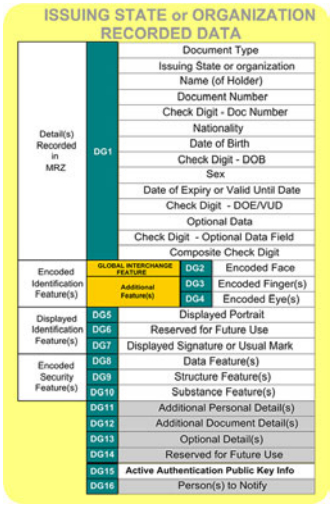
Bundesamt
für Sicherheit in der
Informationstechnik

Digitale Sicherheitsmerkmale im elektronischen Reisepass



Der neue elektronische Reisepass wird mit einem Radio-Frequency (RF)-Chip ausgestattet sein. Bei diesem RF-Chip handelt es sich um einen zertifizierten Sicherheitschip mit kryptographischem Koprozessor, auf dem neben den bisher üblichen Passdaten auch biometrische Merkmale gespeichert werden. Die Integration von biometrischen Merkmalen dient dem Ziel, eine stärkere Bindung zwischen Person und Reisedokument herzustellen.

Die grundlegenden technischen Spezifikationen für den RF-Chip im Reisepass wurden von der International Civil Aviation Organization (ICAO) – einer Unterorganisation der Vereinten Nationen – standardisiert. Ein wesentlicher Bestandteil davon ist die Organisation der Daten auf dem Chip, so sind die auf dem RF-Chip gespeicherten Daten in Datengruppen organisiert, wie in der nebenstehenden Abbildung skizziert. Nur die Datengruppen 1 (MRZ) und 2 (Gesichtsbild) sind verpflichtend, alle weiteren Datengruppen können optional verwendet werden. Der EU-Reisepass wird von diesen optionalen Datengruppen erst in der zweiten Ausbaustufe zusätzlich die Datengruppe 3 (Fingerabdrücke) verwenden.

Nach dem Einbringen der Daten während der Produktion des Reisepasses, sind diese gegen unberechtigtes Auslesen und Verändern geschützt. Im folgenden wird beschrieben, wie die Integrität und die Authentizität sowie die Vertraulichkeit der in diesen Datengruppen gespeicherten Daten gesichert wird.

Digitale Signaturen

Die Integrität und die Authentizität der im RF-Chip gespeicherten Daten wird über eine digitale Signatur gesichert, so dass jede Form von unechten beziehungsweise manipulierten Daten zu erkennen sind. Somit kann überprüft werden, dass die signierten Daten von einer berechtigten Stelle erzeugt und seit der Erzeugung nicht mehr verändert wurden.

Durch die Integration dieser digitalen Signatur über alle relevanten Passdaten, wird die Fälschungssicherheit des Reisespasses auf ein qualitativ neues Niveau gehoben.

Zum Signieren und Überprüfen der digitalen Dokumente wird eine global interoperable Public Key Infrastruktur (PKI) benötigt. Jedes teilnehmende Land erzeugt dazu eine zweistufige PKI, die aus genau einer *Country Signing CA* (CA – Certification Authority) und mindestens einem

Document Signer besteht:

- **Country Signing CA:** Die Country Signing CA ist im Kontext der Reisepässe die oberste Zertifizierungsstelle eines Landes. International gibt es keine übergeordnete Zertifizierungsstelle, da nur so garantiert werden kann, dass jedes Land die volle Kontrolle über seine eigenen Schlüssel besitzt. Das von der Country Signing CA erzeugte Schlüsselpaar wird ausschließlich zur Zertifizierung von Document Signern verwendet. Die Verwendungsdauer des privaten Schlüssels der Country Signing CA wurde auf drei bis fünf Jahre festgelegt. Entsprechend der Gültigkeitsdauer der Reisepässe von derzeit zehn Jahren muss der zugehörige öffentliche Schlüssel zwischen 13 und 15 Jahren gültig sein.
- **Document Signer:** Document Signer sind zum Signieren der digitalen Dokumente berechtigte Stellen, zum Beispiel die Druckereien, die auch die physikalischen Dokumente produzieren. Jeder Document Signer besitzt mindestens ein von ihm erzeugtes Schlüsselpaar. Der private Schlüssel wird ausschließlich zum Signieren der digitalen Dokumente verwendet, der öffentliche Schlüssel muss von der nationalen Country Signing CA zertifiziert werden.
  Die Verwendungsdauer des privaten Schlüssels des Document Signers beträgt maximal drei Monate, so dass im Falle einer Kompromittierung des Schlüssels möglichst wenig Pässe von den Auswirkungen betroffen sind. Entsprechend muss der zugehörige öffentliche Schlüssel zehn Jahre und 3 Monate gültig sein.

