CETECOM ICT Services GmbH
Untertürkheimer Str. 6-10
D-66117 Saarbrücken

Assessment of Shielding Capabilities and the Practical Effect to the Privacy of electronic MRTDs

1 Document History

Version	Applied Changes	Date of Release	Editor
1.0	Initial Document	2008-06-03	A. Ehre
2.0	Consolidated Document – Editorial Restructuring	2008-06-10	A. Ehre
2.1	Editorially Refined Document	2008-06-16	A. Ehre
2.2	Editorially Refined Document	2008-06-24	A. Ehre

2 Status, Confidentiality and Distribution

Status	Confidentiality Level	Distribution
approved by project team	project internal	project team

3 List of Content:

4 Executive Summary

Upon request of the Ministerie van Binnenlandse Zaken en Koninrijksrelaties of The Netherlands, CETECOM ICT Services performed a series of tests for assessing the shielding capabilities of ICAO conform shielded ePassports and eID-card sleeves. This document forms the assessment on a two-fold basis, the measurement of the shielding itself and the possibilities to communicate with a shielded ePassport and a shielded eID-card (NIK within a sleeve) with affordable attacking systems. Finally, there is an assessment of possibilities for detecting the pure presence of a shielded travel document, meaning whether a person is carrying a shielded ePassport or shielded eID-card.

Conclusions at a glance:

Shielding makes it more difficult to communicate with the chip. Thus it becomes more complicated for an attacker to make contact with a shielded chip in a travel document without the consent of the holder.

Concerning e-passports, the configuration where both the front and the back cover are shielded is most effective. From viewpoint of shielding, best results are obtained when the passport is fully closed. In case the passport is partly opened, the shielding capabilities are reduced.

In case passports are equipped with shielding in the front and back cover, this may lead to unacceptance or at least uncomfort for the border control. This is due to the fact that not many ePassports are deployed with shielding (especially not yet with shielding in both covers). Moreover, both the front and the back cover must be kept away from the data page in the RF reading process.

Inserting an eID card into each of the tested sleeves is less effective than a firmly closed ePassport which contains shielding in both the front and back cover of the passport booklet. The attenuation of the shielding of NIK sleeves is slightly less than the attenuation provided by a firmly closed ePassport which contains shielding in both the front and back cover.

In order to detect the presence of a shielded ePassport or eID one is expected to need an X-ray machine. Beside the fact, that such an installation could not be installed in an undiscovered way, the financial effort to implement such machine would be extremely high.

5 Document Purpose

This document forms an assessment of the results which have been achieved in the testing of shielding capabilities of ePassports and sleeves for national identity cards of The Netherlands. These investigations have been performed on request of the Ministerie van Binnenlandse Zaken en Koninrijksrelaties of The Netherlands.

This document has been compiled for a better understanding the shielding capabilities and the effects of such shielding to the privacy of an MRTD holder (ePassport and eID card). Upon recent discussions, there were requests coming up, requiring a shielding of ePassports and eID cards of The Netherlands to better protect the privacy of its holder. Beside the encryption of communication with the RF chip implemented in such ePassports, a method to block unwanted communication with the ePassport/eID card is to supply them with a respective shielding. Such shielding shall not be active when the holder of the ePassport/eID card presents his travel document to a regular check (e.g. at the border control) but it should be active in any other case. The simplest way of providing such shielding is to add some material to the ePassport which acts as a Faraday cage, meaning the adding of conducting material attenuating a magnetic field which might be provided by an attacking system. For the eID card a comparable solution is to put it into a shielding sleeve.

In a series of tests the shielding capabilities of various solutions have been investigated. These shall be seen as input to this document. Further input shall be the publicly available information on reading distances of attacking systems.

