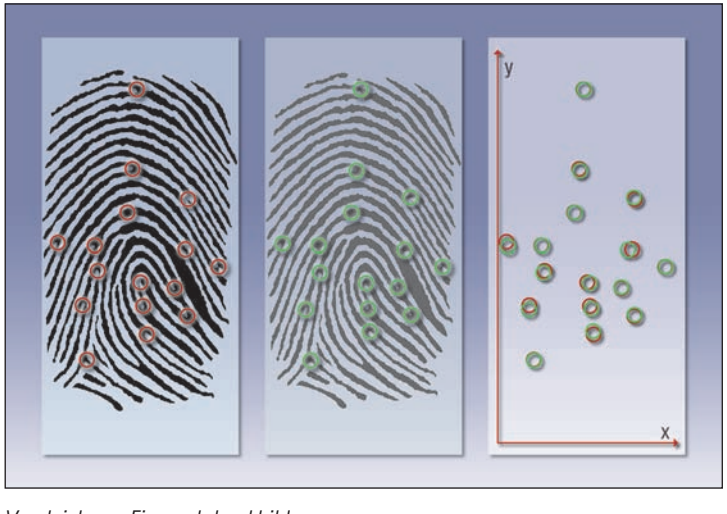
Da ausschließlich die Frontalaufnahme eine softwarebasierte Auswertung von Passfotos erlaubt, wurde diese von der ICAO als Standard für biometrietaugliche bzw. biometrisch auswertbare Passbilder definiert. Die Bundesdruckerei und das BMI stellten zur Steigerung der Bildqualität sowohl den zuständigen Behörden als auch Fotografen eine Fotomustertafel sowie eine Schablone zur visuellen Prüfung von Passbildern bereit. Darüber hinaus erhielten die Behörden eine spezifische Prüfsoftware, die die gescannten Gesichtsbilder automatisch auf die Einhaltung der ICAO-Anforderungen überprüft und in die weiteren Bearbeitungsprozesse überführt. Der Zugriff auf die im Chip gespeicherten Personendaten und auf das gespeicherte Lichtbild wird in Phase 1 durch den Schutzmechanismus Basic Access Control (BAC) gesichert.

1.3.2 Phase 2 – Integration der Fingerabdruckdaten

Ab dem 1. November 2007 werden in deutschen Passbehörden neben dem digitalisierten Gesichtsbild auch zwei Fingerabdrücke des ePass-Antragstellers erfasst.

Während der Erfassung werden die Fingerabdruckdaten einer softwaregestützten Qualitätsprüfung unterzogen. Um die hohen Qualitätsanforderungen an die gespeicherten Datensätze zu erfüllen, müssen pro Finger insgesamt drei Aufnahmen gemacht und analysiert werden, aus denen automatisch das beste Ergebnis ausgewählt wird. Über präzise Sonderregeln ist festgelegt, auf welche Weise auch Personen mit schwach ausgeprägten Fingerabdrucklinien oder fehlenden Fingergliedmaßen in den Erfassungsprozess aufgenommen werden und einen gültigen ePass erhalten können.

Beim Erfassungsprozess werden die aufgenommenen Fingerabdrücke automatisch miteinander verglichen, indem die Lagekoordinaten der Minutien (das sind die Schnittpunkte von Fingerabdrucklinien) zweier digitaler Bilder zur Deckung gebracht werden. Wird ein hinreichend hoher Grad von Übereinstimmung bei den Lagekoordinaten festgestellt, werden beide Bilder derselben Person zugeordnet und die biometrische Verifikation gilt als erfolgreich. Diese Form der Prüfung entspricht dem bei der späteren Grenzkontrolle einzusetzenden Verfahren.



Vergleich von Fingerabdruckbildern

Der Zugriff auf die Fingerabdrücke wird durch einen erweiterten Zugriffsschutz, die Extended Access Control (EAC), geregelt. Die Erlaubnis zum Auslesen der Fingerabdruckdaten erhalten nur berechtigte Länder in Form einer elektronischen Zugriffsberechtigung.

Ebenso wie die gesichtsbiometrischen Informationen werden auch die Daten der Fingerabdrücke als Datei gespeichert und zusammen mit allen übrigen Antragsdaten verschlüsselt und über mehrfach gesicherte Kommunikationsinfrastrukturen (vgl. Pkt. 3) an den Passproduzenten, die Bundesdruckerei, übermittelt. Der Passproduzent speichert die Fingerabdrücke ausschließlich im Chip des Reisepasses. Nach Herstellung und erfolgreicher Qualitätsprüfung des Passes werden die Fingerabdrücke bei der Bundesdruckerei gelöscht. Der fertige ePass wird wie üblich zur Passbehörde geschickt und liegt dort für den Bürger zur Abholung bereit. Nach einer weiteren Qualitätskontrolle durch den Behörden-Mitarbeiter und bei Bedarf auch durch den Antragsteller (über einen ePass-Leser) werden die Fingerabdruckdaten auch in den Systemen der Passbehörde gelöscht. Somit sind die Fingerabdrücke ausschließlich im Chip des Reisepasses gespeichert. Eine Datenhinterlegung im Passregister oder in einer anderen Datenbank ist in Deutschland nicht zulässig. ◄

1.4 ePass-Infrastruktur in den Passbehörden

▶ Den Passbehörden kommt bei der Beantragung und Ausgabe von Reisedokumenten die zentrale Bedeutung zu. Allein aufgrund ihrer großen Anzahl – es gibt in Deutschland rund 6.000 Passbehörden mit etwa 17.000 Arbeitsplätzen und höchst heterogener IT-Infrastruktur – stellt die Integration der neuen Prozesse in die Verfahrensabläufe eine große Herausforderung dar. Die Bundesdruckerei stellt sicher, dass an sämtlichen Arbeitsplätzen die erforderlichen Arbeitsmittel zur Verfügung stehen. Dazu wurden komplexe Informations- und Kommunikationsinfrastrukturen geschaffen, die in der gesamten ID-Prozesskette sichere Datentransfers und Kontrollverfahren gewährleisten.

In Phase 1, also bei der Einführung der Reisepässe mit Chip und gespeichertem Lichtbild als biometrischem Merkmal, wurden alle Arbeitsplätze mit einer Software zur Qualitätssicherung der biometrischen Daten ausgestattet. Zusätzlich ist in Artikel 4 der EU-Richtlinie 2252/2004 festgelegt, dass jeder Dokumenteninhaber das Recht hat, seine im ePass-Chip gespeicherten Daten einzusehen. Dazu sind Lesegeräte erforderlich, die sowohl auf die technischen Sicherheitsmerkmale des Dokuments als auch auf die vorgeschriebenen Verfahren des Zugriffsschutzes für gespeicherte Biometriedaten abgestimmt sind. Die Bundesdruckerei hat sämtliche Passbehörden mit entsprechenden, einfach zu bedienenden ePass-Lesegeräten ausgestattet.

In Phase 2, also mit der zusätzlichen Aufnahme der Fingerabdrücke in den Reisepass, werden die bestehenden Infrastrukturen nochmals erweitert und über zahlreiche zusätzliche Sicherheitsmechanismen geschützt. Hierzu stattet die Bundesdruckerei alle Passbehörden mit Fingerabdruck-Scannern aus. Zudem liefert die Bundesdruckerei für sämtliche Arbeitsplätze in den Passbehörden ein neues Biometrie-Modul für kommunale Einwohnerverfahren, das alle für die Passdatenerfassung notwendigen Funktionen der Bildbewertung und Fingerabdruckerfassung beinhaltet.

Das Biometrie-Modul ist eine Erweiterung des Einwohnerverfahrens und bietet im Einzelnen die folgenden Biometrie-Funktionen:

- Bewertung von Passbildern auf Biometrietauglichkeit
- Anzeige und Ausgabe der Bewertungsergebnisse
- Anzeige und Ausgabe von Korrekturhinweisen
- Bereitstellung der Bewertungsergebnisse und Qualitätsinformationen für das Einwohnerverfahren
- Automatische Komprimierung der aufgenommenen Passbilder
- Aufnahme von Fingerabdruckdaten
- Anzeige des Live-Bildes vom Fingerabdruck-Scanner
- Qualitätsbewertung des Live-Bildes
- Anzeige des ermittelten Qualitätsindexes aufgenommener Fingerabdrücke
- Automatische Komprimierung aufgenommener Fingerabdrücke.

Mit Hilfe dieser neuesten technologischen Verfahren kann für alle Bürger ein reibungsloser Antragsprozess realisiert werden.

Um die gespeicherten Fingerabdrücke auslesen und im Sinne der vorgeschriebenen Datentransparenz anzeigen zu können, wird die Bundesdruckerei im Rahmen der zweiten Einführungsphase ab Oktober 2007, beginnend mit den Landeshauptstädten, zudem alle ePass-Leser an die Anforderungen des erweiterten Zugriffsschutzes EAC (vgl. Pkt. 3.2) anpassen. ◀

2. DIE SICHERHEITSMERKMALE DES DEUTSCHEN ePASSES

▶ Der deutsche Reisepass zählt zu den sichersten Reisedokumenten weltweit. Die zahlreichen sichtbaren und nicht sichtbaren Sicherheitsmerkmale bilden eine kaum überwindliche Hürde für Totalfälschungen oder Verfälschungen des Dokuments.

