DuD
Datenschutz und Datensicherheit

Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass

Ein Überblick über Sicherheitsmerkmale, Risiken und Gegenmaßnahmen

Dennis Kügler, Ingo Naumann

Dieser Artikel gibt einen Überblick über die Ziele und die Funktionsweise der Sicherheitsmechanismen, die im deutschen elektronischen Reisepass (ePass) zur Anwendung kommen. Dieses beinhaltet auch die erweiterten Sicherheitsmechanismen, welche in der zweiten Stufe elektronischer Reisepässe hinzukommen.

Dr. Dennis Kügler

Referent im Bundesamt für Sicherheit in der Informationstechnik

E-Mail: Dennis.Kuegler@bsi.bund.de

Dr. Ingo Naumann

Referent im Bundesamt für Sicherheit in der Informationstechnik

E-Mail: Ingo.Naumann@bsi.bund.de

Einleitung

Der elektronische Reisepass ist mit einem kontaktlosen Chip (Radio-Frequency- oder RF-Chip) ausgestattet. Bei diesem Chip handelt es sich um einen zertifizierten Sicherheitschip [3] [4] mit kryptographischem Koprozessor, auf dem neben den bisher üblichen Passdaten auch biometrische Merkmale gespeichert werden können.

> Die Verwendung von elektronischen Komponenten in Reisedokumenten dient zwei Zielen: die Fälschungssicherheit zu erhöhen sowie den Mißbrauch durch ähnliche Personen zu verhindern.

Die grundlegenden technischen Spezifikationen für elektronische Reisedokumente werden von der International Civil Aviation Organization (ICAO) – einer Unterorganisation der Vereinten Nationen – standardisiert.

Im Chip werden folgende personenbezogenen Daten gespeichert: Name, Geburtsdatum, Geschlecht, Nationalität, Gesichtsbilddaten und ab November 2007 Fingerabdruckdaten des Inhabers. Zusätzlich befinden sich die Dokumentennummer des Reisepasses sowie organisatorische Daten in den auf dem Chip abgelegten Dateien: Angaben über die Datengruppen und die Zertifikate sowie Hash-Werte der einzelnen Datengruppen und die elektronische Signatur des Passproduzenten über die gespeicherten Daten. Die Daten auf dem Chip werden nach den Vorgaben der ICAO in mehreren Datengruppen organisiert (s. Tabelle 1). Nur die Datengruppen DG1 (Personendaten) und DG2 (Gesichtsbild) sind verpflichtend, alle weiteren Datengruppen können optional verwendet werden. Auf den deutschen Reisepass werden von diesen optionalen Datengruppen in der zweiten Ausbaustufe zusätzlich die Datengruppe DG3 (Fingerabdrücke) und DG14 (*Chip Authentication Public Key)* aufgebracht [6].

Die personenbezogenen Daten werden während der Produktion des Passes auf dem Chip gespeichert und sind danach nicht mehr veränderbar.

DG1	Stufe 1	Maschinenlesbare Zone[1]
DG2	Stufe 1	Gesichtsbild
DG3	Stufe 2	Fingerabdrücke
DG14	Stufe 2	Chip Authentication Public Key
DG15	Stufe 1, optional	Active Authentication Public Key
Document Security Object	Stufe 1	Hashwerte aller Datengruppen sowie die elektronische Signatur über diese Hashwerte.

Tabelle 1: Logische Datenstruktur des EU-Reisepasses

Schutz gegen unberechtigte Benutzung

Durch die Integration von biometrischen Merkmalen in den Chip wird die Bindung eines Reisedokumentes an den legitimen Inhaber gestärkt und der unberechtigten Nutzung von Pässen anderer, ähnlich aussehender, Personen (*look-alike fraud*) entgegengewirkt. Zudem eröffnet dies für den Kontrollprozess die Möglichkeit, die bio-

[1] Dokumenttyp, Ausstellender Staat (oder Behörde), Name, Dokumentennummer, Nationalität, Geburtsdatum, Geschlecht, Ablaufdatum, optionale Daten und Prüfsummen

metrischen Daten (Gesichtsbild, Fingerabdruck) durch Software-Systeme zusätzlich bewerten zu können.