The following activity has been agreed to be addressed in this document:

The shielding capabilities of three ePassports and of 8 eID card sleeves shall be assessed by indicating the reading distance of a shielded and unshielded chip. This will be done as follows:

- A literature search will be done. This will indicate existing equipment which can make contact and communicate with the chip in travel documents. For each identified equipment, it will be indicated at what distance an unshielded chip can be contacted and communicated with. An estimation of the effort will be given which is necessary to rebuild the described equipment. The cost and the size of the equipment will be assessed as well.
- It will be assessed for each of the equipment identified at what distance it can contact and communicate with a shielded chip (in relation to the unshielded case)
- It will be assessed in what ways it is possible to identify the presence of a shielded travel document. The cost of the equipment necessary to determine the presence of a shielded travel document will be indicated. Besides it will be assessed at what distance it can be determined that a shielded travel document is present.

This document will show that the respective activities have been addressed. Via the Literature Search three different configurations could be identified for realising different activating distances. Surely, the effort for building such equipment differs; this is addressed by comparing size, cost and required knowledge for implementing. For the monitoring of ePassport/eID card communication two different configurations could be identified. For these the effort for building such equipment was weighted, too. Furthermore, the attenuation capabilities of ePassport shielding and eID-card sleeves were taken at hand to assess the change in activation/reading distance with the identified equipment configurations when a shielded travel document is used instead of a non-shielded one. Finally, an assessment of possibilities for detecting the pure presence of a shielded travel document was added.

5.1 Background

When the shielding capability of a device is to be assessed, the focus for the investigation on the unwanted communication must be laid on the active communication with the ID devices. Phenomena like eavesdropping at which a legitimate communication between reader and chip are monitored does not apply in the sense of this assessment as in that case the respective shielding is not active. Furthermore, relay attacks are not relevant as the relay attack is also invading into an already started legitimate communication. Hence, only the active communication of an illegally attacking reader with the travel document must be addressed.

Nevertheless, it is worth to have a closer look onto this aspect. In the communication one has to have both directions active – from the reader to the chip and backwards. Normal readers combine both directions in one device. When bigger reading distances shall be implemented, it is worth considering the separation of activation components and receiving components. Implementing a high activation distance would mean to implement respective amplifiers for the magnetic field. Without a separation, such amplifier means in any case an additional noise for the receiving part. Hence, the optimal configuration for attacking an electronic travel document from large distances is to have two separated units, one for activating the chip with high magnetic fields and the other one acting like an antenna as it is used for eavesdropping.

Another aspect which requires the detailed consideration of "uplink" and "downlink" is that a communication from the activating device to the chip (uplink) gets possible over bigger distances when the generated field is increasing. The higher the field, the higher the probability, that the travel document gets enough power to be activated. In the downlink from the chip to the reader (or in this case the receiving implementation) one must keep in mind that usually the load modulation amplitude is increasing when the generator field is decreasing. Hence, in this document the following basic distances must be considered to cover the worst cases:

- For the activation path: The distance from which the chip in an electronic travel document can be activated
- For the receiving path: The distance from which an eavesdropping can be implemented
- Both parts being implemented separately, but being available simultaneously.

6 Literature Search on achievable reading distances

When searching for literature which informs about equipment which can be implemented to communicate with electronic travel documents it gets obvious that many documents refer to very few sources. The following publicly available documents have been taken into consideration to evaluate the activities as agreed for the project:

[1] Harko Robroch, Riscure, ePassport Privacy Attack, Cards Asia Singapore, April 26, 2006

[2] Gerhard P. Hanke, University of Cambridge, Practical Attacks on Proximity Identification Systems, May 26, 2006

[3] Serge Vaudenay and Martin Vuagnoux, About Machine-Readable Travel Documents, Journal of Physics: Conference Series 77 (2007)

[4] Ilan Kirschenbaum and Avishai Wool, How to Build a Low-Cost, Extended-Range RFID Skimmer, Security '06: 15th USENIX Security Symposium

[5] Dennis Kügler and Ingo Naumann, Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass, DuD - Datenschutz und Datensicherheit 31 (2007)

[6] Cord Bartels, Die kontaktlose Schnittstelle -Sicherheitsfunktionen des ePasses, 2. Oktober 2007

[7] NXP Semiconductors, ISO/IEC 14443 Eavesdropping and Activation Distance, 13,56 MHz proximity smart cards, September 26, 2007

[8] CETECOM ICT Services GmbH; Test Report 1-0510/08-1-4; June 2008

The basics and the results of the Literature Search can be found in the Appendix to this document. From these investigations the following conclusions have been drawn which also define the basics for the further assessment of the ePassport/eID-card shielding.