Der Chip hebt die Sicherheit des ePasses deutlich an

Über die Integration eines kontaktlosen Chips und die darauf gespeicherten und geschützten biometrischen Merkmale wird ein zusätzliches Sicherheitsmerkmal geschaffen und eine eindeutige Bindung des Dokuments an den Dokumenteninhaber hergestellt. ◀

2.1 Die klassischen Sicherheitsmerkmale des Reisepasses (eine Auswahl)

▶ Das Sicherheitsniveau deutscher Identitätsdokumente wird beständig überprüft und den jeweils aktuellen Anforderungen angepasst. Schon einige Jahre vor Einführung moderner ID-Chiptechnologien konnte die Fälschungssicherheit deutscher Reisepässe über die Integration der von der Bundesdruckerei entwickelten holographischen Sicherheitsmerkmale nochmals erheblich gesteigert werden. Über die Einbindung des so genannten Identigram®, das an verschiedenen Positionen des Dokuments genutzt wird, setzt der deutsche Reisepass national wie international schon seit 2001 neue Sicherheitsstandards.

Sicherheitsmerkmale des deutschen Reisepasses

1 Identigram® – *Holographisches Portrait*

Das Lichtbild des Passinhabers wird bei Betrachtung der Passkarte unter einem flachen Winkel rechts neben dem herkömmlichen Bild ein zweites Mal in holographischer Form erkennbar. Durch das holographische Abbildungsverfahren ergibt sich eine stilisierte Hell-Dunkel-Wiedergabe der Bildinhalte des Ausweisfotos, in die links vier Bundesadlermotive eingearbeitet sind.

2 Identigram® – *3D-Bundesadler*

Unter einem bestimmten Betrachtungswinkel wird eine dreidimensionale Darstellung des Bundesadlers in roter Farbe erkennbar.

3 Identigram® – *Kinematische Bewegungsstrukturen*

Die über dem herkömmlichen Lichtbild angeordneten Bewegungsstrukturen zeigen als zentrales Element einen von zwölf Sternen umgebenen Bundesadler. Durch ein Kippen der Passkarte von links nach rechts verwandelt sich das in der

Mittelposition sichtbare Adlermotiv über eine Sechseckstruktur in den Buchstaben „D". Die Sterne werden abwechselnd größer und kleiner. Die Sechsecke oberhalb und unterhalb des Adlermotivs wandern auf und ab. Eine Kette von Sternen am rechten Bildrand geht in ein „D" über.

4 Identigram® – *Makro- und Mikroschriften*

Am linken Rand des herkömmlichen Lichtbildes bestehen die kinematischen Bewegungsstrukturen aus einem geschwungenen Makroschriftband mit dem Text „BUNDESREPUBLIK DEUTSCHLAND", an das sich links mehrere, parallel verlaufende Mikroschriftzeilen mit gleichem Text anschließen.

5 Identigram® – *Kontrastumkehr*

Beim Abkippen der Passkarte wird der Kontrast des zentralen Adlermotivs umgekehrt, so dass das Motiv dunkel in einer hellen Sechseckfläche erscheint.

6 Identigram® – *Holographische Wiedergabe der MRZ*

Die maschinenlesbaren Zeilen (MRZ) der Passkarte werden holographisch wiedergegeben. Sie liegen jeweils über den herkömmlichen maschinenlesbaren Zeilen.

7 Identigram® – *Maschinell prüfbare Struktur*

Das Identigram® enthält eine maschinell prüfbare Struktur, die zur Unterstützung manueller Sichtkontrollen eine maschinelle Echtheitsprüfung ermöglicht. Diese Struktur beinhaltet keine personen- oder dokumentenbezogenen Daten.

8 Oberflächenprägung

Die Passkarte ist in ein Spezial-Laminat eingebettet. Die reliefartige, haptisch erkennbare Prägung beinhaltet den Buchstaben „D", das Bundesadlermotiv und die Schriftzüge „BUNDESREPUBLIK DEUTSCHLAND" und „REISEPASS".

9 Sicherheitsdruck mit mehrfarbigen Guillochen

Guillochen sind Schutzmuster aus feinen, miteinander verschlungenen Linien, deren Strukturen sich in verschiedenen Farben passgenau zu einem ausgewogenen Gesamtbild ergänzen. Bei Reproduktionen (z.B. Farbkopien) werden die Linienstrukturen des Originals in punktierte Rasterstrukturen aufgelöst.

10 Laserbeschriftung

Name und Vorname des Passinhabers werden am rechten Lichtbildrand durch Lasertechnik in das Ausweismaterial geprägt und sind haptisch erkennbar.

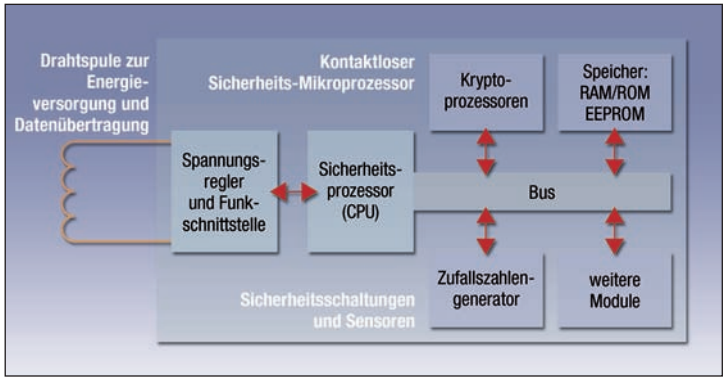
11 Wasserzeichen

Im durchscheinenden Licht ist im Papier der Pass- und Ausweiskarte ein mehrstufiges Wasserzeichen zu erkennen, das mehrere, über die Fläche verteilte, stilisierte Adler darstellt.

Darüber hinaus wird der ePass auf speziellen, extra für die Bundesdruckerei hergestellten Produktionsanlagen und mit exklusiv für die Bundesdruckerei gefertigten Materialien erstellt. Die geschlossene Produktionskette gewährleistet, dass keine unpersonalisierten Rohdokumente vorhanden sind, die für Fälschungen verwendet werden könnten. ◀

2.2 Der Chip als neues Sicherheitsmerkmal

▶ Der im ePass verwendete Chip ist ein Sicherheits-Prozessorchip (Security Controller) und damit ein Computer im Kleinstformat.



Aufbau eines Sicherheits-Mikroprozessors

Die Hardware. Auf wenigen Quadratmillimetern verwaltet der auf einem dünnen Siliziumscheibchen aufgebrachte Sicherheits-Prozessorchip einen 64 bis 72 kByte Speicher für die Biometrie-Anwendungen des ePasses, schützt den Zugriff auf die gespeicherten Daten und gewährleistet die sichere Kommunikation mit Lesegeräten. Die Datenübertragung zwischen dem Chip und dem Lesegerät erfolgt gemäß des Standards ISO/IEC 14443 mit einer Frequenz von 13.56 Megahertz kontaktlos über Funk. Hierfür kann der Abstand zwischen den beiden technischen Einheiten Chip und Lesegerät von einigen Millimetern bis zu maximal 10 Zentimetern variieren.

Der Chip generiert aus den Funkwellen des Terminals seine Betriebsspannung. Über die durch den Chip gesteuerte Modulation der Feldstärke werden Informationen zum Lesegerät übertragen. Dieses induktive Verfahren auf Basis von Drahtspulen als Antennen ermöglicht Datenübertragungsraten von ca. 100 bis 850 Kilobits pro Sekunde. Der deutsche ePass arbeitet heute mit einer Übertragungsrate von etwa 424 Kilobit pro Sekunde und ermöglicht so die schnelle Übermittlung der auf dem Chip gespeicherten Daten. Die im ePass eingesetzten Chips werden in Deutschland von den Firmen Infineon und NXP produziert.

Schutzmechanismen des Chips. Alle für den ePass verwendeten Chips verfügen über starke Abwehrmechanismen gegen äußere Angriffe. Sämtliche Speicherinhalte werden durch kryptografische Verfahren verschlüsselt. Der Prozessor überwacht laufend seine internen Betriebszustände und kann damit sofort auf Störungen bei der Abarbeitung von Programmen reagieren. Spezielle Sensoren identifizieren Manipulationen von Außen, z.B. Veränderungen der Versorgungsspannung, der Arbeitsfrequenz, der Temperatur oder Einwirkungen durch Laserlicht.

Distribution und Weiterverarbeitung. Grundsätzlich müssen alle ePass-Chips vom Hersteller mit digitalen Transportschlüsseln abgesichert werden. Nur wer über die entsprechenden Gegenstücke zum Transportschlüssel verfügt, kann die Chips im nächsten Schritt personalisieren. Damit wird eine Bearbeitung durch nicht autorisierte Prozesse verhindert. Nach der erfolgreichen Personalisierung in der Bundesdruckerei wird der Chip verriegelt, was nachträgliche Änderungen, Ergänzungen oder Verfälschungen der Chipdaten verhindert.