Auf den Chips können die relativ großen Datenmengen biometrischer Merkmale leicht gespeichert werden, während gleichzeitig die Möglichkeit besteht, mithilfe von kryptographischen Mechanismen die Authentizität der Daten zu garantieren sowie den unerlaubten Zugriff zu verhindern.

Fälschungssicherheit

Passive Authentisierung

Die Authentizität der im Chip gespeicherten Datengruppen wird über eine elektronische Signatur gesichert, die vom Lesegerät während des Kontrollvorganges verifiziert wird. Diese Signatur kann ausschließlich mit dem privaten Schlüssel des Passproduzenten generiert werden. Eine Manipulation der Daten würde daher beim Kontrollvorgang auffallen. Dadurch kann überprüft werden, dass die signierten Daten von einer berechtigten Stelle erzeugt und seit der Erzeugung nicht mehr verändert wurden.

Zum Signieren und Überprüfen der gespeicherten Daten wird eine global interoperable Public-Key-Infrastruktur (PKI) benötigt. Jedes teilnehmende Land baut dazu eine zweistufige PKI auf, die aus genau einer *Country Signing Certification Authority* (CSCA) und mindestens einem *Document Signer* (DS) besteht.

Die CSCA ist im Kontext der Reisepässe die oberste Zertifizierungsstelle eines Landes[2]. International gibt es keine übergeordnete Zertifizierungsstelle, da nur so garantiert werden kann, dass jedes Land die volle Kontrolle über seine eigenen Schlüssel besitzt. Die CSCA signiert mit ihrem privaten Schlüssel ausschließlich DS-Zertifikate, Passdaten werden von ihr nicht signiert. Die Verwendungsdauer des privaten Schlüssels der CSCA wurde auf drei bis fünf Jahre festgelegt. Entsprechend der Gültigkeitsdauer der Reisepässe von derzeit zehn Jahren muss der zugehörige öffentliche Schlüssel daher zwischen 13 und 15 Jahren gültig sein.

Die *Document Signer* sind zum Signieren der digitalen Dokumente berechtigte Stellen, im Normalfall also die Passproduzenten, die ebenfalls die Reisepässe drucken. Jeder *Document Signer* besitzt mindestens ein eigenes Schlüsselpaar. Der private Schlüssel wird ausschließlich zum Signieren der digitalen Dokumente verwendet, der zugehörige öffentliche Schlüssel muss von der nationalen CSCA zertifiziert werden.

Die Verwendungsdauer des privaten Schlüssels des *Document Signers* beträgt maximal drei Monate, damit im Falle einer Kompromittierung des Schlüssels möglichst wenig Pässe von den Auswirkungen betroffen sind. Entsprechend muss der zugehörige öffentliche Schlüssel zehn Jahre und drei Monate gültig sein. Aufgrund der relativ langen Gültigkeit müssen sehr starke Schlüssel verwendet werden. Als Signaturverfahren sind international RSA, DSA und ECDSA (*Elliptic Curve Digital Signature Algorithm*) zugelassen, für den deutschen Reisepass wird ECDSA verwendet. Die empfohlenen Schlüssellängen sind in Tabelle 2 dargestellt.

Algorithmus	CSCA [Bit]	DS [Bit]	AA [Bit]
RSA / DSA	3072	2048	1024
ECDSA	256	224	160

Tabelle 2: Empfohlene Schlüssellängen

Aktive Authentisierung und Chip-Authentisierung

Die passive Authentisierung garantiert die Authentizität der gespeicherten Daten. Darüber hinaus kann durch einen zusätzlichen Mechanismus auch die Authentizität des Chips selbst sichergestellt werden. Dazu muss der Chip dem Lesegerät gegenüber seine Echtheit beweisen.