Throughout this document the cost, the size and the required knowledge to build a respective activation of monitoring device is weighted with the classes "low", "medium" and "high". The following table shall give a more illustrative explanation of what these terms shall mean when used in this document:

Definition of effort:

	Cost	Size	Required Knowledge
Low	< 400 €	< shoe carton	technician level
Medium	< 5.000 €	< wheely trash bin	advanced technician level; expert level
High	> 5.000 €	> wheely trash bin	research level; high-grade expert level

Table 2: Definition of Effort

6.1 Analysis of the Literature Search

6.1.1 Configurations for activating an ePassport

It can be seen from the statements in the Appendix, that it is possible to build a cheap and easy reader to attack an ePassport from about 0,25 m distance. Such reader could even be made mobile (assuming some space to hide the devices and the powering with a battery). Such skimming device can be estimated at a financial effort of about 100 € (material), a size effort of a 0,2 – 0,4 m loop diameter antenna, an antenna power of 50 W and a device package in the size of a shoe carton. For increasing the reading distance to a range of about 0,4 m the antenna power must be increased

dramatically. When using a similar antenna of 0,5 m antenna diameter one has to provide already about 120 W antenna power. Surely the diameter of the antenna can be increased, too, but considering a hidden attack, a loop antenna need not be assumed to be bigger than 0,5 m in this case. When trying to further increase the activation distance, the antennas get much bigger and also the power to be brought to such antenna increases. Assuming a loop diameter of 1 m and a power amplifier providing 350 W, theoretically an activation distance of 0,6 m can be achieved.

For the further investigations we assume the following 3 cases:

- activation distance 0,25 m;
  effort in cost and size low: < 400 €; size of a shoe-carton,
  0,2 m antenna loop diameter, 50 W power;
  power supply by a 12 V battery pack possible (for approx. 2 – 3 h)
  required knowledge: technician level

- activation distance 0,4 m;
  effort in cost and size medium: approx. 5000 €; size of a trash bin
  0,5 m antenna loop diameter, 120 W power;
  power supply: timely limited even with car battery (approx. 3 h)
  required knowledge: advanced technician level; expert level

- activation distance 0,6 m;
  effort in cost and (especially) size very high: > 5000 €; bigger than the size of a trash bin
  1,0 m antenna loop diameter, 350 W power;
  power supply: power mains network
  required knowledge: research level; high-grade expert level

6.1.2 Configurations for monitoring an ePassport communication

It can be seen from the information in the Literature Seach, that the monitoring of a chip signal is realistically possible in ranges of maximum 7 m in an absolutely quiet surrounding when the normal principles of the near-field phenomena is taken at hand. This maximum is usually reduced when the normal communication is monitored as for the encryption of the signal a signal-to-noise ratio (SNR) of at least 10 dB must be achieved to guarantee a bit error rate (BER) sufficiently low to reconstruct the signal (see [5] and [2]).

In the case as studied in this document, however, only the lower layer communication shall be addressed to contemplate the worst-case scenario (e.g. distinguishing different makes of ePassports just by the lower layer communication). For such communication a much higher BER can be allowed meaning that the SNR can be allowed to get close to 0 dB. But even in that scenario it is shown in [7], that a reading distance in normal residential environments is in a range of 6,5 m and in business environments as it is to be expected at airports etc. in a range of 6,0 m. The effort to reach the aforementioned reading distances is high with respect to the cost (in the test high-sensitive test equipment was used (> 10.000 €)) and also with respect to the size. The tests have been performed with antennas that are of sizes equal or even bigger than 1 m in diameter. Even the theoretical limit to which one could get with infinite effort shows, that the access distance is limited.