Die Sicherheitszertifizierung. Der eingesetzte Prozessorchip hat gemäß den international verbindlichen Kriterien diverse standardisierte Prüfverfahren durchlaufen und ist in der höchsten Sicherheitsstufe (Common Criteria EAL5+) klassifiziert. Diese Klassifizierung wurde nach intensiven Tests durch autorisierte Sicherheitslabors unter Verwendung des Schutzprofils „BSI-PP-0002" vom Bundesamt für Sicherheit in der Informationstechnik (BSI) durch ein Zertifikat bestätigt.

Auf dem Prozessorchip sorgt ein von T-Systems entwickeltes Betriebssystem (TCOS 4.x) für die elektronische Sicherheit der Daten sowie für die Verwaltung von Zugriffsrechten. Auf Basis der vom BSI entwickelten Schutzprofile „BSI-PP-0026 Machine Readable Travel Document with ICAO-Application, Extended Access Control" und „BSI-PP-0017 Machine Readable Travel Document with ICAO-Application, Basic Access Control" wurde das Betriebssystem und die Datenstruktur auf dem Sicherheitsniveau „Common Criteria EAL4+" zertifiziert.

Alle Herstellungs-, Distributions- und Personalisierungsprozesse in der Bundesdruckerei sind ebenfalls Gegenstand der Sicherheitszertifizierung durch das BSI und werden strengstens kontrolliert und regelmäßig auditiert. ◀

Der deutsche ePass-Leser

3. SCHUTZMECHANISMEN FÜR DIE IM ePASS GESPEICHERTEN DATEN

▶ Die Daten im Chip eines ePasses werden gemäß der ICAO „Logical Data Structure"(LDS) über ein spezifisches Dateisystem gespeichert. In den einzelnen Datengruppen (DG) dieser Datenstruktur sind auch die personen- und dokumentbezogenen Daten hinterlegt. Im Detail werden die folgenden Datengruppen unterschieden:

DG 1 beinhaltet den Vor- und Nachnamen, das Geburtsdatum, Geschlecht und die Staatsangehörigkeit des Passinhabers sowie die Seriennummer des Passes, die Kennnummer des ausstellenden Staates sowie den Dokumententyp (z. B. P= Pass) und das Gültigkeitsdatum

DG 2 beinhaltet das Gesichtsbild des Passinhabers

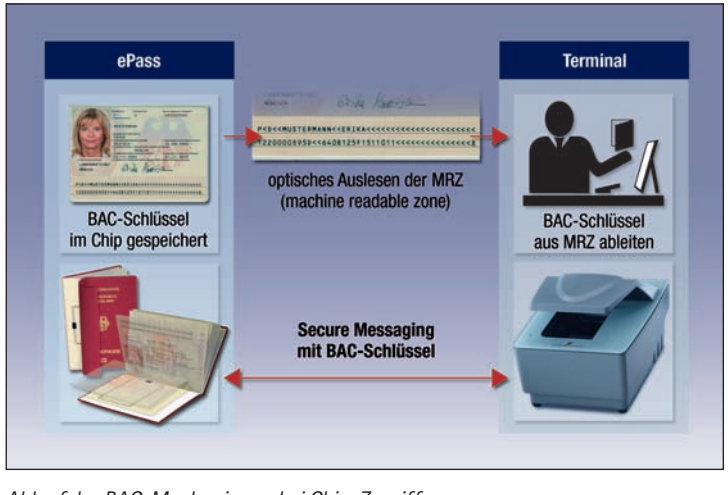
DG 3 beinhaltet zwei Bilder von Fingerabdrücken des Passinhabers.

Der autorisierte Daten-Zugriff wird über verschiedene mit dem Chip korrespondierende Schutzmechanismen geregelt. Im deutschen ePass werden die Informationen der Datengruppen DG 1 und DG 2 über die „Basic Access Control (BAC)" geschützt. Ein Auslesen der Datengruppe DG 3 ist ausschließlich über die Mechanismen des erweiterten Zugriffschutzes „Extended Access Control (EAC)" möglich. Beide Schutzmechanismen sind innerhalb der EU standardisiert und für die Mitgliedsstaaten verpflichtend. ◀

3.1 Basic Access Control (BAC)

▶ In Europa müssen elektronische Reisepässe mit integriertem Chip, auf dem die biometrischen Merkmale des Gesichts gespeichert sind, zur Vermeidung eines unberechtigten Mitlesens (eavesdropping) oder Auslesens (skimming) mindestens den Schutzmechanismen der Basic Access Control (BAC) entsprechen.

Die wesentliche Funktion des BAC-Verfahrens ist es, dass ein Auslesen der Daten nur auf Basis der erfolgreichen Authentisierung eines berechtigten Lesegeräts erfolgen kann. Hierzu werden zunächst das Geburtsdatum des Passinhabers sowie die Passnummer und das Gültigkeitsdatum des Dokuments optisch aus den maschinenlesbaren Zeilen (MRZ) des ePasses ausgelesen. Aus diesen Informationen errechnet das Lesegerät einen spezifischen Zugriffsschlüssel, der den ePass-Chip zur Ausgabe einer Zufallszahl berechtigt und den ePass-Leser aktiviert, die zum Chip passende Schlüsselhälfte für die komplette Datenübertragung zu generieren. Nach einer erfolgreichen BAC-Authentisierung werden zwischen dem Lesegerät und dem ePass-Chip über standardisierte Kryptoverfahren (3DES-Verfahren) nochmals geheime Schlüssel mit einer Schlüssellänge von 112 Bit ausgetauscht. Damit sind die Daten während der Übertragung zuverlässig gegen unberechtigte Zugriffe geschützt. ◀



Ablauf des BAC-Mechanismus bei Chip-Zugriff

3.2 Extended Access Control (EAC)

▶ Zur Absicherung der ab dem 1. November 2007 im deutschen ePass gespeicherten Fingerabdrücke wurde im Auftrag des Bundesministeriums des Innern (BMI) und unter Federführung des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) der erweiterte Zugriffsschutz Extended Access Control (EAC) entwickelt. Mit dem erweiterten Zugriffsschutz EAC kann ein deutlich höheres Sicherheitslevel gewährleistet werden. Das EAC-Verfahren ist für alle EU-Mitgliedsstaaten im Kontext der Speicherung von Fingerabdrücken der vorgeschriebene Sicherheitsstandard.

Die EAC bringt mit Blick auf die höheren Datenschutzanforderungen zwei wesentliche Vorteile mit sich:

1. **EAC sichert den Ausleseprozess der Fingerabdruckdaten durch zusätzliche Schutzmechanismen,**
2. **EAC ermöglicht die Vergabe selektiver Zugriffsrechte, so dass nur autorisierte Lesegeräte auf die Fingerabdruckdaten zugreifen können.**

Deutschland wird als eines der ersten EU-Länder die Ausgabe von ePässen der zweiten Generation realisieren und damit auch erstmalig das Verfahren der EAC in einer hoheitlichen Anwendung einsetzen. Die Bundesdruckerei konnte bereits anlässlich der Fußball-Weltmeisterschaft 2006 in einer ersten Volumenanwendung in der „adidas world of football"-Arena in Berlin die Praxistauglichkeit des EAC-Verfahrens nachweisen.

Da sich fast alle EU-Mitgliedstaaten dazu verpflichtet haben, an ihre Bürger ePässe mit Fingerabdrücken auszugeben, wird sich dieser Standard schrittweise in ganz Europa und in vielen außereuropäischen Staaten durchsetzen.

Was bedeutet EAC?

EAC regelt im Wesentlichen die Zugriffserlaubnis auf die im ePass der zweiten Generation gespeicherten Daten der Fingerabdrücke. Mit Hilfe einer besonderen elektronischen Zugriffsberechtigung erhält ein Lesegerät, wie es beispielsweise bei Grenzkontrollen zum Einsatz kommt, die Erlaubnis zum Auslesen der Fingerabdruckdaten. Ohne ein solches Zugriffszertifikat ist der Ausleseprozess nicht möglich.

Im Rahmen der EAC-Mechanismen muss jedes berechtigte Lesegerät mit einem eigenen Schlüsselpaar, das durch den Chip des Reisepasses überprüft werden kann, ausgestattet sein. Darüber hinaus verfügt es über ein eigenes elektronisches Zertifikat, in dem die spezifischen Rechte des Lesegeräts definiert sind.

Welche spezifischen Zugriffsrechte der auslesenden Instanz (autorisiertes Lesegerät) zugebilligt werden, entscheidet allein das Land, das einen Reisepass ausgibt. Das heißt, auf welche Datengruppen von wem zugegriffen werden darf, ist variabel und ausschließlich der jeweiligen nationalen Country Authority (CA) vorbehalten. Damit kann auch bestimmten Staaten der Zugriff auf die Fingerabdruckdaten eines deutschen Bürgers verwehrt werden.