Um diesen Nachweis zu erbringen, stehen zurzeit zwei verschiedene Verfahren zur Verfügung: die von der ICAO standardisierte aktive Authentisierung (*Active Authentication*) [7] und die im Rahmen der *Extended Access Control* (EAC) entwickelte Chip-Authentisierung. Beide Verfahren basieren darauf, dass in einem sicheren, nicht auslesbaren Bereich des Chips ein individueller privater Schlüssel gespeichert wird. Der zugehörige öffentliche Schlüssel wird hingegen in einer durch passive Authentisierung geschützten Datengruppe verfügbar gemacht. Der private Schlüssel kann somit vom Chip für die Authentisierung verwendet werden, aber im Gegensatz zu den restlichen Daten nicht kopiert werden. Im Folgenden werden die beiden Verfahren beschrieben:

- Bei der aktiven Authentisierung erfolgt der Nachweis über die Kenntnis des privaten Schlüssels über ein Challenge-Response-Protokoll, wobei der Chip eine vom Lesegerät gewählte Zufallszahl signieren muss. Der zugehörige öffentliche Schlüssel wird in Datengruppe DG15 angegeben. Als Signaturverfahren sind wiederum RSA, DSA und ECDSA zugelassen, die (relativ kurzen) empfohlenen Schlüssellängen sind in Tabelle 2 unter AA dargestellt.
- Bei der Chip-Authentisierung wird der Nachweis über die Kenntnis des privaten Schlüssels indirekt über den Aufbau eines stark verschlüsselten und integritätsgesicherten Kanal erbracht. Der dabei ausgehandelte starke Sitzungsschlüssel dient der Absicherung der anschließenden Kommunikation. Als Schlüsseleinigungsverfahren sind DH und ECDH ((*Elliptic Curve) Diffie-Hellman*) zugelassen. Der öffentliche Schlüssel befindet sich in Datengruppe DG14.

Beim deutschen Reisepass wird für die Chip-Authentisierung ECDH mit 224 Bit Schlüsseln eingesetzt werden. Aus Datenschutzgründen wird auch weiterhin auf die Verwendung der aktiven Authentisierung verzichtet, denn damit wäre es denkbar, dem Chip Daten zum Signieren „unterzuschieben“: Das Protokoll der aktiven Authentisierung sieht regulär vor, eine vom Lesegerät generierte Zufallszahl an den Chip zu übermitteln. Diese Zahl wird dann vom Chip mit dem privaten Schlüssel signiert und an das Lesegerät zurückgeschickt, wodurch ein Nachweis über die Authentizität des Chips erfolgt. Ein modifiziertes Lesegerät könnte hingegen keine „echte“ Zufallszahl übermitteln, sondern eine Zahl, die sich z.B. als Hashwert aus Uhrzeit, Ort etc. ergibt aber wie eine Zufallszahl aussieht. Mit der dann vom Chip signierten Zahl könnte der Lesegerätebetreiber Dritten gegenüber den Beweis über den Zugriff auf den Pass und damit z.B. den Nachweis des Grenzübertrittes führen.

> Vor diesem Hintergrund bietet die Chip-Authentisierung neben dem Aufbau eines sicheren Kanals einen weiteren Vorteil gegenüber der aktiven Authentisierung: Es erfolgt kein „Unterschreiben“ der dem Chip vorgelegten Datenblöcke. Damit entfällt dieses Problem. Die Verwendung dieses Verfahrens ist mit der Einführung der zweiten Stufe des EU-Reisepasses verpflichtend, während die

[2] In Deutschland wird die CSCA vom Bundesamt für Sicherheit in der Informationstechnik (BSI) betrieben.

Verwendung der aktiven Authentisierung optional bleibt.

Logische Bindung zwischen Chip und Pass

Ein weiterer Schutz gegen das Kopieren der auf einem Chip gespeicherten Daten wird indirekt über eine logische Verknüpfung dieser Daten mit der zugehörigen Datenseite des Reisepasses erreicht. Die wichtigsten personenbezogenen Daten sind sowohl auf dem Chip (in der Datengruppe DG1) als auch auf der Datenseite in maschinenlesbarer Form in der so genannten MRZ (Machine Readable Zone) abgedruckt. Die Überprüfung dieser Verknüpfung wird implizit durch den Chip erzwungen, denn ein Zugriff auf die Daten (s. *Basic Access Control*) erfordert die Kenntnis der MRZ, die damit selbst als Zugriffschlüssel dient. Ein kopierter Chip wird aufgrund der hohen Fälschungssicherheit des deutschen Reisepasses entdeckt, da sowohl der Inhalt der Datengruppe DG1 (durch passive Authentisierung) als auch die Datenseite inklusive der MRZ (durch physikalische Sicherheitsmerkmale) gegen Fälschung und Verfälschung geschützt sind.