When taking into account a Far-Field approach (e.g. re-calculating the signals from unwanted emissions in the E-field phenomena) the theoretical limit is shown to be in a range of less than 5 m in normal residential and business areas when a minimum BER of 1E-3 shall be achieved. When taking the same approach for a reduced BER and a SNR close to 0 dB, the monitoring distance in business areas remains below 9,5 m. However, in that scenario no communication with the chip is possible as the remaining signal to noise ratio would not allow for sufficiently proper signal retrieval.

For the further assessment the following scenarios shall be taken into account for the monitoring of ePassport communications:

- monitoring distance 5 m;
  effort in cost and size medium: < 5000 €; size of a trash bin
  power supply: timely limited with car battery
  required knowledge: advanced technician level; expert level

- monitoring distance 9,5 m;
  effort in cost and size high (far-field-approach): > 5000 €; size bigger than trash bin
  1,8 dB antenna gain (lambda/2 antenna)
  required knowledge: research level; high-grade expert level
  power supply: timely limited with car battery

6.1.3 Technical Implementation

When implementing an attacking system, both parts – the activation part and the receiving part – must be built and optimised. This means, in addition to the installation of two parts in a usually controlled environment the efforts for implementing both parts must be added. Furthermore, the shielding of an ePassport or an eID-card will have effects on both the activating and the monitoring distance.

7 Assessment of the shielding in ePassports or the shielding of eID-card sleeves

All discussions as given above assume the communication with a non-shielded RFID chip. This document, however, shall also give a feedback for the cases in which a shielding is added to the ePassport or the eID card. Therefore, this document refers also to the attenuation capabilities of shielded ePassports and shielded eID-cards as they have been investigated in test report CETECOM 1-0510-1-4/08. In the case under consideration the RFID chip in the ePassport can only be seen as non-shielded when it is opened or when the NIK is taken out of the sleeve. When the ePassport or the NIK are carried by the holder the ePassport is assumed to be closed and the NIK is expected to be inside the respective sleeve. Especially for the ePassport, Test Report 1-0510-1-4/08 investigated three different ePassport configurations which shall be considered in this document as well:

1) **ePassport firmly closed**

2) **ePassport front open**
   Distance between the holder page and the front cover: 7,5 cm
   Distance between the holder page and the back cover: 0,7 cm

3) **ePassport back open**
   Distance between the holder page and the front cover: 0,2 cm
   Distance between the holder page and the back cover: 6,0 cm

Starting with the scenario selection we have made in this document above, the results of Test Report 1-0510-1-4/08 can be used to assess the accessibility of ePassports and eID-cards (NIK) when they are supplied with a respective shielding.

For the assessment of the resulting reading distance the relation between the field and the distance from an antenna must be taken into consideration. The magnetic field reduces with the distance from the antenna (following the law of Biot and Savart). When a shielding is applied the achieved attenuation can be used to express the decrease in activation/receiving distance compared to the non-shielded case. This is done in the assessment down below.

7.1 Resulting activation and monitoring distances with shielded eID-cards (NIK)

Scenario	equipment capable of activating a non-shielded eID card from 0,25 m distance	equipment capable of activating a non-shielded eID card from 0,40 m distance	equipment capable of activating a non-shielded eID card from 0,60 m distance
Estimated Effort	low	medium	high
Assessed Sleeve	achievable activating distances with the respective equipment when NIK shielding is used		
NIK 1	6,49 cm	not possible	not possible
NIK 2	2,43 cm	not possible	not possible
NIK 3	6,53 cm	not possible	not possible
NIK 4	2,58 cm	not possible	not possible
NIK 5	3,16 cm	not possible	not possible
NIK 6	3,11 cm	not possible	not possible
NIK 7	5,93 cm	not possible	not possible
NIK 8	6,74 cm	not possible	not possible

Note: The term "not possible" in the table means that it is not possible to achieve the activation field strength for a chip when it is shielded with the assumed activation equipment even when reducing the distance to the activation antenna. To activate the shielded chip, there are changes required in the equipment installation (loop antenna diameter, amplifier). The calculation is based on the law of Biot and Savart, when assuming a constant power at the antenna.

