ingenieur
wissenschaften
htw saar

Hochschule für
Technik und Wirtschaft
des Saarlandes
University of
Applied Sciences

STL SYSTEMTECHNIKLABOR

Relaisstationsangriffe auf elektronische Reisepässe

Markus Jungbluth

Technical Report – STL-TR-2015-01 – ISSN 2364-7167

stl.htwsaar.de

Technische Berichte des Systemtechniklabors (STL) der htw saar
Technical Reports of the System Technology Lab (STL) at htw saar
ISSN 2364-7167

Markus Jungbluth: Relaisstationsangriffe auf elektronische Reisepässe
Technical report id: STL-TR-2015-01

First published: February 2015
Last revision: February 2015
Internal review: André Miede

For the most recent version of this report see: https://stl.htwsaar.de/

Title image source: johtal, http://www.freeimages.com/photo/1194402

htw saar – Hochschule für Technik und Wirtschaft des Saarlandes (University of Applied Sciences)
Fakultät für Ingenieurwissenschaften (School of Engineering)
STL – Systemtechniklabor (System Technology Lab)
Prof. Dr.-Ing. André Miede (andre.miede@htwsaar.de)
Goebenstraße 40
66117 Saarbrücken, Germany
https://stl.htwsaar.de

Relaisstationsangriffe auf elektronische Reisepässe

Markus Jungbluth
Seminar "Angewandte Informatik"
Wintersemester 2014/15
htw saar – Hochschule für Technik und Wirtschaft des Saarlandes

***Zusammenfassung*—Relaisstationsangriffe sind schon länger bekannt und haben in der jüngeren Vergangenheit große Aufmerksamkeit durch Sicherheitslücken in den Schließsystemen von Fahrzeugen erhalten. Die nachfolgende Arbeit untersucht die Auswirkungen dieser Art von Angriff auf elektronische Reisepässe und versucht, die Bedrohungen für Staaten und Bürger abzuwägen.**

Einführung

Der Staatsbürger des 21. Jahrhunderts besitzt eine Fülle von neuen hybriden elektronischen Dokumenten, die ihm durch seinen Staat und andere Institutionen ausgestellt werden. Diese neuartigen Dokumente bestehen aus zwei verschiedenen Informationsträgern, einem traditionellen Träger wie Plastik oder Papier und einem neuartigen elektronischen Träger. Der elektronische Träger ist in den konventionellen Träger eingebettet und enthält alle Daten, die auch der traditionelle Träger enthält. Zusätzlich kann der elektronische Träger auch Daten enthalten, die sich nur schwer auf nicht-elektronischen Trägern speichern lassen würden. Das können zum Beispiel biometrische Daten wie Fingerabdrücke oder Daten für Gesichtserkennung sein.

Diese *Hybridisierung* von Dokumenten schreitet immer weiter vorran und dringt langsam in alle Bereiche des öffentlichen Lebens vor. Was zunächst mit Bank- und Krankenkassenkarte im letzten Viertel des vergangenen Jahrhunderts durch die Ergänzung um einem Smartcard-Mikroprozessor begann, setzte sich in Deutschland mit der Einführung von elektronischen Ausweisdokumenten in Form von Reisepass und Personalausweis fort. Diese sind jedoch nur erste Vorboten einer neuen Reihe von Dokumenten der nächsten Generation. In den Forschungsabteilungen der Chip-Hersteller und Spezial-Druckereien warten bereits erste Prototypen von neuen Führerscheinen, KFz-Zulassungen und anderen Dokumenten auf die nächste Technik-Austellung, um den Entscheidern der Nationen präsentiert werden zu können.

Die Gefahren des globalen Terrorismus und der Kampf gegen diesen, waren bei der Einführung der neuen Reisepässe ein zentrales Argument der Politik. Weiterhin wurden eine beschleunigte, sogar teilweise automatisierte Einreise und "die eindeutige und nicht trennbare Zuordnung eines Dokuments zu seinem Inhaber" als weitere Vorteile dieser neuen Technlogie angepriesen. [1]

Die Entwicklung der vergangenen 10 Jahre haben gezeigt, dass der elektronische Pass auch Gefahren und Bedrohungen für die Besitzer der Dokumente in vielen verschiedenen Bereichen mit sich bringt. Mit der Einführung elektronischer Ausweise in vielen Teilen der Welt wurden die Sicherheits- und Datenschutzrisiken für die Passinhaber bereits seit dem Jahr 2004 ausgiebig von Journalisten, Wissenschaftlern und Sicherheitsspezialisten analysiert. Die Umsetzung und Erprobung der Standards hat jedoch gezeigt, dass es immer wieder Sicherheitsprobleme gibt. In meiner Arbeit werde ich mich mit den schon sehr lange aus anderen Bereichen bekannten, aber wenig disktutierten Relaisstationsangriffen befassen. Darüber hinaus werde ich untersuchen, welche Auswirkungen die Wahl der verwendeten Technologien auf die Sicherheit des Dokuments hat.

I. Hintergrund

Der elektronischen Reisepass vereint Biometrie und RFID-Technolgie in einem Chip. Die genauen technischen Spezifikationen der zum Einsatz kommenden Standards, können dem Appendix dieser Arbeit entnommen werden.

II. Elektronischer Reisepass nach ICAO Document 9303

Diese Arbeit behandelt den heutigen de-facto Standard der ICAO. Neben diesen Spezifikationen wurden von einzelnen Ländern individuelle Standards entwickelt, die sich nicht durchsetzen konnten. In Malaysia kam beispielsweise von 1998 bis 2010 ein von der malaysischen IRIS Corporation entwickelter Standard zum Einsatz, welcher im Frühjahr 2010 vom ICAO Standard abgelöst wurde. [2]

A. Entstehung

Die Internationale Zivilluftfahrt-Organisation[1] mit Sitz in Montreal (Kanada) ist eine Sonderorganisation der Vereinten Nationen. Neben der Koordinierung von Standards und Internationalem Recht im Flugverkehr gehört die Spezifizierung von Reisedokumenten in den Aufgabenbereich der ICAO.

Seit den 1980er Jahren begannen viele Staaten mit der Austellung von maschinenlesbaren Reisedokumenten. Die ICAO legte damals in der ersten Version des *Document 9303* Vorschläge über die Vereinheitlichung der Reisepass-Daten-Karte vor. [3] Auch wenn diese Dokumente damals noch keine elektronischen Bestandteile besaßen, sah der Vorschlag die Einrichtung einer maschinenlesbaren Zone im unteren Bereich der Datenkarte[2] vor. Man zielte damit darauf ab, die Einwanderungsbeamten bei ihrer Arbeit zu entlasten. Die spezielle Zone kann automatisiert von einem Computer mittels OCR[3]

[1] International Civil Aviation Organization, kurz ICAO
[2] Seite in einem Reisepass, die alle persönlichen Daten enthält
[3] engl. Object Character Recognition, Texterkennung

ausgelesen werden und machte früher das manuelle Abtippen der Personalien überflüssig.

Seit 1997 führte man den Gedanken der weiteren Automatisierung fort und befasste sich mit der Schaffung eines einheitlichen Standards für *elektronische Reisedokumente*. [4] Im März 2004 veröffentlichte die ICAO eine Empfehlung (Blueprint) über die Einführung von biometrischen Merkmalen in Reisepässen, um "Einreise-Vorgänge zu vereinfachen" und die "Sicherheit und Integrität der Reisedokumente" zu schützen. [4] Da sich biometrische Daten (Templates) nur mit hohen Aufwand nicht-elektronisch speichern lassen, war die Einbettung eines elektronischen Speicher-Chips in den Augen der ICAO der beste Weg, um Biometrie-Daten sicher mit Reise-Dokumenten zu verknüpfen.