Aufgrund der relativ langen Gültigkeit müssen entsprechend starke Schlüssel verwendet werden. Als Signaturverfahren sind RSA (benannt nach seinen Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman), DSA (Digital Signature Algorithm) und ECDSA (Elliptic Curve Digital Signature Algorithm) zugelassen, der deutsche Reisepass wird ECDSA verwenden. Die empfohlenen Schlüssellängen sind in der folgenden Tabelle dargestellt.

Algorithmus	***Country Signing CA [Bit]***	***Document Signer [Bit]***
RSA / DSA	3072	2048
ECDSA	256	224

Zugriffschutz

Die Mechanismen des Zugriffschutzes stellen sicher, dass ein unautorisiertes Auslesen der Daten aus dem RF-Chip sowie ein Belauschen der Kommunikation unterbunden werden.

Im RF-Chip werden in der ersten Stufe des EU-Reisepasses im wesentlichen folgende

personenbezogenen Daten gespeichert: der Name, der Geburtstag, das Geschlecht und das Gesichtsbild des Inhabers. Bereits jetzt sind alle diese Daten in maschinenlesbarer Form in der so genannten MRZ (Machine Readable Zone) auf der Datenseite des Reisepasses enthalten (mit Ausnahme des Gesichtsbilds, welches zwar auf der Datenseite abgedruckt, jedoch nur bedingt maschinenlesbar ist). Die auf der Datenseite "gespeicherten" Daten sind jedoch nur mit der Einwilligung des Passinhabers lesbar – nur wer auch tatsächlich Zugriff auf den Reisepass hat, kann auch den Inhalt der Datenseite lesen.

Solange der Reisepass geschlossen verwahrt wird, sind die darin enthaltenen Daten vor

unberechtigtem Zugriff geschützt. Im Rahmen einer Grenzkontrolle wird der Reisepass an einen

Beamten übergeben. Durch diese Übergabe willigt der Reisende indirekt in die Kontrolle ein und die im Reisepass enthaltenen Daten werden gelesen.

