Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Kommunikation BAKOM
Abteilung Frequenzmanagement

Geht an :	AF/MK; Herr M. W., FEDPOL
z. K. an :	FM/RM
Gegenstand :	Abklärungen über die Datenauslesung auf Distanz beim biometrischen Pass.
Datum:	28. November 2008
Schlussbericht zu Auftrag :	A08005853
Ausgangslage :	- Anfrage FEDPOL vom 20. März 2008 - Auftrag FM/RM vom 31. März 2008
Vorgehen :	Auftragsjournal
Ergebnis :	Auf den ersten Teil der Abklärungen und Messungen wurde bereits im Zwischenbericht vom Juli 2008 eingegangen und die Erkenntnisse konnten anlässlich der ICAO NTWG am 24.09.2008 in Bern präsentiert werden. In diesem Schlussbericht sind nun die restlichen Arbeiten näher erläutert. Die Resultate der im Zwischenbericht erwähnten weiteren Messungen sind in einem separaten Messbericht zusammengefasst. Die ebenfalls im Zwischenbericht erwähnten Berechnungen und Abklärungen über die Aktivierung des Passes wurden von - H.U. R. (magnetische Feldstärken, Berechnungstool für Lesedistanzen) und - Dr. D. S. (magnetische Antennen und mögliche Anwendungen) erstellt. In diesem Schlussbericht sind die bisherigen Resultate und Erkenntnisse kurz zusammengefasst und erläutert.
Weiterbehandlung :	Für FM/RM/FD somit abgeschlossen. Sollten weitere Messungen - vor allem bei der Passherstellung - nötig werden, wird ein Folgeauftrag eröffnet.
Ablage :	Auftragsordner
Der Sachbearbeiter :	H.R. S.
Visum :	H-U. R.

Gemessene Passleser

CROSS MATCH A100 RJ0467 SER. NR. 280526. K2005
In den Messprotokollen bezeichnet als “Grosser Leser”.

Der mobile Leser besitzt ein externes 230V-Netzteil und die Datenübermittlung erfolgt über USB-Kabel.

ACG PASSPORT READER MODULE 145000506; FIRMWARE DUAL 2.1
In den Messprotokollen bezeichnet als “Kleiner Leser”.

Die Stromversorgung und Datenübertragung bei diesem portablen Leser erfolgt über dasselbe USB-Kabel. Dieser Leser besitzt keine optische Schnittstelle, die Passauslesung erfolgt mit dem Golden Reader Tool.

Bemerkungen zu den Passlesern:

- Bei beiden Lesegeräten kann das Signal mit einfachen Mitteln beim normalen Lesevorgang „mitgehört“ werden. Bei unseren Messungen konnte der Datenburst über die Luft auf dem oberen Subcarrier (die Trägerfrequenz beträgt 13.56 MHz, der obere Subcarrier 14.407 MHz), bis zu einer Distanz von ca. 25m festgestellt werden. Für den Empfang wurde eine Loopantenne mit einem Durchmesser von 50cm eingesetzt, die Frequenz um den Subcarrier war störungsfrei. Auch mit einem gewöhnlichen KW-Empfänger kann der Datenstrom auf dem Subcarrier mitgehört werden. Wir erachten eine echte Demodulation des Subcarriers unter den gemessenen Bedingungen als ohne weiteres möglich, sodass der gewonnene Datenstrom (evtl. nach einer Aufzeichnung auch offline) decodiert werden könnte.
- Zusätzlich wird die Trägerfrequenz inkl. Subcarrier ungewollt über das 230V-Netz weitergeleitet. Die Reichweite ist stark von der Netzqualität abhängig (Oberwellen, usw.). Anhand unserer Messungen am Passleser (mit angeschlossenem Notebook) und Berechnungen muss mit einer Distanz von 200 bis über 500m gerechnet werden, in der das Signal noch demoduliert werden kann.
- Beim grossen Passleser fliesst offensichtlich ein beträchtlicher Teil der ans 230V-Netz abgegebenen HF-Energie via USB-Kabel und Notebook. Ein Unterbruch der Netzleitung des Notebooks (Akkubetrieb) reduzierte den Pegel auf dem Netz um bis zu 13 dB (Faktor 4.5).
- Bei beiden Lesern wurde zudem eine grosse „Handempfindlichkeit“ festgestellt.
  Wird beim Lesevorgang der Pass zum Beispiel mit einem Holz-Lineal anstelle der Hand auf das Lesegerät gedrückt, reduziert sich die abgestrahlte Leistung wie auch der Pegel auf dem Netzkabel massiv. Die Differenz beträgt zwischen 14 und 28 dB (bis Faktor 25) auf der Trägerfrequenz wie auch auf den Seitenbändern.

Empfehlungen:

- Bessere Abschirmung bei beiden Lesern, um die abgestrahlte Leistung zu verringern. Ohne Modifikation ist unter idealen Bedingungen das Mitlesen (drahtlos) bis zu einer Distanz von ca. 25m möglich.
- Einsatz von Netzfiltern mit 80 dB Dämpfung auf allen drei Netzleitern. Damit ist eine Demodulation selbst auf kürzeste Distanz auf der Netzleitung kaum mehr möglich. Ohne Modifikation muss damit gerechnet werden, dass ein Mitlesen auf der Hausinstallation bis zu einer Distanz von über 500m möglich ist.

Aktivieren des Passes aus Distanz

Die Aktivierung des Passes, bzw. das heimliche Auslesen der Daten auf dem biometrischen Pass wurde von Dr. D. S. und H-U. R. näher betrachtet und in verschiedenen Szenarien dargestellt. Bei der heimlichen Auslesung eines Passes ist eine optische Auslesung zur Generierung des Schlüssels nicht möglich. Die Decodierung könnte aber z.B. mittels Golden Reader Tool erfolgen. Die nötigen Daten zur Generierung des Schlüssels müssten also vor der Auslesung vorhanden sein.
Die folgende kurze Zusammenfassung beschränkt sich auf zwei durchaus realistische Versionen:

Auslesevorrichtung in einem Koffer (Antennendurchmesser ca. 50cm):

- In dieser Ausleseversion muss damit gerechnet werden, dass ein Pass aus einer Distanz von ca. 35 bis 50 cm heimlich ausgelesen werden kann.

Auslesevorrichtung in einem Türrahmen:

- Das heimliche Auslesen eines Passes sollte möglich sein, sogar wenn sich die Person mit einer Geschwindigkeit von ca. 1.4 m/s bewegt, jedoch nur in einer rauscharmen Umgebung. Die Aktivierung des RFID ist problemlos möglich, für die Auslesung ist jedoch ein genügender Signal-Rauschabstand nötig. Der Bau der „Türrahmenantenne“ ist jedoch sehr aufwändig. Wenn sich die Person für ein paar Sekunden nicht bewegt - der Lesevorgang dauert ca. 10 Sekunden - kann die Antennenkonstruktion aber stark vereinfacht werden, z. Bsp. im Bereich einer Kasse oder eines Schalters.

Empfehlung:

- Den Pass in einer geeigneten Schutzhülle aufbewahren oder bei sich tragen. Die von uns gemessenen point protect ePass Schutzhüllen erreichen Dämpfungswerte zwischen 55 und 60 dB. Damit wird ein heimliches Auslesen verhindert.