Am 13. Dezember 2004 wurde durch den Rat der Europäischen Union die Einführung von elektronischen (biometrischen) Reisepässen in allen Mitgliedsstaaten beschlossen. [5] Die Regierung der Vereinigten Staaten von Amerika drängte die Europäische Union im Vorfeld zu einer schnellen Einführung. Sie drohte, die bis dahin vereinbarte Visumsfreiheit für viele Bürger der Europäischen Union mit dem 2002 verabschiedeten *Enhanced Border Security and Visa Entry Reform Act* aufzukündigen, sollte es nicht zu einer Einführung von elektronischen Reisepässen in der EU kommen. [6]

Im Jahr 2005 wurde der kontrovers diskutierte Gesetzesentwurf [7] von Otto Schilly auf Basis der von der ICAO spezifizierten Standards von Bundesrat und Bundestag gebilligt. Damit wurden in Deutschland zunächst elektronische Reisepässe mit biometrischen Merkmalen in Form von biometrischen Bild-Daten eingeführt. In einem zweiten Schritt wurden beginnend mit dem 1. November 2007 Abbilder der Fingerabdrücke beider Zeigefinger in den Chips der Pässe abgelegt.

B. Technischer Aufbau

Neben dem von einer Spezialdruckerei aufwändig produzierten Papierdokument wird zur Fertigung eines biometrischen Reisepasses ein RFID-Transponder –bestehend aus Chip und Antenne– benötigt. Der in biometrischen bzw. elektronischen Pässen zum Einsatz kommende passive Transponder, welcher in großer Genauigkeit durch Document 9303 [3] der ICAO spezifiziert ist, erfüllt alle Vorgaben des *ISO/IEC-Standards 14443* und verwendet ausschließlich offene Kryptographie-Verfahren.

Um die Fülle an Daten im Speicher des Transponders sicher und korrekt zu verarbeiten, implementiert der Chip eine sog. *Logische Datenstruktur*[4] *(LDS)*, die auf einem *ISO/IEC 7816-4* Dateisystem basiert. Dieses System kennt zwei Arten von Objekten: *Dedicated Files (DF)* und *Elementary Files (EF)*.

EF entsprechen in etwa dem, was in einem gewohnten Dateisystem eine Datei ist. *DF* hingegen lassen sich mit Ordnern vergleichen, sie können weitere *DF*-Ordner oder *EF*-Dateien enthalten. Der elektronische Reisepass enthält, wie in Abbildung 1 verdeutlicht, genau eine solche *Dedicated File* mit der Bezeichnung *DF.1*.

[4]aus dem engl. : "Logical Data Structure"

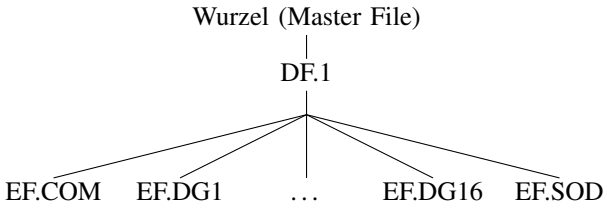

Abbildung 1. Darstellung der Logischen Datenstruktur

Innerhalb dieses "Ordners" befinden sich alle Nutzdaten in verschiedenen *EF*-Dateien.

Die Datei *EF.COM* ("Common Data") enthält ein Inhaltsverzeichnis und gibt Auskunft über Anzahl und Typ der im Dateisystem abgelegten *EF-Dateien*. Alle biometrischen und auf den Passbesitzer bezogene Daten sind in 16 speziellen EF-Dateien, sogenannten *Data Groups (EF.DGn)* organisiert. Tabelle I zeigt die Inhalte dieser Data Groups und gibt gleichzeitig einen Ausblick auf zukünftige Funktionen elektronischer Reisepässe (Data Groups 17-19).

Die letzte Datei *EF.SOD* ("Document Security Object") enthält Prüfsummen und digitale Signaturen für alle *Data Groups* und ist ein zentrales Element der *Logischen Sicherungsmechanismen*.

Tabelle I
DATA GROUPS DER LOGISCHEN DATENSTRUKTUR EINES ICAO-KONFORMEN ELEKTRONISCHEN REISEPASSES

Data Group	*Inhalt*
	`Notwendig`
1	Daten der MRZ
2	Biometrisches Lichtbild (Gesichtserkennung)
	`Optional`
3	Fingerabdrücke
4	Iris Scan
5	Lichtbild (nicht zwingend biometrisch)
6	Reserviert für zukünftige Verwendung
7	Unterschrift
...	...
11	Zusätzliche Angaben zur Person
12	Zusätzliche Angaben zum Dokument
13	Optionale Details
14	Reserviert für zukünftige Verwendung
15	Public Key für Active Authentication
16	Zu benachrichtigende Personen
	`Zukünftig vorgesehen`
17	Automatisierte Einreiseabfertigung
18	Elektronische Visa
19	Einreise/Ausreise Aufzeichnungen

Neben dem digitalen Speicher spielt die im Abschnitt II-A erwähnte *Machine Readable Zone (MRZ)* auch bei elektronischen Reisepässen weiterhin eine wichtige Rolle. Der Bereich im unteren Teil der Datenkarte des Reisepasses liefert alle wichtigen Informationen über den Passbesitzer in einer für automatische Texterkennung optimierten Schriftart. Auf der Basis der darin enthaltenen Informationen bauen die in Abschnitt II-D vorgestellten Sicherungsmechanismen auf.

C. Technische Umsetzung

Abbildung 2. ICAO-Symbol für elektronische Reispässe. Quelle: [3]

Ein zentraler Punkt bei der Herstellung der Pässe ist die Verschmelzung oder Verkettung des traditionellen Papierdokuments und des Chips. Bei deutschen Reisepässen sind Chip und Antenne im Deckel des Passbuchs eingelassen, während andere Länder die elektronischen Bauteile sichtbar[5] oder unsichtbar[6] in der Datenkarte innerhalb des Passbuchs platzieren. Bei der Herstellung des Passses wird nach dem Druck und Binden des Passbuches der Chip mit Daten bespielt. Der Chip ist so konzipiert, dass er sich nur einmal bespielen lässt. Bei dieser initialen Programmierung werden die im vorherigen Abschnitt dargestellen Datengruppen und biometrischen Vorlagen in den Speicher des Chips geladen. Im selben Schritt findet auch die digitale Signierung der Daten sowie die Generierung der kryptographischen Schlüsselpaare für die *Logischen Sicherungsmechanismen* des Passes statt. Im Nachfolgenden bezeichnet der Reisepass die Einheit aus Papierdokument und RFID-Chip.