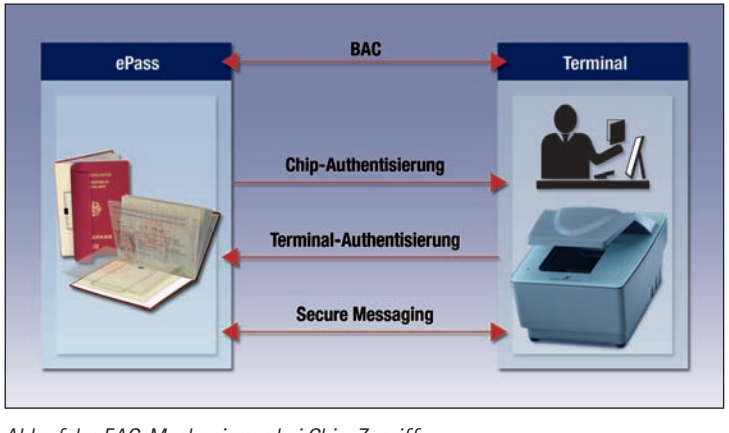
Die zertifikatsbasierte Authentisierung, mit der neben dem berechtigten Zugriff auch die Echtheit des integrierten ePass-Chips überprüft werden kann, bildet somit den eigentlichen Kern der EAC-Technologie. Realisiert wird das Verfahren über asymmetrische kryptographische Verschlüsselungsmechanismen, die auf einer Interaktion zwischen öffentlichen und privaten Schlüsseln beruhen. Ist die Chip- und Terminal-Authentisierung (siehe unten) erfolgreich abgeschlossen, setzt die BAC-geschützte, verschlüsselte Kommunikation zwischen Lesegerät und Chip ein, wobei nochmals verstärkte Sitzungsschlüssel zum Einsatz kommen. ◀

Zum kompletten Auslesen der in einem modernen ePass gespeicherten Daten, inklusive der Fingerabdrücke, bauen in einem EAC-Prozess folgende Abläufe aufeinander auf:

- **Schritt 1:** *Nach erfolgreicher Basic Access Control (BAC) kann auf die persönlichen Daten und das digitale Gesichtsbild zugegriffen werden.*
- **Schritt 2:** *Im Vorgang der so genannten Chip-Authentisierung beweist der Chip, dass er nicht gefälscht oder kopiert ist. Hierzu wird über kryptographische Verfahren in der verschlüsselten Kommunikation zwischen ePass und Lesegerät ein asymmetrischer Mechanismus des Schlüsselaustauschs aufgebaut. Nur ein „echter" Chip (d.h. ein Chip, der ein eigenes Schlüsselpaar besitzt, dessen öffentlicher Schlüssel zertifiziert ist) ist in der Lage, mit dem Lesegerät zu kommunizieren. Damit entsteht automatisch ein sicherer Kopierschutz für die gespeicherten Dateninhalte. Nach der erfolgreichen Chip-Authentisierung ist die Echtheit des Dokuments sicher gestellt.*
- **Schritt 3:** *Abschließend muss sich das Lesegerät mit Hilfe der Terminal-Authentisierung als eine für das Auslesen von Fingerabdruckdaten zugriffsberechtigte Einheit ausweisen. Zu diesem Zweck wird das Authentisierungszertifikat des Lesegeräts während der Kommunikation zwischen Chip und Lesegerät überprüft. In Deutschland entscheidet allein das BMI durch die Vergabe hoheitlicher Zertifikate darüber, wer und welche Geräte Zugriff auf die Fingerabdrücke haben darf. Die Gültigkeit der Zertifikate ist zeitlich begrenzt. Die notwendigen Zertifikate werden über eine Public Key Infrastruktur (PKI) zur Verfügung gestellt.*
- **Schritt 4:** *Die Kommunikation zwischen Lesegerät und Chip erfolgt verschlüsselt und basiert auf dem bereits im BAC-Mechanismus verwendeten „3DES-Verfahren" mit Sitzungsschlüsseln hoher Güte.*

Da die für den Zugriff auf Fingerabdrücke notwendigen Zertifikate in nationaler Verantwortung vergeben werden, sind im internationalen Reiseverkehr zukünftig folgende Szenarien denkbar:

- *Länder, die ihre Lesegeräte nicht an die Chiptechnologie anpassen, werden die Reisepässe auf herkömmliche Weise, also optisch und/oder durch Scannen der Machine Readable Zone (MRZ), prüfen.*
- *Länder, die keine Zertifikate für das Auslesen der Fingerabdrücke erhalten, aber Lesetechnik für e-Pässe besitzen, können von den biometrischen Daten nur das Gesichtsbild aus dem Chip lesen und für die biometriegestützte Kontrolle verwenden.*
- *Länder, die über entsprechende Zertifikate verfügen, können auch die Fingerabdruckdaten von Reisenden auslesen.*

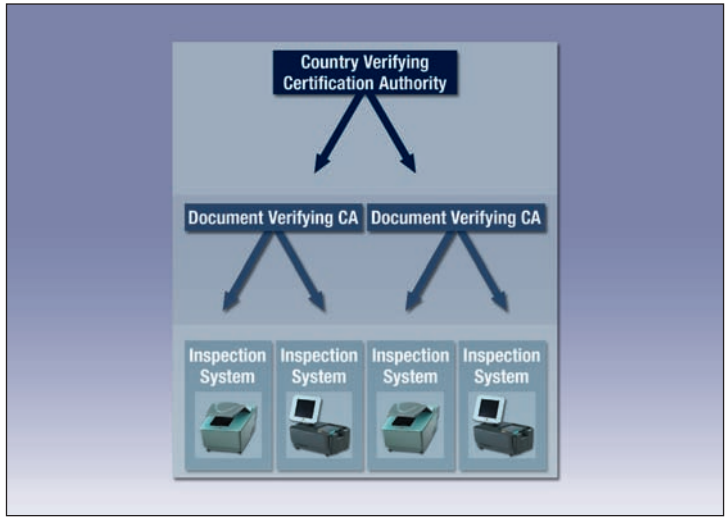


Ablauf des EAC-Mechanismus bei Chip-Zugriff

3.3 Public Key Infrastrukturen (PKI)

▶ Die Zugriffsrechte auf den kompletten Datensatz eines ePasses der zweiten Generation können sowohl auf ein bestimmtes Gerät als auch für eine bestimmte Dauer eingeschränkt werden und müssen auch in inhomogenen Infrastrukturen, z.B. bei Geräten in Botschaften, an Flughäfen oder im mobilen Einsatz, zuverlässig verteilt und zugeordnet werden können.

Für diesen komplexen Verteilungsvorgang bedient sich das EAC-Verfahren einer zweistufigen PKI: Als oberste Vergabeinstanz für hoheitliche nationale Zertifikate fungiert die *Country Verifying Certification Authority (CVCA).* Sie vergibt Berechtigungszertifikate an die zweite Vergabe-Instanz, die so genannte *Document Verifying Certification Authority (DVCA).* Von dieser Ebene werden für einen Pool von Lesegeräten die gültigen Zertifikate verteilt und die Zugangsrechte verwaltet. Auf Basis der von der DVCA vergebenen Zugangsrechte für Dokumente können die *Inspection Systems* der Dokumentenlesegeräte schließlich die erforderlichen Auslese- und Kontrollvorgänge steuern. Dieses Verfahren gilt zunächst nur für die Zugangsberechtigungen innerhalb eines Staates.



3-stufige EAC Public Key Infrastruktur

Will ein Staat einem anderen die Fingerabdrücke „seiner" Bürger zu Kontroll- und Sicherheitszwecken zugänglich machen, steigt die Komplexität des EAC-Verfahrens erheblich. Denn nun müssen sich zusätzlich die national unterschiedlichen Country Verifying Certification Authorities untereinander Berechtigungszertifikate ausstellen und diese verwalten.

EAC ist ein hochkomplexes Thema, das nur wenige Anbieter von Hochsicherheitssystemen professionell steuern und in allen Teilbereichen realisieren können. Die Bundesdruckerei stellt die notwendige Interoperabilität nationaler eDokumente im internationalen Grenzverkehr sowie die notwendigen Infrastrukturen im deutschen ePass-Projekt gemeinsam mit ihrem Tochterunternehmen D-TRUST, einem der ersten zertifizierten Trustcenter in Deutschland, sicher. ◀

4. DATENSCHUTZ UND DATENSICHERHEIT

▶ Mit Blick auf Datenschutz und Datensicherheit elektronischer Reisepässe sind zwei Aspekte zu unterscheiden:

1. Die Frage der grundsätzlichen Datenspeicherung und –verwendung
2. Die Sicherheit der im ePass-Chip gespeicherten Daten.

Auf europäischer Ebene wurden zahlreiche Datenschutz- und Datensicherheitsbestimmungen, insbesondere eine klare Zweckbindungsregelung sowie die Sicherstellung der Integrität, Authentizität und Vertraulichkeit der Daten, abgestimmt. Dabei wurden die Vorschläge der Arbeitsgruppe der Datenschutzbeauftragten aller EU-Staaten (nach Artikel 29 der EG-Datenschutzrichtlinie) im EU-Verordnungsentwurf weitestgehend übernommen.