Sollten dennoch die Daten aus einem Chip ausgelesen und auf einen anderen Chip kopiert werden, müsste auch noch die passende Datenseite gefälscht werden, andernfalls sind die kopierten Daten schlichtweg wertlos. Ein „Klonen" deutscher Reisepässe ist daher ausgeschlossen.

Zugriffschutz

Die Zugriffschutzmechanismen des deutschen Reisepasses dienen der Vermeidung unautorisierten Auslesens der Daten aus dem Chip. Der Begriff „unautorisiert" muss hierbei genauer differenziert werden: Primär ist darunter der Zugriff auf die Daten eines Passbuches im zugeklappten Zustand zu verstehen, also z.B. während sich der Pass in einer Reisetasche oder Geldbörse befindet (*Basic Access Control*). Für das Auslesen der Fingerabdruckdaten aus Reisepässen der zweiten Stufe wird diese Anforderung dahingehend erweitert, dass lediglich durch *berechtigte* Lesegeräte ein Zugriff erfolgen kann (*Extended Access Control*).

Basic Access Control

Bereits vor der Einführung des elektronischen Reisepasses waren die personenbezogenen Daten in maschinenlesbarer Form in der MRZ auf der Datenseite des Reisepasses enthalten (mit Ausnahme des Gesichtsbilds, welches zwar auf der Datenseite abgedruckt, jedoch nur bedingt maschinenlesbar durch „scannen" ist). Diese Daten sind jedoch nur mit der Einwilligung des Passinhabers lesbar – nur wer Zugriff auf den Reisepass hat, kann auch den Inhalt der Datenseite lesen. Solange der Reisepass geschlossen verwahrt wird, sind die aufgedruckten Informationen vor „unberechtigtem Zugriff" geschützt. Im Rahmen einer Grenzkontrolle wird der Reisepass an einen Beamten übergeben. Durch diese Übergabe stimmt der Reisende einer Überprüfung seiner personenbezogenen Daten zu.

Der grundlegende Zugriffschutz soll für die im Chip abgelegten Daten genau die Eigenschaften des bisherigen Reisepasses nachbilden: Um auf die im Chip gespeicherten Daten zugreifen zu können, muss das Lesegerät die Daten der MRZ kennen. Diese werden durch optischen Zugriff auf die Datenseite des Reisepasses gewonnen.

Die technische Umsetzung erfordert, dass sich das Lesegerät gegenüber dem Chip authentisieren muss. Für diese Authentisierung benötigt das Lesegerät einen Zugriffschlüssel, der sich aus den Daten der MRZ des Reisepasses ableitet. Das Lesegerät liest also erst die MRZ optisch, berechnet daraus den Zugriffschlüssel und kann sich dann gegenüber dem Chip authentisieren.

In die Berechnung des Zugriffschlüssels gehen die Passnummer, das Geburtsdatum des Inhabers und das Ablaufdatum des Reisepasses ein. Daraus wird ein Hash-Wert berechnet, aus dem die initialen Schlüssel für die Verschlüsselung und die Integritätssicherung (MAC) abgeleitet werden. Diese werden dann für das Aushandeln der dynamischen Sitzungsschlüssel verwendet.

Um das unberechtigte Auslesen des Reisepasses („aktives Auslesen") zu verhindern, ist die Stärke des Mechanismus ausreichend, da das Ausprobieren aller Schlüssel in kurzer Zeit unmöglich ist – selbst wenn der Angreifer Zusatzinformationen hat, wie Zusammenhänge zwischen Passnummer und Ablaufdatum. Denn der komplette Ablauf einer einzelnen BAC-Authentisierung benötigt bereits ca. 1 Sekunde an Berechnungs- und Kommunikationszeiten. Wie in Tabelle 3 dargestellt, resultieren aus bereits sehr kleinen effektiven Schlüssellängen sehr große Zeiten. Wie sich zeigt, ist ein aktives Auslesen praktisch unmöglich.