D. Logische Sicherungsmechanismen

Im Zuge der Entwicklung eines elektronischen Reisepasses für die Vereinigten Staaten sah das *U.S. Department of State (DOS)*[7] zunächst keinen Bedarf für die Implementierung von Sicherungsverfahren. *Meingast et al.* werfen dem *DOS* in ihrer Arbeit vor, sich nicht ausreichend mit den Datenschutzrisiken und Sicherheitsbedenken vor der Einführung befasst zu haben. [8] Das DOS war damals der Ansicht, dass der elektronische Pass keine Sicherungsmechanismen benötge, da "die persönlichen Daten auf dem elektronischen Chip des Passes lediglich aus Informationen bestünden, die herkömmlicherweise sichtbar auf der Datenkarte des Passes erscheinen" [9] Dies mag auf den ersten Blick plausibel sein, jedoch sind solide Sicherungsmechanismen bei der Verwendung von RFID-Techologie unumgänglich. Eine großer Vorteil von RFID-Systemen ist die Möglichkeit von drahtlosen Lese- und Schreiboperationen auf einen Speicher. Anders als bei kontaktbehafteten Smartcards muss keine direkte physikalische Verbindung über Schleifkontakte hergestellt werden. RFID-Systeme sind damit wesentlich praktikabler und schneller in der Handhabung als traditionelle Systeme. Die Vorteile des Auslesens aus der Ferne stellen jedoch gleichzeitig ein Datenschutzproblem dar. Ein Angreifer könnte unbemerkt und ohne Wissen des Passbesitzers Daten aus dem Speicher des Chips abrufen. Das DOS hat nach Meinung von *Meingast et al.* nicht erkannt, dass die Verwebung von RFID-Technolgie und Reisedokumenten den Reisepass von einem "[technisch] inaktiven Identifikationsdokument in einen fern-auslesbaren technlogischen Gegenstand verwandelt hat." [8]

Um diesen Problemen entgegenzuwirken, hat die ICAO in Document 9303 verschiedene Sicherungsmechanismen spezfiziert. Um den Grund für die Anwendung dieser Verfahren zu verstehen, muss man sich zunächst die Interessen der beiden Parteien anschauen. Auf der einen Seite steht der Staat, der daran interessiert ist, dass die Daten eine hohe Authentizität aufweisen. Es muss also sichergestellt werden, dass die Daten die der Chip liefert, korrekt sind und nicht verfälscht werden können. Der Bürger hingegen hat ein großes Interesse daran, seine Persönlichkeitsrechte zu schützen und damit sicherzustellen, dass nicht jeder auf die Daten im Chip zugreifen kann. Er ist also an möglichst sicheren und effizienten Zugriffskontrollen interessiert.

Dass hierbei ein großes Ungleichgewicht zu Lasten des Bürgers herrscht, lässt sich bereits in den Spezifikationen des Document 9303 erkennen. Alle aufgeführten Verfahren zur Zugriffskontrolle werden lediglich als "optional" klassifiziert, während Authentifizierungsverfahren ein "verpflichtender" Bestandteil jeder Implementierung sein müssen. [3, Part 1, Volume 2, S. IV-10]

Man unterscheidet grundsätzlich zwischen 2 Arten von Sicherungsmechanismen: *Authentifizierung (Authentication)* und *Zugriffskontrolle (Access Control)*.

1) Passive Authentication: Das *Document Security Object (EF.SOD)* im Dateisystem des Passes enthält eine digital signierte Liste von *Hash-Werten* aller auf dem Chip abgelegten Dateien. Diese digitale Signatur lässt sich über eine Vetrauenskette (Chain of trust) bis zum Wurzelzertifikat des austellenden Landes verifizieren. Ein Lesegerät mit Zugriff auf diese Wurzelzertifikate, welche die ICAO in einer PKD (Public Key Database) öffentlich verfügbar macht, kann so innerhalb von Sekunden die mathematisch bewiesene Gewissheit erhalten, dass es sich um ein authentisches Dokument handelt. Für die Durchführung dieses Verfahrens werden keine besonderen Eigenschaften des Chips genutzt. Die Verifizierung der Korrektheit der Daten erfolgt allein durch das Lesegerät, daher handelt es sich um ein *passives* Verfahren. *Passive Authentication* ist ein verpflichtender Bestandteil jedes elektronischen Reisepasses, da ohne sie die Echtheit der Daten auf dem Chip nicht garantiert werden kann. Sie schützt damit die Daten im Chip vor unberechtigter Veränderung.

2) Active Authentication: Neben dem verpflichtenden passiven Verfahren schlägt die ICAO ein optionales aktives Verfahren vor, welches den Chip vor unberechtiger Duplizierung schützen soll.

Das passive Verfahren kann keine exakten Klone von echten Pässen unterscheiden, wenn die Daten auf dem geklonten Chip nicht verändert werden. Es bindet die Daten nicht an einen einzelnen Chip.

Um also das Klonen von korrekten Pass-Datensätzen zu verhindern, muss eine feste Verbindung zwischen den Datensätzen und einem einzigen Chip hergestellt werden. Active Authentication sieht daher eine Einbettung eines Schlüssel-

[5]Beispielsweise im Reisepass des Vereinigten Königreiches
[6]Beispielsweise im Reisepass des Königreichs Dänemark
[7]Innenministerium der Vereinigten Staaten von Amerika

paars K_{AA} in den Pass vor.

$$K_{AA} := (KPu_{AA}, KPr_{AA})$$

Das Schlüsselpaar besteht aus einem privaten Schlüssel KPr_{AA} und einem öffentlichen Schlüssel KPu_{AA}. Der öffentliche Schlüssel ist im Klartext aus dem Speicher des Chips abrufbar, während der private Schlüssel vor dem Auslesen geschützt ist. Der Prozessor des Chips erlaubt jedoch die Durchführung von kryptographischen Operationen mit dem privaten Schlüssel, deren Ergebnisse an das Lesegerät zurückgeliefert werden.

Diese Konstellation erlaubt dem Lesegerät die Durchführung eines *Challenge-Response-Verfahrens*, welches den Besitz des privaten Schlüssels beweisen kann, ohne ihn zu kompromittieren.

Lesegerät		Transponder (Pass)
		(KPu_{AA}, KPr_{AA})
	$\xleftarrow{KPu_{AA}}$	
KPu_{AA}		
$R_c \in M_{Zufall}$		
	$\xrightarrow{R_c}$	
		$X_r := \{R_c\}_{KPr_{AA}}$
	$\xleftarrow{X_r}$	
$L := \{X_r\}_{KPu_{AA}}$		
$L \stackrel{?}{=} R_c$		

Abbildung 3. Vereinfachtes Schema des Challenge-Response Verfahrens
Quelle: [10, S. 9]

Zu Beginn ruft das Lesegerät den öffentlichen Schlüssel KPu_{AA} aus dem Speicher des Passes ab und generiert eine 8 Byte große Zufallszahl R_c. Im nächsten Schritt übermittelt der Leser die Zufallszahl an den Transponder. Dieser verschlüsselt R_c mit dem nur ihm bekannten privaten Schlüssel KPr_{AA} und übermittelt die Chiffre X_r zurück an das Lesegerät. Abschließend entschlüsselt der Leser die Chiffre mit dem zuvor abgerufenen öffentlichen Schlüssel KPu_{AA}. Wenn der Klartext L gleich der vom Leser generierten Zufallszahl R_c ist, hat der Transponder den Besitz des privaten Schlüssels auf Grundlage der Eigenschaften eines asymetrischen Krypto-Systems bewiesen.

Unter der Annahme, dass man den privaten Schlüssel nicht aus dem Speicher des Chips extrahieren kann, liefert das Verfahren eine hinreichend große Sicherheit darüber, dass der Pass nicht geklont wurde.

3) Basic Access Control: Ähnlich wie Active Authentication ist auch *Basic Access Control (BAC)* ein *Challenge-Response Verfahren*. BAC schränkt den Zugriff auf die Daten im Speicher des Chips ein, indem es sie an ein physikalisches Dokument bindet.