Deutschland geht im nationalen Passgesetz allerdings noch weit über die europäischen Vorgaben zum Datenschutz hinaus. Im Unterschied zu vielen anderen EU-Mitgliedstaaten wird es in Deutschland keine bundesweite Datenbank mit biometrischen Daten geben. Die Passdaten und das Lichtbild werden ausschließlich im kommunalen Passregister gespeichert. Die Fingerabdrücke werden nach der Ausgabe des Passes durch die Passbehörden gelöscht.

Der ePass ist ein Reisedokument. Damit besteht die wichtigste und ausdrücklich gewollte Funktion des Chips in seiner Lesbarkeit an Grenzkontrollstellen und in der Möglichkeit, durch den maschinellen 1:1-Abgleich biometrischer Daten eine zweifelsfreie Verbindung zwischen Dokument und Dokumenteninhaber herstellen zu können.

Gleichzeitig muss ein unbemerktes Auslesen der Chipinhalte durch Unbefugte zuverlässig verhindert werden. Deshalb sind die Sicherheitseigenschaften elektronischer Reisepässe so angelegt, dass sie sowohl den Forderungen einer reibungslosen und zuverlässigen Auslesbarkeit für autorisierte Kontrollzwecke als auch dem gesetzlich vorgeschriebenen Datenschutz des Bürgers im vollen Umfang gerecht werden.

Datentransparenz. Bürger haben in den Passbehörden jederzeit die Möglichkeit, die auf ihrem ePass-Chip gespeicherten Daten an speziellen Anzeigegeräten, den ePass-Lesern, einzusehen. Diese Daten sind:

- **die personenbezogenen Daten:** Vor- und Nachname, Geburtsdatum, Geschlecht und Staatsangehörigkeit des Dokumenteninhabers,
- **die dokumentenbezogenen Daten:** Serienummer, ausstellender Staat, Dokumententyp und Gültigkeitsdatum,
- **die biometrischen Daten:** ein digitalisiertes Gesichtsbild, zwei Fingerabdrücke.

Datensicherheit. Die Sicherheit der im Chip gespeicherten Daten wurde in internationalen und europäischen Gremien abgestimmt und in EU-weit festgelegten Sicherheitsvorkehrungen verbindlich geregelt. Auf dieser Basis müssen:

- alle im Chip gespeicherten Daten elektronisch signiert werden, so dass sie nicht unbemerkt verändert werden können,
- alle ePass-Chips unmittelbar nach der Personalisierung für weitere Schreibzugriffe gesperrt werden,
- alle ePässe europaweit über die technischen Mechanismen BAC und EAC vor unberechtigten Zugriffen geschützt werden.

Die Zugriffschutzverfahren BAC und EAC wurden maßgeblich durch deutsche Experten vom Bundeskriminalamt (BKA) und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) mitgestaltet.

Schutz vor Angriffen

Trotz dieser weit reichenden Sicherheitsvorkehrungen ist die Angst vor unberechtigten Zugriffen und/oder kriminellen Delikten wie Identitätsdiebstahl oder Dokumentenfälschung auch im Zusammenhang mit den neuen ePässen für deutsche Bürger ein gewichtiges Thema.

Aus diesem Grund sollen im Folgenden einige der meist diskutierten Angriffsszenarien aus der sicherheitstechnologischen Perspektive kurz betrachtet werden:

- Unberechtigtes Auslesen der Chipinhalte
- Ändern der digitalen Daten im ePass
- Klonen der digitalen Daten im ePass
- Erstellen von Bewegungsprofilen
- Abhören der Kommunikation zwischen ePass und Inspektionsgerät.

Unberechtigtes Auslesen der Chipinhalte

Die Überprüfung der im Reisepass optisch lesbaren Daten (Identitätsdaten, Passbild und maschinenlesbare Zeilen) und der im Chip gespeicherten Daten ist die Basisfunktionalität eines interoperablen Reisedokuments: Jeder Grenzbeamte muss in der Lage sein, diese Daten für die Verifikation der Identität eines Passinhabers zu nutzen. Gleichzeitig ist sicher zu stellen, dass der Zugriff auf die maschinenlesbaren und chipbasierten Daten nicht ohne Einwilligung des Passinhabers (willentlicher Akt des autorisierten Auslesens), z.B. wenn das Dokument geschlossen in Taschen verwahrt wird, möglich ist.

Diese beiden Grundannahmen liegen den Schutzmechanismen der BAC und der EAC zugrunde. Die Korrektheit und Robustheit der Implementierung der beschriebenen Schutzvorkehrungen auf dem ePass wurde im Rahmen aufwendiger Testverfahren durch unabhängige Testlabore untersucht und abschließend durch das BSI bestätigt.

Welche Schritte müsste nun ein Angreifer unternehmen, der NICHT im Besitz der optisch lesbaren Informationen ist und der trotzdem Zugriff auf die digitalen Daten eines Reisepasses erlangen möchte, der z.B. geschlossen in einer Manteltasche mitgeführt wird?

Zunächst einmal müsste sich der Angreifer dem ePass bis auf wenige Zentimeter nähern, da es erst in einem solchen Abstand möglich wird, eine Kommunikation mit dem Chip aufzunehmen. Die Gesetze der Elektrodynamik erzwingen, dass der Chip eines ePasses mit seiner eher kleinen Antenne und geringen Leistungsaufnahme realistischerweise nur über Distanzen unterhalb von etwa 25 cm fehlerfrei aktiviert und per Kommunikation angesprochen werden kann. Beim Überbrücken größerer Entfernungen steigt die benötigte Leistung exponentiell an. Gleichzeitig steigt mit dem Abstand zwischen Pass und Lesegerät durch das vorhandene Grundrauschen auch die Fehlerrate, die zu Bitfehlern in der Übertragung und damit zu falschen Daten beim Lesegerät führt.

Nehmen wir einmal an, dass dem Angreifer eine solche Kontaktaufnahme trotz der beschriebenen Schwierigkeiten unbemerkt gelungen wäre. Verfügt der Angreifer nicht über die auf der Datenseite im Pass aufgedruckten Daten, so bleibt ihm nichts anderes übrig, als sämtliche mögliche Schlüsselvarianten zu testen. Dies kann geschehen, indem der Angreifer hypothetische Daten annimmt, aus diesen den BAC-spezifischen Schlüssel generiert und dann das Basic Access-Protokoll

durchführt. Akzeptiert der ePass den erzeugten Schlüssel, so hat der Angreifer die richtigen Daten erraten und damit Zugriff auf das digitale Lichtbild erlangt.

Entscheidend für die Bewertung des Sicherheitsniveaus und damit der Eignung des Verfahrens ist also die Abschätzung, wie lange ein Angreifer benötigt, um den korrekten Schlüssel zu erraten. Die Anzahl der benötigten Versuche hängt maßgeblich von der Anzahl der insgesamt möglichen Schlüsselvarianten ab. Selbst wenn eine benötigte Teilinformation erfolgreich vermutet wurde oder bereits bekannt ist, werden gemäß aktueller Analysen des BSI etwa 12 Tage benötigt, um „nur" sechs Ziffern des benötigten Schlüssels zu erraten.

Für die praktische Durchführung des Angriffs ist die physikalische Präsenz des Passes in der Nähe des möglicherweise getarnten Lesegeräts erforderlich. Ein Auslesen digitaler Daten „im Vorübergehen" ist also nicht realistisch. Der entscheidend limitierende Faktor ist der Chip im ePass selbst. Ein einzelner Zugriffsversuch auf einen ePass unter Verwendung des BAC-Mechanismusses dauert ca. 1 Sekunde. Ein Angreifer könnte auch bei Einsatz von Hochleistungsrechnern im Hintergrund den Angriffsprozess nicht beschleunigen, denn nur der ePass selbst kann durch seine Antwort die Korrektheit der vom Angreifer gemachten Hypothesen bestätigen.

Sind einem Angreifer mehr Informationen bekannt, liegt ihm wahrscheinlich die Datenseite des betreffenden Passbuchs bereits in Kopie vor. Der Zugewinn an Information durch Auslesen des Chips ist daher eher gering. Selbst ein hochwertiges Foto der Zielperson lässt sich über größere Entfernung ohne Risiko auf technisch weniger aufwendigem Wege, beispielsweise unter Verwendung einer Kamera, erhalten.

Bei dem gezeigten Vorgehen sprechen wir ausschließlich von den durch BAC geschützten Daten, die ohnehin auf der Passkarte sichtbar verzeichnet sind. Wollte ein Angreifer auch Zugriff auf die über EAC gesicherten Fingerabdruckdaten erlangen, müsste er nicht nur den BAC-Mechanismus überwinden, sondern zusätzlich die Authentizität und Autorisierung im Rahmen des EAC-Protokolls nachweisen.

Die asymmetrischen Schlüsselpaare werden jedoch ausschließlich von autorisierten Instanzen, wie der Country Verifying Certification Authority (CVCA) und der nachgelagerten Document Verifying Certification Authority (DVCA), in Form eines Zertifikats ausgegeben und digital signiert. Insofern müsste die gesamte Hochsicherheitsumgebung der High Security Module (HSM) ausgehebelt werden, was aus sicherheitstechnologischer Sicht im Rahmen der derzeitigen PKI-Infrastrukturen ausgeschlossen werden kann.