Art des Suchraums	Mögliche Schlüssel	Maximale Dauer
Voller Suchraum	2^{56}	2 Milliarden Jahre
Reduzierter Suchraum	2^{40}	35000 Jahre
Stark reduzierter Suchraum[3]	2^{30}	34 Jahre
Überwiegend bekannter Suchraum	2^{20}	12 Tage

Tabelle 3: Zeiten für das unberechtigte aktive Auslesen

Selbst bei einer sehr unwahrscheinlichen Reduzierung des Suchraums auf nur noch 2^{20} Schlüssel (ca. 6 Ziffern) dauert der Angriff noch bis zu 12 Tagen. Hierbei müsste ständiger und direkter Kontakt zur Zielperson bestehen, um im Ergebnis die unbekannten 6 Ziffern in Erfahrung zu bringen. Dies dürfte jedoch mit einfacheren Mitteln (z.B. durch „*social engineering*") und in kürzerer Zeit in Erfahrung zu bringen sein.

Ein wichtiger Punkt in diesem Zusammenhang ist auch die Reichweite, über die ein aktives Auslesen überhaupt ermöglicht werden kann. Nach den Ergebnissen der BSI-Studie MARS [2] ist ein aktives Auslesen eines ISO 14443 konformen Chips nur in einer maximalen Reichweite von ca. 15-25cm möglich (unter der Voraussetzung einer bekannten MRZ!). Eine weitere Untersuchung [9] kommt zu ähnlichen Ergebnissen.

Extended Access Control

Mit der Einführung der zweiten Stufe des elektronischen Reisepasses werden nach Vorgaben der EU die Fingerabdrücke des Passinhabers auf dem Chip gespeichert. In Deutschland werden diese Reisepässe ab November 2007 ausgegeben.

Sensitive personenbezogene Daten wie Fingerabdrücke bedürfen eines besonders starken Schutzes und vor allem der Vorgabe einer engen Zweckbindung. Innerhalb der Arbeitsgruppe zur technischen Standardisie-

[3] Dieser stark reduzierte Suchraum setzt bereits Detailwissen (z.B. das exakte Geburtsdatum und eine starke Einschränkung der Behördenkennziffer) über die Zielperson voraus.

rung des EU-Reisepasses wurde daher basierend auf einer Technischen Richtlinie des BSI [1] die Spezifikation eines erweiterten Zugriffschutzes ausgearbeitet, der so genannten *Extended Access Control* (EAC). Das Ziel dieses erweiterten Zugriffschutzes ist es, die im Chip abgespeicherten Fingerabdruckdaten ausschließlich autorisierten nationalen Lesegeräten zugänglich zu machen. Darüber hinaus ist zu prüfen, wann und in welchem Umfang EU-Mitgliedstaaten bzw. den Staaten des Schengener Abkommens und ggf. ausgewählten Drittstaaten ebenfalls ein autorisierter Zugriff ermöglicht werden soll.

Funktionsweise des erweiterten Zugriffschutzes

Der Chip zwingt jedes Lesegerät, sich gegenüber dem Chip als berechtigt „auszuweisen", bevor es Zugriff auf die Fingerabdruckdaten erhält. Das Verfahren wird Terminal-Authentisierung genannt und basiert auf einer PKI für Lesegeräte, die im Folgenden näher beschrieben wird. Der Terminal-Authentisierung ist die Chip-Authentisierung vorgeschaltet, die neben der Echtheitüberprüfung des Chips auch eine stark verschlüsselte Kommunikation zwischen Lesegerät und Chip aufbaut. Dadurch ist garantiert, dass alle nachfolgend übertragenen Daten, insbesondere die Fingerabdruckdaten, stark verschlüsselt werden und nicht unberechtigt abgehört werden können.

> Innerhalb der EU ist die Verwendung der Chip-Authentisierung (sofern vom Chip unterstützt) für alle Lesegeräte verpflichtend, auch wenn keine Fingerabdrücke ausgelesen werden. Somit werden alle personenbezogenen Daten grundsätzlich stark verschlüsselt übertragen.