Um diese Verknüpfung zu erreichen, werden im RFID-Chip zwei geheime kryptographische Schlüssel abgelegt:

$$K_{ENC}, K_{MAC}$$

Beide Schlüssel leiten sich aus Informationen (Passnummer, Geburtsdatum, Ablaufdatum und jeweilige Prüfziffern) ab, die sich auf der Pass-Datenkarte in der zweiten Zeile der *Machine Readable Zone (MRZ)*[8] befinden.

```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<<
L898902C<3UT06908061F9406236ZE184226B<<<<<14
```

Abbildung 4. Beispiel einer Machine Readable Zone
Quelle: [3, Part 1, Volume 2, S. IV-41]

Mit einem speziellen *Challenge-Response Verfahren* beweist der Leser dem Transponder, dass er sich im Besitz der geheimen Schlüssel befindet und einigt sich mit dem Chip auf zwei weitere Sitzungs-Schlüssel KS_{ENC}, KS_{MAC}, mit denen die nachfolgende Kommunikation gesichert wird. Erst wenn dieser Vorgang abgeschlossen ist und das Lesegerät bewiesen hat, dass es Kenntnis über den Inhalt des physikalischen Dokuments besitzt, gibt der Chip den Zugriff auf die Daten frei. Basic Access Control stellt damit sicher, dass ein elektronischer Zugriff auf den Pass nur möglich ist, wenn man auch direkten physikalischen Zugriff auf das Papierdokument hat. Das Verfahren verhindert, dass der Chip beispielsweise durch eine verschlossene Aktentasche ausgelesen werden kann.

BAC wird von Sicherheitsanalysten oft kritisiert [10, S. 9], da es unmöglich ist, eine einmal erteilte Zugriffsberechtigung (durch Auslesen der MRZ) zu widerrufen, da ein einziger nicht-veränderlicher Schlüssel verwendet wird. Händigt man einem Staat einmal die Daten der MRZ bei einer Passkontrolle aus, ist es dem Land auch in Zukunft -bemerkt und unbemerkt- möglich, auf die Daten im Chip zuzugreifen.

Weiterhin ist die Entropie, also die Einzigartigkeit des Schlüssels mit ca. 56 bis 52 bit sehr gering. [10, S. 8] [11, S. 1] Dies liegt hauptsächlich daran, dass Werte wie Passnummer und Geburtssdatum leicht vorhersagbar sind. In Deutschland wurden bis zur Einführung von elektronischen Reisepässen nur rein-numerische direkt aufeinanderfolgnde Passnummern vergeben. Zur Verbesserung der Sicherheit von BAC wechselte man daher in der beginnend mit der 2007 ausgegebenen zweiten Version des deutschen Passes zu zufällig gewählten einzigartigen alpha-numerischen Pass-Seriennummern.

Dem britischen Sicherheitsaktivisten Adam Laurie ist es auf Grund der geringen Entropie 2007 gelungen, die Zugriffsschlüssel eines britischen Reisepasses durch einen verschlossenen Umschlag innerhalb von 4 Stunden zu erraten [12].

Tabelle II
ZUGRIFFSKONTROLLSTUFEN

Data Group	*Inhalt*	*Zugriffskontrolle*
1	Daten der MRZ	BAC
2	Biometrisches Lichtbild	BAC
3	Fingerabdrücke	BAC & EAC
4	Iris Scan	BAC & EAC
...	...	...
15	KPu_{AA}	BAC
16	...	BAC

[8]Maschinenlesbare Zone

4) Extended Access Control: Neben BAC, welches Zugriff auf Stammdaten und das elektronische Passbild des Passbesitzers gibt, kommt *Extended Access Control (EAC)* dort zum Einsatz, wo mit sensiblen Biometrie-Templates (vgl. Appendix) gearbeitet wird. Die ICAO empfiehlt die Verwendung als Schutz von Fingerbadruck- und Iris-Scan-Daten. Mit EAC wird eine zusätzliche Sicherheitsschicht geschaffen, die austellenden Staaten die Kontrolle darüber gibt, wer auf sensible biometrische Daten zugreifen darf. Die genauen Abläufe von EAC variieren je nach Umsetzung und sind von der ICAO nicht näher spezifiziert. Hauptprinzip bei allen Implementierungen ist jedoch, dass die sensiblen Biometrie-Daten verschlüsselt auf dem Pass abgelegt werden. Nur ein Lesegerät, welches die passenden Schlüssel zum Entschlüsseln der Daten besitzt, kann auf die Sensiblen zugreifen. Mit EAC kann ein Staat zum Beispiel dafür sorgen, dass nur Verbündete Zugriff auf die Biometrie-Daten ihrer Bürger haben und so potentiellen Missbrauch durch "Schurkenstaaten" vermeiden.

5) Randomized UID: Da der RFID-Chip des Passes ISO-14443 konform ist, implementiert er einen sog. Antikollisionsalgorithmus (vgl. Appendix). Bei diesem Verfahren wird jedem Transponder eine eindeutige UID[9] zugeordnet. Sobald sich mehrere Transponder gleichzeitig im Wirkfeld der Antenne des Lesers befinden, kann das Lesegerät die Tags anhand ihrer UID unterscheiden und bei der Kommunikation adressieren. Durch das Verfahren lassen sich Kommunikationsfehler vermeiden. Jedoch wird dadurch jeder Transponder eindeutig identifzierbar, bevor irgendeine Form der Zugriffskontrolle ablaufen kann. Die Übermittlung der UID an das Lesegerät erfolgt als Teil der Protokollinitiierung von ISO-14443 und lässt sich nicht beschränken, da sie ein zentrales Element auf der untersten Kommunikationsschicht des Protokolls ist. Um dieses Risiko aus dem Weg zu räumen, ohne den Standard zu verletzen, generiert der Reisepass eine zufällige UID bei jedem Einschaltvorgang. Sie ist für die Zeit, in der sich der Transponder in der Nähe eines Lesegeräts befindet, gültig und wechselt, sobald sich der Chip aus dem Wirkbereich entfernt und somit nicht mehr mit Strom versorgt wird.

E. Physikalische Sicherungsmechanismen

Der deutsche Reisepass besitzt keine physikalischen Sicherungsmechanismen. *Markus Kuhn* schlug der Arbeitsgruppe der ICAO 2003 vor, die Länder dazu zu verpflichten, ein Drahtgitter in den Passdeckel einzulassen. [13] Mit Hilfe eines solchen Gitters wird ein Faraday-Käfig geschaffen, der einen Zugriff auf den Chip verhindert, solange das Passbuch geschlossen ist. Die Arbeitsgruppe lehnte seinen Vorschlag ab, da es sich um ein "Datenschutz-Anliegen handelt und daher nicht von Interesse " wäre. [13] Die Pässe einiger weniger Länder sind jedoch heute in der Außenhülle mit einem solchen Drahtgitter versehen.

[9]Unique Identifier

III. Angriffe auf den elektronischen Reisepass

A. Relaisstationsangriffe

Das Grundprinzip des Angriffs stellte der Mathematiker *John H. Conway* bereits 1976 dar. In *On Numbers and Games* [14] erzählt er die Geschichte eines kleinen Mädchens, das gleichzeitig gegen zwei Schachgroßmeister spielte und einen der Großmeister schlagen konnte. Das Mädchen spielte abwechselnd Schwarz gegen Großmeister A und Weiß gegen Großmeister B. Großmeister A machte den ersten Zug, den das Mädchen kopierte und als ersten Zug gegen Großmeister B verwendete. Sie kopierte wiederrum den darauffolgenden ersten Zug von Großmeister B und verwendete ihn gegen Großmeister A. Das Mädchen setzte seine Strategie fort und gewann letztenendes gegen einen der Großmeister. Durch ihre Taktik ließ Sie Großmeister A und Großmeister B unwissentlich gegeneinander spielen und konnte so scheinbar eines der Spiele gewinnen. Das Mädchen agiert damit als eine Art bidirektionaler Verstärker, der die Signale (Spielzüge) von einer Seite auf die Andere und in umgekehrter Richtung zurück überträgt.