Änderung der im ePass gespeicherten digitalen Daten

Werden optisch lesbare Passdaten verändert, müssten auch die im Chip gespeicherten Daten verändert werden, da eine Abweichung zwischen optischen und digitalen Daten keiner Überprüfung Stand halten würde.

Nach den Vorgaben der ICAO und der EU ist die auf dem Chip verfügbare digitale Reisepassapplikation so gestaltet, dass im Wirkbetrieb des Passes nur der lesende Zugriff möglich ist. Die Schreibmechanismen, mit deren Hilfe die Daten bei der Personalisierung in den Chip eingebracht werden, stehen aufgrund der Konfiguration der Applikation nach der Ausgabe des Dokuments nicht mehr zur Verfügung.

Darüber hinaus verfügen auch die im ePass eingesetzten Chipkomponenten selbst über generische Sicherheitsmechanismen, die sowohl die Vertraulichkeit und Integrität der gespeicherten Daten auf Hardwareebene als auch das Erkennen äußerer Manipulationen automatisch sicherstellen. Die Wirksamkeit dieser Mechanismen wird im Rahmen regelmäßiger Evaluierungs- und Zertifizierungsverfahren überprüft und bestätigt. Damit wird sowohl auf Applikationsebene als auch schon auf Hardwareebene eine Manipulation der digitalen Daten verhindert.

Zusätzlich sind alle gespeicherten Daten über digitale Signaturen abgesichert. Die Schlüssellängen der autorisierten Document Signer wurden derart groß dimensioniert, dass ein Erraten der notwendigen privaten Schlüssel selbst bei Verwendung aller weltweit verfügbaren Rechenkapazitäten nicht umsetzbar wäre.

„Klonen" der im Chip gespeicherten Daten

Unter „Klonen" wird das Übertragen der ausgelesenen Daten eines ePasses auf einen anderen Chip verstanden. Dazu ist festzustellen:

1. Die Daten können, wie oben dargestellt, nicht unberechtigt ausgelesen werden,
2. Eine Änderung/Verfälschung der Daten im Chip ist nicht möglich,
3. Chips der zweiten ePass-Generation sind grundsätzlich nicht „klonbar", da selbst bei Verwendung eines hoheitlich autorisierten Lesegerätes die im Chip verwendeten privaten Schlüssel nicht preisgegeben werden.

Mitschneiden der kontaktlosen Kommunikation

Das BAC-Protokoll erzwingt die Verschlüsselung der ausgetauschten Informationen mittels Secure Messaging, also der Absicherung der Vertraulichkeit und der Integrität der ausgetauschten digitalen Informationen unter Verwendung von sitzungsspezifischen symmetrischen Schlüsseln auf Basis des Triple-DES-Verfahrens. Mit Zunahme der Entfernung zwischen dem Leseterminal und dem Aufnahmegerät nimmt das ausgestrahlte Signal stark ab und die Fehlerrate steigt. Daher ist ein Mitschneiden der kontaktlosen Kommunikation aus praktischen Erwägungen nahezu unmöglich.

Ein versuchter Zugriff auf möglicherweise aufgezeichnete Informationen erfordert zudem eine erfolgreiche Entschlüsselung der gewonnenen Daten.

Erstellen von Bewegungsprofilen

Grundsätzlich stellt ein Chip, der im kontaktlosen Modus betrieben wird, Informationen auf unterschiedlichen Abstraktionsebenen zur Verfügung. Diese Informationen werden benötigt, um das kontaktlose Protokoll nach den Vorgaben der ISO Norm 14443 zu etablieren.

Ein ePass, der wie der deutsche ePass nach dem Protection Profile „MRTDs with BAC Application" zertifiziert wurde, erzeugt bei jedem neuen Zugriff zwingend einen sitzungsabhängig wechselnden, zufällig erzeugten Identifier. Im Gegensatz zu einem Mobiltelefon, das immer den gleichen Identifier sendet und damit Bewegungsprofile ermöglicht, ist dies bei einem ePass also nicht möglich.

Angreifern, die an präzisen Bewegungsprofilen bestimmter Zielpersonen interessiert sind, stehen sehr viel einfachere Methoden (z.B. die Benutzung von Datenaufzeichnungen der Mobilfunkanbieter) als der Umweg über den hochgradig geschützten ePass zur Verfügung. Damit ist ein derartiger Angriffsversuch ebenso sinnlos wie er in der praktischen Umsetzung am notwendigen Aufwand zur Überwindung der Sicherheitsmaßnahmen des Chips scheitern würde.◀

5. FAZIT

▶ Persönliche Daten und Informationen sicher zu bewahren und jederzeit verfügbar zu haben, gehört zu den Grundbedürfnissen des modernen Menschen. Reisen, internationaler Austausch und die Möglichkeit, sich überall auf der Welt sicher und frei bewegen zu können, sind Forderungen, die im Zuge der fortschreitenden Globalisierung auch im internationalen Grenzverkehr neue technische Sicherheitslösungen erforderlich gemacht haben. Schon längst reicht das einfache Ausweis-„Papier" nicht mehr aus, um nationalen und internationalen Sicherheitsstandards gerecht zu werden. Zahlreiche hochkomplexe Sicherungssysteme sind notwendig, um die datentechnische Identität des Individuums zu schützen und eine verlässliche Verbindung zwischen Dokumenteninhaber und ID-Dokument herstellen zu können.

Mit der Einführung des ePasses der zweiten Generation am 1. November 2007 wird Deutschland als einer der ersten Staaten weltweit für seine Bürger eine neue Dimension an Identitätssicherheit erreichen. Dass dieser neue Meilenstein von der Öffentlichkeit überaus sorgfältig und kritisch beobachtet und hinterfragt wird, ist im Sinne eines verlässlichen Datenschutzes notwendig und richtig.

Die vergangenen zwei Jahre seit Beginn der ersten Phase zur Einführung biometriegestützter, elektronischer Identitätsdokumente wurde aus sicherheitstechnologischer und datenschutzrechtlicher Sicht intensiv genutzt. Die bestehenden Infrastrukturen, die Sicherungs- und Schutzmechanismen sowie die Verfahren zur Abwehr möglicher Angriffe konnten nochmals deutlich optimiert werden. Damit kann für deutsche Dokumenteninhaber das derzeit höchste denkbare Niveau an Identitätsschutz und Dokumentensicherheit gewährleistet werden.

Mit der neuen ePass-Technologie wurde ein gewaltiger Sicherheitsvorsprung erreicht. Ihn zu halten und weiter auszubauen, ist eine Herausforderung.

Sachliche, offene und kritische Dialoge werden auch zukünftig dazu beitragen, dass wir dem gemeinsamen Ziel, die Identität jedes Bürgers über verlässliche ID-Prozesse und -Systeme sicher zu bewahren und zu schützen, heute und in der Zukunft gerecht werden. ◀

– ANHANG –

DIE WESENTLICHEN INFORMATIONEN IN DER ÜBERSICHT

Im Folgenden sind einige wesentliche Informationen bzw. Fragen zum ePass in Kurzform zusammengestellt.

A AUF EINEN BLICK

Der neue ePass der zweiten Generation...

- wird ab dem 1. November 2007 in Deutschland ausgegeben,
- speichert im integrierten Chip die personenbezogenen Daten sowie ein digitalisiertes Gesichtsbild und zwei Fingerabdrücke des Dokumenteninhabers,
- hat für Bürger ab 24 Jahren eine Gültigkeit von 10 Jahren, für Kinder und Bürger unter 24 Jahren eine Gültigkeit von 6 Jahren,
- kostet bei einer Gültigkeit von 10 Jahren € 59,00, bei einer Gültigkeit von 6 Jahren € 37,50.

Die Aufnahme und Bewertung von Gesichtsbildern...

- wird über eine von der Bundesdruckerei bereit gestellte Qualitätssicherungs-Software (QS) sowie eine aktualisierte Foto-Mustertafel und eine neue Passbild-Schablone unterstützt.
- Die Entscheidung, ob ein Passbild biometrietauglich ist, obliegt ausschließlich dem zuständigen Sachbearbeiter der Passbehörde.
- Die Erfassung der digitalen Daten des Gesichtsbildes erfolgt in den Schritten:
  1. Visuelle Prüfung des Passbildes (Foto-Mustertafel und Passbild-Schablone)
  2. Einscannen des Passbildes (Qualitätscheck durch die QS-Software)
  3. Speichern der Daten im digitalen Antragssatz.

Die Aufnahme und Bewertung von Fingerabdrücken....