Table 5: Resulting Activation Distances for eID-cards (NIK)

As it could be seen in the table above, with the installations as selected for this evaluation the shielded eID-card could not be activated in some cases. Therefore, another approach was taken to visualise the appropriateness of the shielding. In the following table it is given, what power would be necessary for activating the shielded chip at the relevant distance from the activation antenna.

Scenario	equipment capable of activating a non-shielded eID card from 0,25 m distance	equipment capable of activating a non-shielded eID card from 0,40 m distance	equipment capable of activating a non-shielded eID card from 0,60 m distance
Estimated Effort for the initial installation	low	medium	high
Assessed Sleeve	required power at the activation antenna for activating the shielded eID-card in the respective distance as given above (0,25 m; 0,4 m; 0,6 m)		
NIK 1	170 W	407 W	1188 W
NIK 2	212 W	508 W	1481 W
NIK 3	169 W	406 W	1185 W
NIK 4	210 W	505 W	1473 W
NIK 5	206 W	494 W	1440 W
NIK 6	206 W	495 W	1443 W
NIK 7	176 W	423 W	1234 W
NIK 8	167 W	400 W	1168 W

Table 6: Required Power for activating eID-cards (NIK)

As it can be seen from the figures in Table 6, the effort to achieve the same activating distance when an eID-card is placed into a shielding sleeve increases seriously. Even in the case where an antenna power of roughly 170 W is required, such equipment would not fit anymore into a shoe-carton. Also the powering with a battery is only possible over a very limited time (approx. 45 min.). For the cases with even higher activating distances the resulting power demand would require a fixed installation with a powering from the power mains network. An aspect which is kept totally out of the investigation

is the health threat of persons passing along such installations, especially when they are dependent on electronic health facilities (such as cardiac pacemakers, insulin pumps, etc.). This document is not intended to answer that question, as extensive EMC testing would be required.

Scenario	equipment capable of monitoring a non-shielded eID card from 5 m distance	equipment capable of monitoring a non-shielded eID card from 9,5 m distance	
Estimated Effort	medium	high	
Assessed Sleeve	achievable monitoring distances with the respective equipment when NIK shielding is used		
NIK 1	221 cm	421 cm	
NIK 2	191 cm	363 cm	
NIK 3	222 cm	421 cm	
NIK 4	192 cm	364 cm	
NIK 5	195 cm	370 cm	
NIK 6	194 cm	369 cm	
NIK 7	216 cm	410 cm	
NIK 8	224 cm	425 cm	

Table 7: Resulting Monitoring Distances for eID-cards (NIK)

7.2 Resulting activation and monitoring distances with shielded ePassports

Scenario	equipment capable of activating a non-shielded ePassport from 0,25 m distance	equipment capable of activating a non-shielded ePassport from 0,40 m distance	equipment capable of activating a non-shielded ePassport from 0,60 m distance
Estimated Effort	low	medium	high
Assessed Type of Shielding	achievable activating distances with the respective equipment when the ePassport is having a shielding in the back cover (Shielding A)		
ePassport firmly closed	14,56 cm	18,24 cm	11,22 cm
ePassport front open	18,60 cm	27,28 cm	35,40 cm
ePassport back open	23,84 cm	37,77 cm	55,90 cm
Assessed Type of Shielding	achievable activating distances with the respective equipment when the ePassport is having a shielding in 2 visa pages (Shielding B)		
ePassport firmly closed	12,55 cm	12,84 cm	not possible
ePassport front open	18,42 cm	26,90 cm	34,60 cm
ePassport back open	24,24 cm	38,54 cm	57,32 cm
Assessed Type of Shielding	achievable activating distances with the respective equipment when the ePassport is having a shielding in the front and the back cover (Shielding C)		
ePassport firmly closed	0,27 cm	not possible	not possible
ePassport front open	16,54 cm	22,83 cm	25,34 cm
ePassport back open	13,59 cm	15,77 cm	not possible