Public-Key-Infrastruktur

Für die Durchführung der Terminal-Authentisierung muss das Lesegerät mit einem Schlüsselpaar und einer vom Chip verifizierbaren Zertifikatskette ausgestattet werden. In diesen Zertifikaten sind 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.

Die Zertifikate der Lesegeräte werden von einem *Document Verifier* (DV) ausgestellt. Ein DV verwaltet eine Reihe von Lesegeräten, z.B. die Lesegeräte, die im Rahmen der Grenzkontrolle verwendet werden. Jeder Staat kann somit mehrere DVs haben. Die DV-Zertifikate werden wiederum von einer nationalen Wurzelinstanz herausgegeben, der *Country Verifying Certification Authority* (CVCA). Der öffentliche Schlüssel der nationalen CVCA wird auf dem Chip gespeichert und stellt eine Art Vertrauensanker dar. Ein berechtigtes Lesegerät muss sich also mithilfe eines privaten Schlüssels und einer Zertifikatskette gegenüber dem Chip authentisieren, wobei die Zertifikatskette mit dem auf dem Chip gespeicherten öffentlichen Schlüssel der nationalen Wurzelinstanz enden muss.

> Sollen ausländische (d.h. EU und Drittstaaten) Lesegeräte zum Zugriff auf die gespeicherten Fingerabdruckdaten berechtigt werden, muss daher die nationale CVCA für den entsprechenden ausländischen DV ein Zertifikat ausstellen.

Abhören der Kommunikation

Neben dem unberechtigten aktiven Auslesen – gegen das *Basic Access Control* primär entwickelt wurde – ist prinzipiell ein weiterer Angriff auf die Vertraulichkeit der Passdaten vorstellbar: Das „passive Mitlesen", womit das Abhören einer Kommunikation zwischen Lesegerät und Chip bezeichnet wird. Ein Angreifer begibt sich also mit einer speziellen Abhöreinrichtung in die Nähe des Lesegerätes und versucht, einen oder mehrere Chip-Lesegerät-Dialoge aufzuzeichnen. Da die Kommunikation verschlüsselt erfolgt, müsste er danach mit leistungsstarken Rechenanlagen die aufgezeichneten Dialoge nachträglich entschlüsseln.

Ein derartiges passives Mitlesen ist zwar theoretisch möglich, in der Praxis aber nicht relevant. Um die Sicherheit gegen passives Mitlesen zu bewerten, sind zwei Fragen von Bedeutung:

- Bis zu welcher Entfernung lässt sich die Kommunikation mitlesen?
- Mit welcher Stärke ist die Kommunikation verschlüsselt?

Diese beiden Fragestellungen sind eng miteinander verbunden, da die effektive Verschlüsselungsstärke – wenn auch nur indirekt – von der Entfernung abhängig ist.

Mitleseentfernung

In der Literatur finden sich Spekulationen (z.B. [5][9]) über mögliche Reichweiten in denen eine kontaktlose Kommunikation nach ISO14443 mitgelesen werden kann, aber nur in wenigen Fällen wird dieses mit praktisch durchgeführten, nachvollziehbaren Messergebnissen belegt. In der vom BSI durchgeführten Studie MARS [2] wurde diese Fragestellung nun eingehend untersucht. Basierend auf einer theoretischen Betrachtung der Mitlesereichweite wurden aufwändige Messungen durchgeführt und belastbare Ergebnisse erzielt. Danach ist ein passives Mitlesen einer Kommunikation in einer Entfernung von 2m noch möglich, ab einer Entfernung von 2,70m konnte die Kommunikation jedoch nicht mehr erfolgreich mitgelesen werden.

Verschlüsselungsstärke

Nach einem – wenn auch unwahrscheinlichen – erfolgreichen Mitlesen der verschlüsselten Kommunikation muss diese im nächsten Schritt entschlüsselt werden. Zur Verschlüsselung wird Triple-DES im CBC-Modus (*Cipher Block Chaining*) verwendet. Bitfehler im Chiffretext haben sehr starke Auswirkungen auf den zu entschlüsselnden Klartext. Ein einziger Bitfehler in einem abgehörten Chiffretextblock (mit der Länge von 64 Bit) macht diesen und den folgenden Block unbrauchbar, d.h. selbst wenn der Sitzungsschlüssel dem Angreifer bekannt wäre, müsste er zunächst alle Bitfehler durch Ausprobieren manuell korrigieren. Dieser Vorgang ist sehr aufwändig, da die Anzahl und die Position der Bitfehler unbekannt ist.