- wird über die von der Bundesdruckerei bereit gestellte neue Biometrie-Software gesteuert und unterstützt.
- Es werden Fingerabdrücke von zwei verschiedenen Fingern verwendet.
- Die bereit gestellte Software unterstützt bei der Einhaltung der geforderten Aufnahmereihenfolge sowie bei der Ermittlung der qualitativ besten Fingerabdrücke.
- Die Erfassung der digitalen Daten der Fingerabdrücke erfolgt in den Schritten:
  1. Finger auflegen
  2. Prüfung der Qualität
  3. Auswahl des qualitativ besten Fingerabdrucks
  4. Aufnahmevorgang abschließen
  5. Den Vorgang zur Speicherung eines zweiten Fingerabdrucks wiederholen

Datenschutz und Datensicherheit...

- wird über die Sicherheitsverfahren Basis Access Control (BAC) und Extended Access Control (EAC) sowie über Public Key-Infrastrukturen (PKI) sichergestellt.
- Eine zentrale Datenbank mit biometrischen Daten existiert in Deutschland nicht.
- Die Fingerabdrücke sind ausschließlich im Chip des ePasses gespeichert.
- Der Inhalt des ePass-Chips kann vom Passinhaber am ePass-Leser der Passbehörde überprüft werden.
- Die persönlichen Daten der Passantragsteller werden nach Ende des Produktionsverfahrens in der Bundesdruckerei gelöscht.
- Die in der Meldebehörde aufgenommenen Fingerabdrücke werden nach Ausgabe des ePasses gelöscht.

B ANTWORTEN AUF HÄUFIG GESTELLTE FRAGEN

1.) Erhöht der Chip die Fälschungssicherheit des Passes?

► Der Chip ergänzt die bereits vor Einführung elektronischer Komponenten vorhandene Fälschungssicherheit deutscher Reisedokumente. Auf ihm wurden in Phase 1 die in den Pass gedruckten Personendaten und das Lichtbild zusätzlich elektronisch gespeichert. In Phase 2 kommen ab dem 01. November 2007 noch die Bilder von zwei Fingerabdrücken hinzu. Damit wird die Bindung von Dokument und Dokumenteninhaber deutlich erhöht. Gleichzeitig wäre ein enormer Aufwand nötig, um – wenn überhaupt möglich – eine Totalfälschung von ePässen herzustellen. Der neue ePass behält auch dann seine Gültigkeit, wenn der Chip zerstört oder das Auslesen der gespeicherten Daten nicht möglich ist. ◄

2.) Welche persönlichen Daten sind auf Chip des ePasses gespeichert?

► Heute sind auf dem Chip exakt die persönlichen Daten des Passinhabers gespeichert, die auch auf dem Pass aufgedruckt sind. Dazu gehört auch das Foto.◄

3.) Werden in Zukunft weitere Daten im Chip gespeichert?

► Die nächste Generation des elektronischen Reisepasses, die ab dem 1. November 2007 ausgegeben wird, speichert auch zwei Fingerabdrücke des Passinhabers auf dem integrierten Chip. ◄

4.) Unterliegen die Fingerabdrücke in den zukünftigen Pässen einem besonderen Schutz?

► Ja. Zum Schutz der Fingerabdrücke ist deren Speicherung auf dem Chip des Passes nur dann erlaubt, wenn der entsprechende Passtyp über einen erhöhten Schutz durch erweiterte Verschlüsselungsmechanismen verfügt. Das Lesegerät muss sich gegenüber dem Chip bei jedem Auslesen als rechtmäßig ausweisen, was mit einem Schlüsselsystem erreicht wird. Außerdem bestimmt ausschließlich das Land, das den Reisepass ausgibt, auf welche Daten ein ausländisches Lesegerät zugreifen darf. Auch dies kann mit der Ausgabe (oder Nichtausgabe) von Schlüsseln an die einzelnen Länder gesteuert werden. ◄

5.) Warum werden in Zukunft auch Fingerabdrücke im Reisepass gespeichert?

► Bereits am 13. Dezember 2004 reagierte die Europäische Union mit der Richtlinie 2252/2004 auf die internationale Sicherheitslage und beschloss verpflichtend für alle EU-Mitgliedsstaaten die Einführung elektronischer Reisepässe mit biometrischen Merkmalen.

In der EU-Richtlinie sind die Standards und technischen Spezifikationen für Material und Drucktechniken sowie für die erforderlichen biometrischen Daten des neuen ePasses festgelegt. Mit einem digitalisierten Bild als Pflichtkriterium legt sie die Gesichtsbiometrie als Standardtechnologie für europäische Reisedokumente fest und definiert Fingerabdrücke als weiteres, in einer zweiten Phase zu integrierendes biometrisches Standardmerkmal. ◄

6.) Kann man die im Reisepass verwendeten Chips im „Laden" kaufen?

► Nein, denn bei den im Reisepass verwendeten Chips handelt es sich nicht um so genannte RFID-Tags, wie sie für die Kennzeichnung von Waren verwendet werden, sondern um Sicherheits-Prozessorchips. Im Gegensatz zu den RFID-Tags sind die Chips, die in den Pässen eingesetzt werden, nicht frei verfügbar, sondern werden in einer gesicherten Umgebung entwickelt, hergestellt, gelagert und in die Pässe eingebracht. Die Sicherheitsmaßnahmen sind ebenso wie der Angriffsschutz der Chips selbst Gegenstand strengster Sicherheitsvorkehrungen und verlangen komplexe elektronische Zertifizierungsprozesse. ◄

7.) Was ist der Unterschied zwischen „RFID-Tags" und den in den Pässen eingesetzten Sicherheits-Chips?

▶ Im elektronischen Reisepass werden Sicherheits-Prozessorchips eingesetzt, die praktisch einen Computer im Miniformat darstellen. Sie beinhalten im Gegensatz zu RFID-Tags für die Warenkennzeichnung einen eigenen Prozessor, verwalten Zugriffsrechte und haben eingebaute Schutzmechanismen gegen Angriffe. ◀

8.) Wie wird die Sicherheit des Chips getestet?

▶ Für die elektronischen Reisepässe werden nur Sicherheits-Chips eingesetzt, die die derzeit international höchste erreichbare Sicherheitsstufe „Common Criteria EAL5+" erreicht haben. Diese Sicherheitsstufe wird nach intensiven Angriffstests, die von zugelassenen Sicherheitslaboren ausgeführt werden müssen, vom Bundesamt für Sicherheit in der Informationstechnik (BSI) durch ein entsprechendes Zertifikat bestätigt. ◀

9.) Strahlt der ePass eigenständig Funkwellen aus?

▶ Nein. Der Chip im Reisepass braucht Strom, um zu funktionieren. Da der Pass über keine eigene Stromquelle verfügt, muss ihm Energie aus Funkwellen aus dem Lesegerät zugeführt werden. Er sendet selbst aber keine Funkwellen aus. Befindet sich der Chip nicht im Bereich eines Lesegeräts, ist er somit auch nicht aktiv und kann auch keine Daten ausgeben. ◀

10.) Der elektronische Reisepass überträgt Daten per Funkwellen. Kann man die Funkwellen abhören?

▶ Funkwellen lassen sich prinzipiell immer mit entsprechenden Empfängern aufnehmen. Mit größerem Abstand werden die energiearmen Funkwellen jedoch schwächer, so dass man je nach Entfernung sehr aufwändige Methoden benötigt, um die Funkwellen aufzufangen. Bei elektronischen Reisedokumenten wird davon ausgegangen, dass mindestens einige Meter Abstand überbrückt werden müssen. Da eine generelle Gefahr des Abhörens von Funkwellen bekannt ist, wird die Datenübertragung durch zusätzliche Maßnahmen geschützt. Zu diesen Maßnahmen gehören im Wesentlichen der Einsatz von Verschlüsselungstechniken und die gegenseitige Autorisierung von Chip und Lesegerät. ◀

11.) Sollte man einen Reisepass in einer Schutzhülle gegen Funkwellen aufbewahren?

▶ Angeregt durch die öffentlichen Diskussionen, bieten Händler bereits Schutzhüllen aus besonderen Metallen an, die ein unerlaubtes Auslesen des Passes verhindern sollen. Die Schutzhüllen schirmen die Funkwellen größtenteils ab. Diese Maßnahme macht allerdings wenig Sinn, da der Chip nur dann ein Auslesen erlaubt, wenn er mit dem korrekten BAC-Schlüssel „aufgeschlossen" wird. Für dessen Berechnung müssen aber die in der MRZ stehenden personenbezogenen Daten schon bekannt sein. ◀

12.) Benötigt man zum Auslesen des Chips teure Spezialgeräte?

▶ Die Chips verwenden Methoden der Funkübertragung, die aus dem Bereich der Chipkarten-Technik bereits bekannt sind. Deshalb sind zum Auslesen aus technischer Sicht keine teuren Spezialgeräte nötig. Dies stellt jedoch keine Bedrohung dar. Entscheidend für die Sicherheit ist, ob der Chip es erlaubt, dass Daten ausgelesen werden dürfen, d.h. die Daten „preisgibt". Dies ist nur der Fall, wenn vorher eine gegenseitige Überprüfung erfolgt ist und somit der Chip die Anfrage nach Daten freigibt. Dies geschieht nur, wenn entsprechende Schlüssel bekannt sind bzw. automatisch generiert werden können. ◀

13.) Muss der Reisepass zum Auslesen des Chips geöffnet sein?