Genau nach diesem Prinzip funktionieren Relaisstationsangriffe (engl. Relay Station Attacks) auf RFID-Systeme.

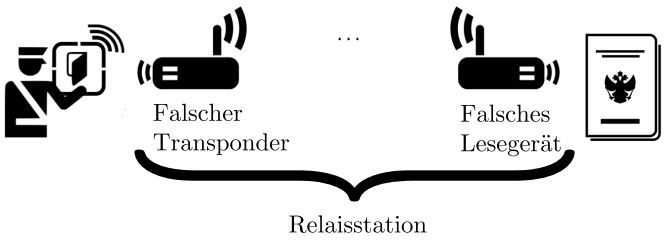

Abbildung 5. RFID-Relaisstationsangriff. Bild-Quellen: "Immigration Officer": Public Domain, "Router-Piktrogramm": Pedro Lalli, "RFID-Symbol": Nicola Galluzzi, "Reisepass-Symbol": Eugen Belyakoff. Lizensierung: Creative Commons - Atrribution (CC BY 3.0), wenn nichts anders angegeben.

Der Relaisstationsangriff wird mit Hilfe einer *Relaisstation*, bestehend aus einem *falschen Transponder* und einem *falschen Lesegerät*, durchgeführt. Beide Bestandteile sind über einen drahtgebundenen oder drahtlosen Kommunikationskanal miteinander verbunden und schalten sich zwischen Leser und Transponder. Das *falsche Lesegerät* simuliert gegenüber dem Pass ein legitimes Lesegerät, indem es die Signale eines legitimen Lesegerätes -aufgefangen durch den *falschen Transponder*- spiegelt. Umgekehrt simuliert der *falsche Transponder* gegenüber dem legitmen Lesegerät einen Reisepass-Transponder.

Die Relaisstation erweitert damit die Lesedistanz des legitmen Lesegeräts von einigen Zentimetern auf einen nahezu beliebigen Abstand.

Die ICAO-Spezifikation erwähnt diesen Angriff als "Grandmaster Chess Attack" in 5 kurzen Sätzen, verschweigt aber die konkreten Gefahren, die von ihm ausgehen. [3, Part 1, Volume 2, S. IV-52]

Relaisstationsangriffe sind jedoch eine ernstzunehmende Bedrohung für RFID-Systeme. In der jüngeren Vergangenheit wurden Sie der Allgemeinheit durch Angriffe auf "Keyless

Entry“-Systeme von Fahrzeugen bekannt. [15] Diese Systeme arbeiten ebenfalls mit RFID-Technologie. Ein Lesegerät im Fahrzeuginnenraum kann den Transponder, der meist in einem Schlüsselanhänger untergebracht ist, detektieren. Befindet sich der Transponder in unmittelbarer Nähe des Fahrzeugs, entriegelt das Fahrzeug seine Türen und hebt die Blockierung der Zündung auf, sodass man das Fahrzeug mit einem Knopfdruck starten kann. Die Aktionen der Fahrzeugelektronik beruhen auf der Annahme, dass sich ein authorisierter Fahrer in unmittelbarer Nähe des Fahrzeugs befindet. Diese Annahme, die *Michael Weiß* in seiner Master-Arbeit [16], als “Proximity Assumption“ bezeichnet, wird durch den Relaisstationsangrif widerlegt.

Dadurch, dass die gesamte Kommunikation zwischen dem legitimen Lesegerät und dem Transponder unverändert weitergeleitet wird, werden keine logischen Sicherheitsmechanismen verletzt. Alle zuvor vorgestellten Verfahren werden die Authentizität des Dokuments bestätigen, da das legitime Lesegerät weiterhin mit einem legitimen Transponder kommuniziert. Es kann jedoch nicht feststellen, dass die Daten von einem möglicherweise mehrere Kilometer entfernten Reisepass über eine Relaisstation zu ihm gelangen.

Ein Betrüger könnte dieses Verfahren zusammen mit einem Komplizen nutzen, um sich unbemerkt mit dem Pass einer anderen Person auszuweisen. Der Komplize positioniert das *falsche Lesegerät* dazu in der Nähe einer Aktentasche und greift so auf den Pass der Person zu. Der Angreifer nutzt dann den *falschen Transponder*, um sich gegenüber einem Lesegerät mit dem Pass der Person auszuweisen.

Damit das Lesegerät *Basic Access Control* durchführen kann, muss der Betrüger die Daten der *MRZ* des Passes kennen und diese auf einem gefälschten Papierdokument anbringen.

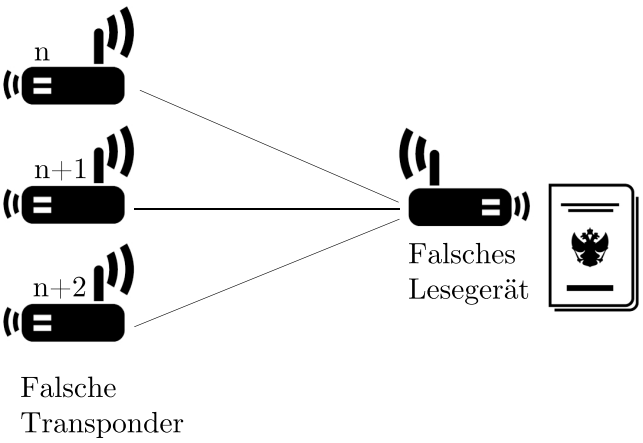

Abbildung 6. RFID-Relaisstationsangriff (n-zu-1) Bild-Quellen: “Router-Piktrogramm“: Pedro Lalli, “Reisepass-Symbol“: Eugen Belyakoff. Lizensierung: Creative Commons - Atrribution (CC BY 3.0).

Der Ex-NSA Mitarbeiter *Edward Snowden* buchte bei seiner Flucht aus Hongkong nach Russland mehrere Flugtickets, um seine genaue Fluchtroute zu verschleiern. [17] Bis zu dem Zeitpunkt, an dem sich Snowden am Flughafen auswies und eincheckte, war es den Geheimdiensten unbekannt, welche Flugroute der Flüchtige wählen würde. *Snowden* hätte seine Taktik durch einen Relaisstationsangriff auf seinen eigenen Pass perfektionieren können. Durch die Verwendung mehrerer *falscher Transponder* lässt sich ein einziger Pass gleichzeitig von n-verschiedenen Individuen nutzen. Die einzelnen Geräte können dann abwechselnd auf den legitimen Pass zugreifen. Man könnte mit Hilfe von Komplizen gleichzeitig an n-verschienden Flughäfen in verschiedenen Ländern einchecken und so eine falsche Fährte legen. Die zunehmende automatisierte Flug-Abfertigung erleichtert solche Angriffe, da keine Person den Vorgang kontrolliert und das Relay-Gerät bemerken könnte.

Umgekehrt ließen sich auch n-verschiedene Identitäten mit einem *falschen Transponder* nutzen.

B. Beurteilung und Lösungen

Allgemein scheint es so, dass die ICAO nicht sehr viel Zeit und Mühe in eine Risiko-Analyse investiert hat. Vergleicht man den dreieinhalb Seiten langen Anhang “PKI and Security Threats“ der ePass-Spezifikation [3] mit dem Rest des 150 Seiten starken Dokuments, so ist die Risiko-Abwägung bei weitem nicht so ausführlich gehalten wie beispielsweise die Dokumentation der einzelnen Protokolle und Mechanismen. Auch ist es sehr verwunderlich, dass die ICAO Mechanismen wie *BAC* und *EAC*, die dem Schutz der Persönlichkeitsrechte eines Passbesitzers dienen, lediglich als optional einstuft. Gleichwohl implementieren alle Reisepässe der Europäischen Union *BAC*.