Note: The term "not possible" in the table means that it is not possible to achieve the activation field strength for a chip when it is shielded with the assumed activation equipment even when reducing the distance to the activation antenna. To activate the shielded chip, there are changes required in the equipment installation (loop antenna diameter, amplifier). The calculation is based on the law of Biot and Savart, when assuming a constant power at the antenna.

Table 8: Resulting Activation Distances for ePassports

As it could be seen in the table above, with the installations as selected for this evaluation the shielded ePassport could not be activated in some cases. Therefore, another approach was taken to visualise the appropriateness of the shielding. In the following table it is given, what power would be necessary for activating the shielded chip at the relevant distance from the activation antenna.

Scenario	equipment capable of activating a non-shielded ePassport from 0,25 m distance	equipment capable of activating a non-shielded ePassport from 0,40 m distance	equipment capable of activating a non-shielded ePassport from 0,60 m distance
Estimated Effort for the initial installation	low	medium	high
Assessed Type of Shielding	required power at the activation antenna for activating the shielded ePassport in the respective distance as given above (0,25 m; 0,4 m; 0,6 m) for an ePassport having a shielding in the back cover (Shielding A)		
ePassport firmly closed	94 W	226 W	659 W
ePassport front open	72 W	173 W	504 W
ePassport back open	53 W	128 W	372 W
Assessed Type of Shielding	required power at the activation antenna for activating the shielded ePassport in the respective distance as given above (0,25 m; 0,4 m; 0,6 m) for an ePassport having a shielding in 2 visa pages (Shielding B)		
ePassport firmly closed	109 W	261 W	761 W
ePassport front open	73 W	175 W	510 W
ePassport back open	52 W	125 W	364 W
Assessed Type of Shielding	required power at the activation antenna for activating the shielded ePassport in the respective distance as given above (0,25 m; 0,4 m; 0,6 m) for an ePassport having a shielding in the front and the back cover (Shielding C)		
ePassport firmly closed	221 W	530 W	1546 W
ePassport front open	82 W	197 W	576 W
ePassport back open	101 W	242 W	705 W

Table 9: Resulting Activation Distances for ePassports

As it can be seen from the figures in Table 9, the effort to achieve the same reading distance with a shielded ePassport increases seriously, especially when the ePassport is firmly closed. While the activation of a partly opened ePassport seems to be possible with only a marginal additional effort in most cases, the power demand in the case of a firmly closed ePassport is increasing to a grade, where it is getting difficult to activate an ePassport with a mobile solution (e.g. powered by a battery).

Scenario	equipment capable of monitoring a non-shielded ePassport from 5 m distance	equipment capable of monitoring a non-shielded ePassport from 9,5 m distance	
Estimated Effort	medium	high	
Assessed Type of Shielding	achievable monitoring distances with the respective equipment when the ePassport is having a shielding in the back cover (Shielding A)		
ePassport firmly closed	328 cm	623 cm	
ePassport front open	392 cm	745 cm	
ePassport back open	480 cm	912 cm	
Assessed Type of Shielding	achievable monitoring distances with the respective equipment when the ePassport is having a shielding in 2 visa pages (Shielding B)		
ePassport firmly closed	298 cm	566 cm	
ePassport front open	389 cm	740 cm	
ePassport back open	487 cm	925 cm	
Assessed Type of Shielding	achievable monitoring distances with the respective equipment when the ePassport is having a shielding in the front and the back cover (Shielding C)		
ePassport firmly closed	185 cm	353 cm	
ePassport front open	359 cm	682 cm	
ePassport back open	313 cm	595 cm	

Table 10: Resulting Monitoring Distances for ePassports

8 Detecting the presence of a shielded ePassport

There are different types of ePassports deployed over the world (e.g. with shielding and without). If such different types of travel documents are provided with a certain signal (e.g. magnetic field, electric field, x-rays), each of the solutions might mean a specific influence to the respective signal. If that influence to the respective signal could be classified, one could imagine a method for detecting a (even hidden) shielded travel document

The question which is raised by this section is, whether a shielded ePassport can be detected by certain means and what effort would be required to do so.