► Grundsätzlich muss der ePass zum Zugriff auf die gespeicherten Daten geöffnet sein und die Informationen aus der maschinenlesbaren Zone (MRZ) der Datenseite müssen optisch ausgelesen werden können. Zu diesen Daten gehören die Passnummer, das Geburtsdatum des Inhabers und das Gültigkeitsdatum des Passes. Aus diesen Daten wird vom Lesegerät ein Schlüssel generiert, der vom Chip verifiziert werden muss, bevor die Daten zum Auslesen bereitgestellt werden. ◄

14.) Kann ein Angreifer die zum Auslesen benötigten MRZ-Daten auch „erraten"?

► Interessiert sich ein Angreifer nur für die MRZ-Daten einer ganz bestimmten Person und besitzt er bereits weitgehende Informationen über diese Person, so kann er versuchen, den Rest der benötigten MRZ-Daten zu „erraten". Solche Ratevorgänge benötigen jedoch viel Zeit, so dass ein Auslesen „im Vorübergehen" unwahrscheinlich ist. Kürzlich wurde über einen solchen Angriffstest berichtet: Hier wurden mehrere zehntausend Versuche benötigt, bevor die MRZ-Daten „erraten" werden konnten. ◄

15.) Sind die Daten auf dem Chip mit den Passdaten verbunden? Kann man den Chip mit dem eines anderen Passes austauschen?

► Die Daten auf dem Chip sind die gleichen, die auch auf der Passkarte aufgedruckt sind. Wird ein Chip in einen anderen Pass eingesetzt, so passen die Daten des Chips und die Daten auf dem Pass nicht zusammen. Die Fälschung wird also entdeckt werden. ◄

16.) Könnte man mit einem kopierten Chip einen gefälschten Reisepass herstellen?

► Neben einer genauen Kopie des Chips eines Reisepasses müsste man auch das Passdokument selbst duplizieren, um eine Übereinstimmung der Daten zwischen Chip und Passdokument zu erreichen. Dieses Duplikat müsste natürlich alle Sicherheitsmerkmale aufweisen, damit das Dokument an der Grenze anerkannt wird. Da der im Chip gespeicherte Datensatz mit einer elektronischen Signatur gegen Veränderung geschützt ist, kann dieser Chip nicht für eine auf eine andere Person lautende Passfälschung verwendet werden. Eine typische Passfälschung, bei dem das aufgedruckte Foto und die personenbezogenen Daten zum illegalen Nutzer passen müssen, ist auf diese Weise also nicht herstellbar. ◄

17.) Kommt man allein mit einem Chip durch die Grenzkontrolle?

► Nein, der Chip muss Teil des gültigen Passdokuments selbst sein. ◄

18.) Kann man per Funk die Daten auf dem Reisepass verändern?

► Nein. Der Chip im elektronischen Reisepass wird einmalig bei der Herstellung des Passes mit Daten beschrieben. Danach wird durch den Chip selbst verhindert, dass Daten in seinem Speicher verändert werden. Hierfür sind im Chip Schutzvorrichtungen eingebaut, die im Rahmen der Sicherheits-Zertifizierung der Chips untersucht und hierbei sogar spezifischen Angriffsversuchen ausgesetzt werden. ◄

19.) Kann man die Übertragung der Daten zwischen Reisepass und Lesegerät stören?

► Das Stören einer Funkübertragung ist prinzipiell immer möglich. Im Fall der elektronischen Reisedokumente wird hierfür allerdings eine sehr hohe Stärke des Störsenders benötigt. Ein solcher Störsender müsste daher in direkter Nähe

des Lesegerätes aufgestellt werden, was z. B. im Bereich eines Flughafens sofort auffallen würde. Das Erkennen und Auffinden eines Störsenders ist technisch sehr leicht möglich. ◀

20.) Lässt sich der Chip im Reisepass zerstören?

▶ Der Chip befindet sich in einem so genannten „Inlay" im Reisepass, das ihn bestmöglich gegen äußere Einflüsse schützt. Ein völliger Schutz, insbesondere gegen mutwillige Beschädigung, z. B. mit Werkzeugen, kann allerdings nicht erreicht werden. Auch bei herkömmlichen Reisepässen und anderen Dokumenten ist mutwillige Beschädigung möglich, wenn etwa versucht wird, die Qualität des aufgedruckten Fotos absichtlich zu verschlechtern. ◀

21.) Was passiert, wenn der Chip im Reisepass zerstört wird?

▶ Wird der Chip im Reisepass zerstört, so behält das Dokument trotzdem seine Gültigkeit. Dies ist möglich, da die verbleibenden Sicherheitsmerkmale nach wie vor ausreichende Möglichkeiten der Echtheitsüberprüfung erlauben. Der Vorteil der vereinfachten Grenzkontrolle fällt allerdings weg. Wird der Chip also zerstört, muss die Identität des Passinhabers während der Grenzkontrolle durch die Beamten ohne technische Hilfe festgestellt werden. ◀

22.) Wie kann der Passinhaber überprüfen, welche Daten auf seinem ePass gespeichert sind?

▶ Alle Passbehörden sind mit ePass-Lesegeräten ausgestattet. Damit kann jeder Bürger seine auf dem Chip gespeicherten persönlichen Daten einsehen. ◀

23.) Bleiben alte Pässe gültig?

▶ Alle vor dem 01.11.2005 beantragten Pässe ohne Chip behalten ihre reguläre Gültigkeit. Das gilt auch für die vor dem 01.11.2007 ausgestellten Pässe, die nur das Foto, aber keine Fingerabdrücke im Chip enthalten. In einer Übergangszeit wird es also alte und neue Pässe parallel geben. ◀

24.) Werden im Umlauf befindliche ePässe mit digitalen Fingerabdrücken „nachgeladen"?

▶ Nein. Die auf dem Chip gespeicherten Daten werden direkt bei der Passpersonalisierung durch die Bundesdruckerei elektronisch signiert und der Chip wird nach der Personalisierung gegen Löschen oder Ändern der Daten verriegelt. Ein „Nachladen" ist also nicht möglich. ◀

Weitere aktuelle Informationen und Antworten auf Fragen zum ePass können über die Website des Bundesministeriums des Innern unter www.ePass.de abgerufen werden.

C GLOSSAR

BAC Basic Access Control, Zugriffsschutz auf die im ePass gespeicherten Daten

CSCA Country Signing Certification Authority, oberste Instanz einer Public Key Infrastruktur bei der Personalisierung und Verifikation von ePässen

CVCA Country Verifying Certification Authority, oberste Instanz einer Public Key Infrastruktur bei der Durchführung der Extended Access Control

DES Data Encryption Standard, symmetrischer Verschlüsselungsalgorithmus

DVCA Document Verifying Certification Authority, Instanz zur Weiterleitung von Zugriffsberechtigungen an Lesegeräte, die auf die Fingerabdrücke im ePass zugreifen dürfen

DG Datengruppe. Die Logical Data Structure (LDS) wird in Datengruppen unterteilt. Darin befinden sich bspw. Fingerabdrücke oder das Gesichtsbild

EAC Extended Access Control, erweiterter Zugriffsschutz auf die im ePass gespeicherten Fingerabdrücke

HSM Hardware Security Module (Hardware-Sicherheitsmodul), Computerkomponenten zur Speicherung von Daten und zur Generierung von Schlüsseln

ICAO International Civil Aviation Organization, Internationale Zivile Luftfahrtorganisation

IS Inspection System ("Lesegerät"), Dokumentenlese- und Prüfgeräte, bspw. in Meldestellen oder bei Grenzkontrollen

ISO International Standards Organization, oberste internationale Organisation zur Definition von Normen

Inlay Ein Verbund von Chipmodul, Antenne und Trägermaterial, der als Bestandteil zur Fertigung von intelligenten Dokumenten, (z.B. Smartcards, ePassbücher) verwendet wird.

LDS Logical Data Structure, Standard in welcher Art und Weise die Daten im Chip eines ePasses gespeichert werden.

MRP Machine Readable Passport (Maschinenlesbarer Reisepass)

MRZ Machine Readable Zone, Maschinenlesbare Zeilen auf einem ePass zum Auslesen mittels optischer Schrifterkennung

MRTD Maschine Readable Travel Document (Maschinenlesbares Reisedokument)

PKI Public Key Infrastructure, technische Infrastruktur zur Verteilung von Schlüsseln und Zertifikaten.

RFID Radio Frequency Identification, Verfahren zur automatischen berührungslosen Identifizierung von Gegenständen und Lebewesen

Triple-DES, 3DES Dreimaliges Ausführen von DES nacheinander unter Verwendung unterschiedlicher Schlüssel

KONTAKT

Bundesdruckerei GmbH · Oranienstraße 91 · D-10969 Berlin
Tel +49 (0) 30 - 25 98-0 · Fax +49 (0) 30 - 25 98-22 05
E-Mail Info@bdr.de · www.bundesdruckerei.de

IMPRESSUM:

Herausgeber *Bundesdruckerei GmbH, Oranienstraße 91, 10969 Berlin, www.bundesdruckerei.de*