Basic Access Control

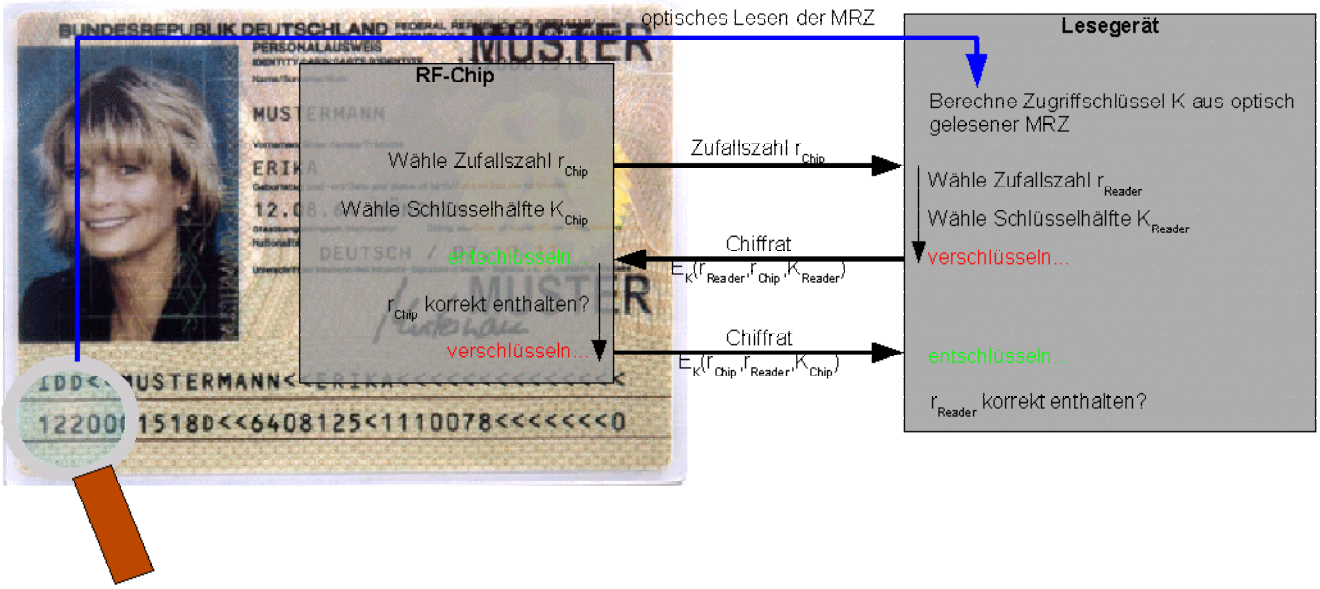
Dieser grundlegende Zugriffschutz soll für die im RF-Chip abgelegten Daten genau die Eigenschaften des bisherigen Reisepasses nachbilden: Um auf die im RF-Chip gespeicherten Daten zugreifen zu können, muss das Lesegerät auch tatsächlich optischen Zugriff auf die Datenseite des Reisepasses haben.

Technisch wird das dadurch umgesetzt, dass sich das Lesegerät gegenüber dem RF-Chip authentisieren muss. Für diese Authentisierung benötigt das Lesegerät einen geheimen Zugriffschlüssel, der sich aus der maschinenlesbaren Zone des Reisepasses berechnet. Das Lesegerät muss also die maschinenlesbare Zone erst optisch lesen, daraus den Zugriffschlüssel berechnen und kann sich dann erst gegenüber dem RF-Chip authentisieren.

In die Berechnung des Zugriffschlüssels gehen die durch Prüfziffern gegen Lesefehler gesicherten Felder der MRZ ein: die Passnummer, das Geburtsdatum des Inhabers und das Ablaufdatum des Reisepasses. Geht man vom derzeitigen Reisepass aus, ist die Passnummer eine neunstellige Zahl, das heißt, es gibt 10^9 Möglichkeiten. Für das Geburtsdatum gibt es näherungsweise $365 \cdot 10^2$ Möglichkeiten und für das Ablaufdatum gibt es – bei einer Gültigkeit des Reisepasses von zehnJahren – $365 \cdot 10$ Möglichkeiten. Insgesamt ist die Stärke des Zugriffschlüssels daher mit etwa 56 Bit ($365^2 \cdot 10^{12} \approx 2^{56}$) zu bewerten und entspricht somit der Stärke eines normalen DES-Schlüssels.

Um das unberechtigte Auslesen des Reisepasses zu verhindern, ist die Stärke des Mechanismus sicher ausreichend, da das Ausprobieren aller 2^{56} Schlüssel in kurzer Zeit unmöglich ist – selbst wenn der Angreifer Zusatzinformationen hat, wie Zusammenhänge zwischen Passnummer und Ablaufdatum.

Das folgende Bild gibt einen Überblick über die Realisierung von Basic Access Control.



Extended Access Control

In der zweiten Stufe des EU-Reisepasses ist geplant, zusätzlich Fingerabdrücke auf dem RF-Chip zu speichern. Derartig sensitive Daten bedürfen eines besonders starken Schutzes und vor allem der Vorgabe einer engen Zweckbindung. Innerhalb der Arbeitsgruppe zur technischen Standardisierung des EU-Reisepasses findet daher zur Zeit die Spezifikation eines erweiterten Zugriffschutzes statt.