8.1 Detection by Near-Field-Technologies (magnetic field)

First, a detection by the means of the near-field phenomena shall be addressed. In fact for such detection exactly the same rules apply as for the communication with the ePassport, hence, for this section the investigation on the activation and monitoring of proximity chips as given in section 6 above in this document apply.

One could imagine, that the presence of the shielded ePassport or a NIK sleeve could be detected simply by the additional load such shielding would mean for a magnetic field. However, such apparatus would detect only the present metal, hence, there would be similar responses by any other metallic object, that is carried by the holder. Such technique is for instance used at airport security controls. Problem of such technique would not only be that there are other objects giving the same response as an ePassport shielding but also, that the location of the ePassport would be unknown. The distance between the generator antenna and the detected object, however, will influence the objects response dramatically. The same applies for the orientation of the object. Hence, it can be rated as impossible to simply detect the presence of an ePassport shielding or an eID-card sleeve by the means of near-field technologies (except in cases of normal communication). As it can be deemed as technically impossible to detect the presence of an ePassport by means of the magnetic-field approach, a cost and size estimation of a respective installation does not apply.

8.2 Detection by Far-Field-Technologies (electric field)

Again, as soon as a communication with the shielded chip can be established the same conditions apply for the far-field phenomena as described in section 6 above in this document.

When trying to detect an ePassport shielding or an eID card sleeve by means of the response which is received when the ePassport/eID card holder is brought into an electric field, in principle the same problems apply as given for the near-field technologies. Nevertheless, it is easier to form a certain antenna pattern which is more directional. This could help to locate reflecting material. To find out the shape of such object, however, would require a resolution of such apparatus, which is not achievable. Hence, also in this case a reflected response can come from any reflecting object. Also in this case the distance of the object forms a problem, however, when using a pulsing signal with signal round trip analysis, the distance of objects might be predictable for further investigation processes. Nevertheless, the effort to build such an apparatus and especially to place such apparatus in mostly controlled areas is nearly impossible to bear. Such installations would get close to the radar approach and the financial effort would be very high (much bigger than the aforementioned 5000 €). Furthermore, the technical skills to build such equipment and especially to classify different objects would definitely require research and high-grade expert level.

8.3 Detection by X-Ray Technologies

In fact, like at the security control gates it is possible to locate and identify various materials by the penetration response such materials provide to x-rays. With such a detection method it is surely possible to locate a shielded ePassport or a shielded eID-card (as any other material of interest as well). Nevertheless, such detection machine requiring an x-ray source and also an x-ray detection panel is not easy to procure and even more complicated to install at a respective location. Furthermore, it must be kept in mind that such method is not very healthy for the people passing by or being in the surroundings. In fact such machine would easily be detected and identified. Anyhow, someone using a method like x-ray detection would definitely not only be interested in finding out, which person is the holder of a shielded ID document. Surely the financial effort to detect an electronic device by means of x-ray technology is extremely high, the knowledge level which would be required to implement such solution requires special expertise and research capabilities in the field of x-ray technology as well as signal processing.

9 Conclusions

When assuming the equipment for attacking ePassports/eID-cards as described above in this document it can be stated that with the eID-card shielding (e.g. implemented in form of a NIK sleeve) the unwanted communication with the eID-card can be seriously complicated for the attacker. Even if further phenomena which have not been addressed in this investigation might discover further aspects, the shielding does increase the privacy of an eID-card holder with respect to unwanted data access.