In der Regel wird der Angreifer den zufälligen Sitzungsschlüssel nicht ermitteln können. Der 112 Bit starke symmetrische Sitzungsschlüssel wird allgemein als sicher betrachtet[4]. Allerdings wird die Übertragung des Sitzungsschlüssels im Rahmen des BAC-Protokolls mit dem wesentlich schwächeren Zugriffschlüssel (zur Zeit beträgt die effektive Entropie höchstens 56 Bit, s. Tabelle 3) abgesichert. Somit besteht prinzipiell die Möglichkeit, die verschlüsselte Übertragung des Sitzungsschlüssel ebenfalls abzuhören und diesen per Brute-Force,

[4] Schlüssellängen von symmetrischen und asymmetrischen Verfahren unterscheiden sich in der Regel stark, so entspricht ein 112-Bit-Triple-DES Schlüssel ungefähr einem 2048-Bit-RSA-Schlüssel.

d.h. durch Ausprobieren aller möglichen Zugriffschlüssel zu entschlüsseln. Dieses wiederum setzt aber ein fehlerfreies Abhören der Kommunikation voraus, was nur in unmittelbarer Nähe zum Lesegerät möglich ist.

Aufgrund des Aufbaus der Chiffretexte beim Schlüsselaustausch führt ein einziger Bitfehler in den letzten drei Chiffretextblöcken dazu, dass der Sitzungschlüssel nicht korrekt entschlüsselt werden kann. Zwar kann der Angreifer versuchen, die Fehler durch Ausprobieren zu korrigieren, bei einer Anzahl von *n* vermuteten Fehlern gibt es dabei allerdings etwa 196^n Möglichkeiten – bei angenommenen 4 Fehlern gibt es also bereits ca. 2^{30} Möglichkeiten, um diese anzuordnen. Da dem Angreifer sowohl der (relativ schwache) Zugriffschlüssel als auch die Anzahl und die Anordnung der Bitfehler unbekannt sind, erhöht sich der Aufwand für den Angreifer drastisch.

Einfluß des erweiterten Zugriffschutzes

Die Spezifikation des EAC-Protokolls sieht vor, nach einem erfolgreichen Durchlauf der BAC-Authentisierung einen neuen, stärkeren Sitzungsschlüssel zu verwenden, der über eine Diffie-Hellman-Schlüsseleinigung erzeugt wird (s. Chip-Authentisierung). Die Verwendung dieses starken Sitzungsschlüssels wird zum Zugriff auf die Fingerabdruckdaten vom Chip erzwungen. Zukünftig wird aber innerhalb Europas jedes Lesegerät auch vor dem Auslesen der weniger sensitiven Daten diesen Schlüssel mit dem Chip aushandeln und verwenden müssen. Damit entspräche die Schlüsselentropie der in jedem Fall ausreichenden Stärke von 112 Bit.

Location Privacy

Unter einem Bewegungsprofil versteht man ein Auftragen von Ortskoordinaten einer Person oder eines *tags* über der Zeit. In vielen Bereichen in denen RFID-Technologie angewandt wird, ist gerade dieses die gewünschte Anwendung. Üblicherweise haben die entsprechenden *tags* eine eindeutige Nummer, die mittels einer Datenbank einem Produkt (oder auch einer Person) zugeordnet werden kann. Bewegungsprofile von Personen können interaktiv oder nichtinteraktiv aufgenommen werden. Ersteres kann auch ohne jegliche *tags* oder Chipkarten realisiert werden, z.B. einfach durch das Eingeben einer ID-Nummer an Zugangskontrollen, die dann in einer Datenbank gespeichert wird.