Dieser erweiterte Zugriffschutz spezifiziert einen zusätzlichen Public-Key Authentisierungsmechanismus mit dem sich das Lesegerät als zum Lesen von Fingerabdrücken berechtigt ausweist. Dazu muss das Lesegerät mit einem eigenen Schlüsselpaar und einem vom RF-Chip verifizierbaren Zertifikat ausgestattet werden. In diesem Zertifikat sind dann die Rechte des Lesegeräts exakt festgelegt. **Dabei bestimmt immer das Land, das den Reisepass herausgegeben hat, auf welche Daten ein (ausländisches) Lesegerät zugreifen kann.**

Durch dieses Vorgehen ist sichergestellt, dass Lesegeräte nur auf die Daten zugreifen können, für die sie auch legitimiert wurden. Weiterhin sind selbst diese Lesegeräte nicht in der Lage, die Daten aus einem geschlossenen Reisepass auszulesen, da Basic Access Control weiterhin vom RF-Chip erzwungen wird.

Verschlüsselung

Grundsätzlich wird nach der erfolgreichen Durchführung von Basic Access Control die Kommunikation zwischen Lesegerät und RF-Chip mit 112-Bit-Triple-DES verschlüsselt und ist somit prinzipiell gegen unberechtigtes Abhören geschützt. Das Aushandeln des dynamischen Sitzungsschlüssels erfolgt bei der Durchführung von Basic Access Control. Dabei werden zwei Schlüsselhälften (K_{Reader} und K_{Chip}) jeweils mit dem Zugriffschlüssel verschlüsselt übertragen. Da die Stärke des Zugriffschlüssels mit etwa 56 Bit bewertet werden muss (s. Basic Access Control), ist es theoretisch möglich, eine vollständig abgehörte und aufgezeichnete Sitzung nachträglich zu entschlüsseln. Dazu muss zunächst der Zugriffschlüssel gebrochen werden, denn mit diesem werden die zwei Hälften des wesentlich stärkeren Sitzungsschlüssels verschlüsselt übertragen. Ein Brute-Force-Angriff (Ausprobieren aller möglichen Schlüssel) auf diesen Zugriffschlüssel benötigt jedoch viel Zeit oder ist entsprechend der verwendeten Hardware sehr teuer. Wenn man bedenkt, dass die durch Basic Access Control geschützten Daten relativ öffentlich sind und auf anderem Wege wesentlich einfacher gesammelt werden können, ist die Stärke der Verschlüsselung ausreichend.

Die zur Zeit auf EU-Ebene diskutierte BSI-Spezifikation von Extended Access Control zum Schutz von Fingerabdrücken sieht vor, nach einem erfolgreichen Durchlauf des Basic Access Controls einen neuen, stärkeren Sitzungsschlüssel auszutauschen, der über Public-Key Mechanismen (Diffie-Hellman Schlüsselvereinbarung) erzeugt wird. Die Verwendung dieses starken Sitzungsschlüssels ist zum Zugriff auf Fingerabdrücke verpflichtend und wird vom RF-Chip erzwungen, kann aber von jedem Lesegerät auch verwendet werden, um die weniger sensitiven Daten noch stärker zu schützen.

Dokumentenbindung

Durch die Integration von biometrischen Merkmalen in den RF-Chip wird die Bindung eines Reisedokumentes an den legitimen Inhaber gestärkt. Dies eröffnet für den Kontrollprozeß die Möglichkeit, mit Hilfe von Gesichtserkennungssystemen bzw. Fingerprintsystemen die Zugehörigkeit des Passes zur präsentierenden Person besser bewerten zu können.

Literatur

Eine ausführlichere Beschreibung der Sicherheitsmechanismen ist in folgendem Artikel zu finden: Risiko Reisepass – Schutz der biometrischen Daten im RF-Chip, c't Magazin 05/05, Heise Verlag 2005