Stellen elektronische Reisepässe mit ihren Sicherheitsproblemen damit eine Bedrohung für die innere Sicherheit bzw. für die Persönlichkeitsrechte einer Person dar?

Aus einer Präsentation von *Uwe Seidel*, Mitarbeiter des Bundeskriminalamts, vor der New Technolgies Working Group der ICAO erhält man einen Einblick in die bei Passkontrollen der Bundespolizei zum Einsatz kommenden Verfahren und Technolgien. [18] Das 17 Seiten lange PDF-Dokument zeigt, dass die Überprüfung der Echtheit eines Passes hauptsächlich durch eine Analyse des Papierdokuments durchgeführt wird. Die Verifikation des Chips spielt in Deutschland weiterhin nur eine Nebenrolle. Die Lesegeräte tasten das Dokument automatisch mit speziellen Sensoren ab und messen das reflektierte Lichtspektrum auf verschiedenen Wellenlängen. Daneben erfolgt eine Analyse der Muster, Linien und Mikroschrift auf der Datenkarte des Passes. Lesegeräte einer neueren Version verfügen darüber hinaus über weitere Sensoren zur Messung von Magnetfeldern und anderen physikalischen Eigenschaften. Die Präsentation zeigt, dass die Sicherheitslücken elektronischer Reisepässe nur eine geringe Bedrohung für die innere Sicherheit darstellen. Der beschriebene Angriff ließe sich zwar bei einer Passkontrolle anwenden, jedoch erfordert er eine Veränderung der Datenkarte, was dazu führt, dass die automatisierte optische Überprüfung fehlschlägt.

Für Einzelpersonen stellen die Reisepässe aber leider nach wie vor eine Bedrohung ihrer Persönlichkeitsrechte dar. *BAC* erlaubt einem Angreifer beispielsweise auf Grund der geringen Entropie auf die Daten eines Passes zuzugreifen, wenn er

ausreichend Zeit hat, um die Schlüssel zu erraten. Kombiniert man diese Schwachstelle mit der Durchführung eines Relaisstationsangriffs ergeben sich zahlreiche Missbrauchszenarien. *Richter, Mostowski und Poll* stellen in ihrer Arbeit *Fingerprinting Passports* [11] ein weiteres Konzept vor. Sie greifen den Pass auf einer tieferen Kommunikationsschicht des ISO-14443 Protokolls an. Durch die unterschiedlichen Reaktionen der Pässe auf verschiedene Kommandos, konnten sie in Experimenten relativ schnell die Nationalität des Reisepassbesitzers bestimmen, ohne dass eine Authentifizierung mit *BAC* erfolgte. Als eine eher unerfreuliche Anwendung dieses Verfahrens nennen *Richer et. al*, das Konzept einer "Passport bomb" [11, S. 8]. Eine solche Bombe könnte beispielsweise nur dann detonieren, wenn sich eine ausreichend hohe Anzahl von Reisepässen einer bestimmten Nationalität in ihrer näheren Umgebung befindet. Eine eher realistischere Anwendung könnte das *Fingerprinting* auch im Einzelhandel finden, um die Nationalitäten der Kunden zu erfassen.

Ein weiteres Problem ist, dass viele Lesegeräte inkorrekt implementiert wurden. Die in Check-In Automaten zum Einsatz kommenden Leser führen keine detaillierte optische Analyse der Datenkarte durch. Auch die Überprüfung der logischen Sicherungsmechanismen ist oft fehlerhaft. Dies hat *Jeroen van Beek* 2008 am Amsterdamer Flughafen demonstriert, indem er sich gegenüber einem Check-In Gerät mit einem manipulierten RFID-Chip als "Elvis Presley" ausgeben konnte. [19] Gerade im innereuropäischen Flugverkehr, bei dem durch das Schengener Abkommen Grenz- und Passkontrollen wegfallen, bieten sich durch die niedrigeren Sicherheitsstandards in den Systemen der Fluggesellschaften zahlreiche Missbrauchsmöglichkeiten.

Der Informatiker *Michael Weiß* stellt in seiner Master-Arbeit [16] Verfahren und Ansätze vor, mit denen die vorgestellten Relaisstationsangriffe erkannt werden können. Die Erkennung stützt sich dabei auf eine Messung von Signallaufzeiten. Auf Grund der Relay-Verbindung tritt eine Verzörgerung bei der Dateübertragung gegenüber einer direkten Verbindung auf. Auf Basis der daher verlängerten Antwortzeiten hat *Weiß* ein spezielles "Distance Bounding Protkoll" entwickelt mit dem ein Lesegerät oder RFID-Chip sicherstellen kann, dass es/er nicht über eine Relais-Station kommuniziert. Gegenwärtig findet dieses Verfahren leider noch keine Anwendung in elektronischen Reisepässen.

Das Minsterium für Innere Sicherheit der Vereinigten Staaten von Amerika[10] erkannte bereits 2006, dass RFID in Verbindung mit Biometrie nur "wenig Vorteile bringt, wenn man die Konsequenzen [...] für Datenschutz und Datenintegrität abwägt." [20, S. 2]

Nahezu alle bekannten Angriffe sind nur durchführbar oder von Nutzen, weil RFID-Technolgie zum Einsatz kommt. Es stellt sich daher die Frage, warum die ICAO gerade diese Technolgie vorzog. Als Hauptargument für die Nutzung von RFID wurden immer wieder die schnelleren Zugriffszeiten herrausgestellt. Im Gegensatz zu einem kontaktbehafteten System bietet RFID die Möglichkeit, auf einen Chip zuzgreifen, sobald er sich nur in der Nähe eines Lesegeräts befindet. Das Einführen einer Karte oder eines Tokens in ein Gerät entfällt. Durch die Umsetzung von *Basic Access Control* macht die ICAO jedoch die von ihr angepriesenen Vorteile obsolet, da ein physikalischer (optischer) Kontakt mit dem Pass für den Zugriff auf den Chip nötig wird.

Allgemein kann man behaupten, dass die Wahl eines kontaktbehafteten Systems zu weniger Sicherheitsproblemen geführt hätte. [8, S. 6] Durch einen notwendigen elektrischen Kontakt zum Chip wäre ein unbemerktes Auslesen generell unmöglich. Während die vorgestellten Relaisstationsangriffe theoretisch auch mit einem kontaktbehafteten System möglich sind, verlieren sie jedoch auf Grund des zwingenden physikalischen Kontakts (zum Pass des Opfers) jeden Mehrwert für einen Angreifer.