Die Spezifikationen für kontaktlose Chipkarten nach ISO 14443 [8] sehen die Erstellung von Bewegungsprofilen nicht vor. Bereits die vorgesehene maximale Reichweite von ca. 10cm spricht deutlich gegen diesen Anwendungsfall.
Neben den physikalischen Grenzen und dem bereits beschriebenen Zugriffschutz verhindert zusätzlich die Verwendung von zufälligen Chip-UIDs („Unique“ ID) die Erstellung von unerwünschten Bewegungsprofilen. Die UID wird bei den Chips des deutschen Reisepasses jedes mal zufällig neu generiert, wenn der Chip erneut in das Feld eines Lesegerätes eingeführt und mit Spannung versorgt wird[5]. Somit kann auch diese Information nicht für die Erzeugung eines Bewegungsprofils genutzt werden.

Etwas anders sieht die Situation aus, wenn man nur das Bewegungsprofil einer (oder sehr weniger) Person(en) gezielt aufnehmen will, deren MRZ-Informationen dem System bereits bekannt sind. In dem Fall könnte die komplette BAC-Authentisierung und das Auslesen beispielsweise der Datengruppe DG1 durchlaufen werden, deren Inhalt für eine eindeutige Zuordnung zur Person ausreichen würde. Die o.g. physikalischen Reichweiten der Lesegeräte von bis zu 25 cm (s. Zugriffschutz) und die benötigte Zeit für einen vollständigen Ablauf der Authentisierung lassen einen derartigen Angriff allerdings für die Praxis als untauglich erscheinen.

Fazit

Bereits mit der ersten Stufe des elektronischen Reisepasses wurde die Fälschungssicherheit des Dokuments auf ein völlig neues Niveau gehoben. Durch den integrierten grundlegenden Zugriffschutz (BAC) wird das unberechtigte aktive Auslesen und das passive Mitlesen einer Kommunikation unter realistischen Bedingungen wirkungsvoll verhindert. Auch das Erstellen von Bewegungsprofilen ist praktisch nicht möglich.

Mit der zweiten Stufe wird der erweiterte Zugriffschutz (EAC) eingeführt. Über das Verfahren wird nicht nur sichergestellt, dass ausschließlich berechtigte, hoheitliche Lesegeräte auf die gespeicherten Fingerabdrücke zugreifen können, sondern auch der Schutz aller personenbezogenen Daten noch weiter erhöht.

Literatur

[1] BSI; *Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version;* Technische Richtlinie TR-03110; 2006

[2] BSI; *Messung der Abstrahleigenschaften von RFID-Systemen (MARS); Teilbericht zu den Möglichkeiten des passiven Mitlesens einer RFID-Kommunikation*; zur Veröffentlichung anstehend.

[3] BSI; *Protection Profile for Machine Readable Travel Document with „ICAO Application“, Basic Access Control*; Version 1.0

[4] BSI; *Protection Profile Machine Readable Travel Document with „ICAO Application“, Extended Access Control*; Version

[5] D. Carluccio, K. Lemke-Rust, C. Paar, A. Sadeghi; *E-Passport: The Global Traceability or How to Feel Like an UPS Package;* Workshop on RFID Security 2006

[6] EU Kommission; *Spezifikationen für EU-Pässe – Anhang zur Entscheidung 28/VI/2006 der Kommission K(2006)2909*

[7] ICAO; *Machine Readable Documents – PKI for Machine Readable Travel Documents Offering ICC Read-Only Access;* Version 1.1; Oktober 2004

[8] *ISO/IEC 14443: Identification cards – Contactless integrated circuit(s) cards – Proximity cards*

[9] A. Juels, D. Molnar, D. Wagner; *Security and Privacy Issues in E-passports*.

[10] I. Kirschenbaum, A. Wool*; How to Build a Low-Cost, Extended-Range RFID Skimmer*; 15th USENIX Security Symposium, 2006

[5] Bei Chips nach ISO 14443 Typ A wird normalerweise eine statisch festgelegte UID verwendet. Die Spezifikationen erlauben aber explizit auch die Verwendung von zufällig generierten UIDs (wie beim deutschen Pass). In den ICAO-Spezifikationen ist diese Vorgehensweise inzwischen empfohlen aber nicht verpflichtend.