[10]United States Department of Homeland Security

IV. Appendix

A. Biometrie

Jules et al. definieren Biometrie bzw. Biometrische Erkennung als die "Verfizierung menschlicher Identität durch die Messung von biologischen Eigenschaften" [10, S. 4] Im Kontext dieser Arbeit versteht man unter dem Begriff *Biometrie* also eine *Mensch-zu-Maschine Interaktion* mit dem Ziel, die Identität des Menschen eindeutig zu bestätigen. Es gibt eine Vielzahl von Biometrischen Merkmalen, angefangen bei der aus Science Fiction Filmen bekannten Sprach-Verifikation, bis zum Iris-Scan, wie er gegenwärtig vom US-Militär im nahen Osten eingesetzt wird. Diese Merkmale haben jedoch unterschiedliche Stellenwerte bezüglich ihrer Sicherheit und Praktibilität. Während eine Sprach-Verifikation sehr bequem und schnell durchgeführt werden kann, ist sie eines der unsichersten und unzuverlässigsten biometrischen Merkmale. Ein möglicher Betrüger könnte ein System mit einer einfachen Ton-Aufnahme überlisten. Ein Iris-Scan ist hingegen wesentlich aufwendiger. Eine Person muss für einen bestimmten Zeitraum konzentriert in eine Spezial-Kamera schauen, damit die Strukturen ihrer Iris erfasst werden können. Dieser Vorgang nimmt daher wesentlich mehr Zeit in Anspruch, weshalb ein Iris-Scan weniger praktikabel ist. Eine Überlistung eines solchen Systems ist jedoch wesentlich schwieriger, aber auch nicht unmöglich, wie ein Forscher der TU Berlin auf dem 31. Chaos Communications Congress (31C3) demonstriert hat. [21] Bei der Spezifikation von biometrischen Reisepässen hat man sich auf Grund der zuvor dargestellten Kriterien auf 3 Arten von Merkmalen konzentriert. [3, Part 1, Volume 2, S. II-11 ff.] Fingerabdrücke, Gesichtserkennung und Retinaerkennung bieten ein ausgewogenes Maß an Praktibilität und Wiedererkennungssicherheit und eignen sich daher für den Einsatz bei Pass- bzw. Identitätskontrollen. *Jules et. al* unterteilen ein Biometrie-System zur Erfassung und Verifikation in 3 Bestandteile: [10]

1) Sensor: Ein Sensor, wie ein Fingerabdruckleser oder eine Kamera, erfassen die biometrischen Merkmale und wandeln sie in ein digitales Signal um.

2) Vorlage (Template): Die Vorlage oder auch das Template, sind die Referenz-Daten, mit denen ein Abgleich durchgeführt wird. Die Vorlage kann entweder ein direktes Abbild des biometrischen Merkmals sein, beispielsweise ein Bild des Gesichts einer Person oder auch "abgeleitete Information" [10]. Im Falle des Gesichts, können dies bestimmte Konturen oder Formen sein. Dieses Verfahren ähnelt der Anwendung einer *Streuwertfunktion* aus der Informatik. Die abgeleiteten Daten lassen sich hierbei gar nicht oder nur unter sehr hohem Aufwand *(Brute-Force)*[11] in das exakte Abbild eines Gesichts zurückwandeln. Ein Template der Person, deren Identität verfiziert werden soll, muss vor dem Prozess der Verifikation bereits exisitieren bzw. durch einen Sensor erfasst worden sein.

3) Verifizierender Bestandteil (Verifikation): Der verifizierende Bestandteil ist Kern eines Biometrie-System. Die vom Sensor erfassten Daten werden gegen ein Template mit einem vorbestimmten Algorithmus auf ihre Ähnlichkeit hin überprüft. Nur wenn das System eine ausreichend hohe Anzahl von Ähnlichkeiten feststellt, ist die Verifikation erfolgreich. Es gibt zwei verschiedene Arten von Verifikationssystemen. *1-zu-1* Systeme gleichen ihre erfassten Daten gegen *ein einziges* Template ab, während bei der Variante *1-zu-Vielen* die Daten gegen *eine Menge* von Templates abgeglichen werden.

[11] engl. "rohe Gewalt": Erraten eines Schlüssels oder Lösung eines mathematischen Problems durch Ausprobieren aller Möglichkeiten

B. RFID

Der Begriff *RFID* ist eine Abkürzung aus dem Englischen für *Radio Frequency Identification* (Identifizierung durch elektromagnetische Wellen) und hat sich als Begriff für Systeme aus Sender und Empfänger etabliert, die der drahtlosen Identifikation von Objekten dienen. [8, S. 1]

Ein RFID-System besteht meist aus einem Lesegerät und einem Transponder, auch als *Tag* bezeichnet. Der Leser strahlt ein elektromagnetisches Feld aus. Sobald ein Tag in den Wirkbereich dieses Feldes gelangt, kann der Leser auf Daten innerhalb des Tags zugreifen. Die Kommunikation bzw. die Modulierung erfolgt hierbei durch eine Schwächung des Feldes. [16, S. 3] Der Transponder besteht aus zwei wesentlichen Bauteilen: Einer Antenne für die Kommunikation mit dem Lesegerät und einem daran angeschlossenen Mikroprozessor. Der Chip bewerkstelligt die Kommunikation mit dem Leser nach einem festgelegten Protokoll und gibt –insofern der Leser berechtigt ist– den Zugriff auf bestimmte Speicherinhalte frei. Bei einigen Systemen kann die Kommunikation auch verschlüsselt erfolgen.

Man unterscheidet grundsätzlich zwischen zwei Arten von Tags. Aktive bzw. semi-aktive Transponder, besitzen eine interne Stromversorgung, die einen Mikroprozessor und im Fall von aktiven Tags auch das Sendemodul für den Rückkanal mit Strom versorgen. Die Reichweite aktiver Transponder kann einige Kilometer betragen.

Passive Transponder besitzen keine eigene Energiequelle. Sie beziehen ihre Versorgungsspannung aus dem Feld des Lesegeräts und sind nur aktiv, wenn Sie sich in der Nähe eines Lesers befinden. Ihre Reichweite ist damit schon rein physikalisch durch die in etwa im Quadrat zur Entfernung abnehmende Feldstärke begrenzt. Die Lesereichweite spielt sich daher, je nach Lesegerät, im Bereich von einigen Zentimetern ab. Weiterhin ist die Herstellung von passiven Transpondern wesentlich kostengünstiger, da weniger komplexe Bauteile als bei aktiven Varianten benötigt werden. Sie finden daher in der Industrie und in Logistiksystemen höhere Verbreitung als aktive Tags. [22]

C. ISO/IEC 14443

Der elektronische Reisepass basiert auf dem RFID-Standard *ISO/IEC 14443*. [3, Part 1, Volume 2, S. I-1] Der ISO-Standard setzt auf passive Transponder, mit einer Arbeitsfrequenz von 13,56 MHz und einer (vorgesehen) maximalen Lesedistanz von 10 Zentimetern. [10, S. 3] Man spricht hier von einer vom Hersteller *vorgesehenen* Lesedistanz, da es Möglichkeiten gibt, den maximalen Abstand mit speziellen Antennen bzw. durch

eine, womögliche gegen gesetzliche Vorgaben verstoßende, höhere Sendeleistung auf einige Meter zu erhöhen. [10, S. 4] Verglichen mit anderen RFID-Protokollen, ist *ISO/IEC 14443* sehr komplex.

Einfache Transponder des Typs *EM 4102* dienen beispielsweise lediglich dazu, einzelne Objekte zu identifizieren. Sie sind genau wie Transponder nach dem ISO-Standard passiv, arbeiten jedoch auf einer viel geringeren Frequenz von 125 KHz und können lediglich ausgelesen werden. [23] Es besteht also keine Möglichkeit, direkt Befehle an den Transponder zu senden. Damit gibt es bei diesen Tags keine Möglichkeit einer Zugriffsbeschränkung auf den Speicherinhalt, da eine Legitimationsprüfung des Lesers gegenüber dem Transponder mangels bidirektionaler Kommunikation nicht möglich ist. Nach einer Aktivierug durch das Feld des Lesers senden die Tags diesen Typs unaufhörlich eine UID[12] aus. Anhand dieser Daten kann dann der Besitzer des Transponders eindeutig indentifiziert werden. Transponder dieses Typs werden beispielsweise von Veterinärämtern eingesetzt um Nutz- und Haustiere zu kennzeichnen.

Da diese einfachen Systeme keine Verschlüsselung, Zugriffsbeschränkungen oder die Ablage von größeren Datenmengen unterstüzen, wären Sie für die sicherheitskritischen Anwendungen, wie den Reisepass gänzlich ungeeignet.

ISO/IEC 14443 verfolgt daher eine anderes Konzept. Ein Transponder, auch als *Proximity Integrated Circuit Card (PICC)* bezeichnet, enthält einen Mikroprozessor mit einem entsprechend für die Anwendung dimensionierten Speicher. Die Leseeinheit, welche innerhalb des Standards als *Proximity Coupling Device (PCD)* bezeichnet wird, kann bidirektional mit dem Transponder kommunzieren. Die Kommunikation erfolgt hierbei, wie in Abbildung 7 verdeutlicht, durch abwechselnde Feldschwächung von *PICC* und *PCD*.

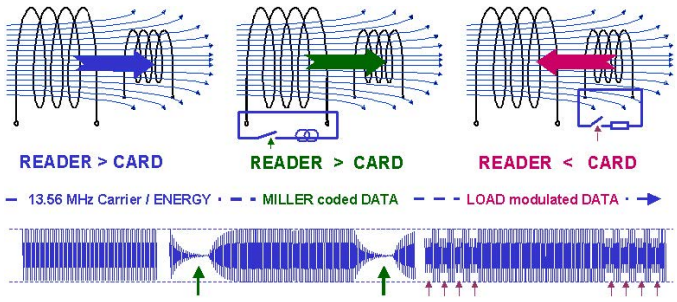

Abbildung 7. Darstellung des Kommunikationsprinzips in einem ISO/IEC 14443-konformen RFID-System (hier: MIFARE) Quelle: [24, S. 5]

Dies ermöglicht dem System die Umsetzung von Verschlüsselungsalgorithmen sowie eine Zugriffsbeschränkung und Zugriffsberechtigungsprüfung. RFID-Systeme die, wie der elektronische Reisepass, alle Teile des Standards implementieren, verwenden lediglich offene Verschlüsselungsalgorithmen, wie DES oder RSA und genügen somit dem *Kerckhoff'schen Prinzip* [13] der Kryptographie. In der Vergangenheit hat sich gezeigt, dass die Verfolgung eines *Security through Obscurity*-Ansatzes, also die Verwendung von proprietären, nichtöffentlichen Verschlüsselungssystemen fatale Folgen für die Sicherheit eines RFID-Systems haben kann.

Der Standard schreibt weiterhin einen sog. *Anti-Kollisions-Algorithmus* vor. Das Ziel dieses Verfahrens ist es, Fehler, Störungen sowie unerwartetes Verhalten des Lesegeräts durch das Vorhandensein mehrerer Transponder im Wirkbereich zu vermeiden. Hierbei erhält jeder PICC eine UID, mit der er sich zur Protokoll-Initierung bei dem PCD meldet. Das PCD kann so aus mehreren Transpondern denjenigen ansprechen, mit dem es kommunizieren möchte.

[12] Unique Identifier, einzigartes Indentifizierungsmerkmal

[13] Sicherheit eines Kryptographie-Systems muss auf der Geheimhaltung des Schlüssels beruhen und nicht auf der Geheimhaltung des Verschlüsselungsverfahrens

LITERATUR

[1] O. Schily. (2005, Juni) Statement des Bundesinnenministers auf der Pressekonferenz in Berlin am 1. Juni 2005. Geprüft: 07.02.2015. [Online]. Verfügbar: http://www.bmi.bund.de/SharedDocs/Reden/Archiv/DE/2005/06/epass.html

[2] (2010, Februar) ICAO version of Malaysian passport launched. Borneo Post online. The Borneo Post - Geprüft: 07.02.2015. [Online]. Verfügbar: http://www.theborneopost.com/2010/02/03/icao-version-of-malaysian-passport-launched/

[3] I. C. A. Organization, „Document 9303 Machine Readable Travel Documents," Tech. Rep., Oktober 2004.

[4] ——, „Biometric Technology in Machine Readable Travel Documents - The ICAO Blueprint," 2004.

[5] (2004, Dezember) COUNCIL REGULATION (EC) No 2252/2004. Rat der Europäischen Union. Geprüft: 07.02.2015. [Online]. Verfügbar: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:EN:PDF

[6] „Enhanced Border Security and Visa Entry Reform Act of 2002." [Online]. Verfügbar: http://www.gpo.gov/fdsys/pkg/BILLS-107hr3525enr/pdf/BILLS-107hr3525enr.pdf

[7] „Passgesetz," Bundesrepulik Deutschland. [Online]. Verfügbar: http://www.gesetze-im-internet.de/pa_g_1986/

[8] M. Meingast, J. King, und D. Mulligan, „Security and Privacy Risks of Embedded RFID in Everyday Things: the e-Passport and Beyond," *Journal of Communications*, Vol. 2, Nr. 7, 2007. [Online]. Verfügbar: http://ojs.academypublisher.com/index.php/jcm/article/view/02073648

[9] „Federal Register Vol. 70, No. 33," Februar 2005, U.S. Department of State.

[10] A. Juels, D. Molnar, und D. Wagner, „Security and Privacy Issues in E-passports," in *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, Serie SECURECOMM '05. Washington, DC, USA: IEEE Computer Society, 2005, S. 74–88. [Online]. Verfügbar: http://dx.doi.org/10.1109/SECURECOMM.2005.59

[11] H. Richter, W. Mostowski, und E. Poll, „Fingerprinting passports," in *NLUUG Spring Conference on Security*, 2008.

[12] J. Lettice. (2007, März) How to clone a bimoetric passport while it's still in the bag. The Register. Geprüft: 07.02.2015. [Online]. Verfügbar: http://www.theregister.co.uk/2007/03/06/daily_mail_passport_clone/

[13] M. Kuhn. (2003, Oktober) RFID friend and foe, with a note on biometric passports. Geprüft: 09.02.2015. [Online]. Verfügbar: http://catless.ncl.ac.uk/Risks/22.98.html#subj7

[14] J. H. Conway, *On Numbers And Games*, 1976.

[15] A. Francillon, B. Danev, und S. Čapkun, „Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," in *Network and Distributed System Security Symposium (NDSS) (to appear)*, 2011.

[16] M. Weiß, „Performing Relay Attacks on ISO 14443 Contactless Smart Cards using NFC Mobile Equipment," Master's thesis, Technische Universität München, 2010.

[17] Snowden's Great Escape. Leak Source. Geprüft: 07.02.2015. [Online]. Verfügbar: http://leaksource.info/2015/01/24/snowdens-great-escape/

[18] U. Seidel, „Machine Assisted Document Security Verification," New Technologies Working Group, International Civil Aviation Organization.

[19] dexlab. Geprüft: 08.02.2015. [Online]. Verfügbar: http://dexlab.nl/epassports.html

[20] *The Use of RFID for Human Identification Version 1.0*, United States Department of Homeland Security, 2006. [Online]. Verfügbar: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf

[21] P. Beuth. (2014, Dezember) Zeit Online. Geprüft: 07.02.2015. [Online]. Verfügbar: http://www.zeit.de/digital/datenschutz/2014-12/31c3-biometrie-austricksen-iris-scanner-fingerabdruck

[22] Frequently Asked Questions. RFID Journal. Geprüft: 07.02.2015. [Online]. Verfügbar: http://www.rfidjournal.com/faq/show?68

[23] EM 4102. ZeitControl cardsystems GmbH - Geprüft: 07.02.2015. [Online]. Verfügbar: http://www.transponder.de/kh4102.htm

[24] „mifare® (14443A) 13.56 MHz RFID Proximity Antennas," Philips Semiconductors, Tech. Rep., November Mifare2002. [Online]. Verfügbar: http://www.nxp.com/documents/application_note/AN78010.pdf