When assessing the case of ePassports, the shielding can only work efficiently, when the distance between the shielding and the data page which carries the proximity card chip is kept low. Not surprising, the best attenuation results (best protection) are achieved with an ePassport which carries the shielding in both, the front and the back cover of the booklet. Nevertheless, as soon as the ePassport booklet is partly opened in the way it is described in Test Report 1-0510-1-4/08 one must accept that the shielding capabilities are reduced. Again the case in which the shielding is in both, the front and the back cover the situation must be rated as the best (with respect to increasing privacy) as in any of the investigated conditions at least one of the shieldings was relatively close to the data page.

Even if the resulting distances for the ePassport seem to be significantly bigger than in the case with the eID cards (except for the case with a firmly closed ePassport having shielding in both, the front and the back cover) one must keep in mind that always both systems (activating and monitoring system) must be in place to attack an electronic travel document in situations where it is not anyhow presented for a legitimate control. Having this in mind, at least for the firmly closed ePassport as well as for the eID card in a sleeve, acceptable attenuations can be achieved.

What must be kept in mind is, that at border controls all over the world there will be a typical way of putting ePassports to the reader. It can be assumed, that the ePassport is opened and the data page is placed on the optical reader before the reader accesses the chip via the RF interface. When there is a shielding in both the front and the back cover, also both covers must be kept away from the data page in the RF reading process. As not many ePassports are deployed with a shielding (especially not yet with shielding in both covers) a certain rate of "unacceptance" or at least "uncomfort" for the border control and the holder must be assumed.

In any case when assessing the results of this document it must be kept in mind, that the figures above address the absolute worst-cases for the holder (best cases for an attacker). Such worst case will not be present in typical environments. The investigations in Test Report 1-0510-1-4/08 as well as the referred reader implementations always assume that the antenna of the chip and the activation/reader device have a good coupling (meaning that they are more or less co-oriented and the loops are located parallel to each other). In reality, the orientation of an RFID chip antenna in a holder's pocket is unknown and can only be guessed. Hence, there is a natural decrease in all the values as shown above upon that orientation uncertainty. Test Report 1-0510-1-4/08 gives some more detailed information on the field strengths which are achievable in situations where the loops are not located in parallel to each other.

In any case it must be kept in mind that all results as reported in this document assume some basic parameters which are dependent on the actual application. Other RFID applications (such as tags only providing a single ID number as used in logistics etc.) might lead to different results due to changed parameters (e.g. lower activation field strength). Furthermore, the estimations are only valid for the 5 selected installations.

In order to detect the presence of a shielded ePassport or eID one is expected to need an X-ray machine. Beside the fact, that such an installation could not be installed in an undiscovered way, the financial effort to implement such machine would be extremely high.

10 Appendix A – Basics and Results of the Literature Search

10.1 Background

When the shielding capability of a device is to be assessed, the focus for the investigation on the unwanted communication must be laid on the active communication with the ID devices. Phenomena like eavesdropping at which a legitimate communication between reader and chip are monitored does not apply in the sense of this assessment as in that case the respective shielding is not active. Furthermore, relay attacks are not relevant as the relay attack is also invading into an already started legitimate communication. Hence, only the active communication of an illegally attacking reader with the travel document must be addressed.

Nevertheless, it is worth to have a closer look onto this aspect. In the communication one has to have both directions active – from the reader to the chip and backwards. Normal readers combine both directions in one device. When bigger reading distances shall be implemented, it is worth considering the separation of activation components and receiving components. Implementing a high activation distance would mean to implement respective amplifiers for the magnetic field. Without a separation, such amplifier means in any case an additional noise for the receiving part. Hence, the optimal configuration for attacking an electronic travel document from large distances is to have two separated units, one for activating the chip with high magnetic fields and the other one acting like an antenna as it is used for eavesdropping.

Another aspect which requires the detailed consideration of "uplink" and "downlink" is that a communication from the activating device to the chip (uplink) gets possible over bigger distances when the generated field is increasing. The higher the field, the higher the probability, that the travel document gets enough power to be activated. In the downlink from the chip to the reader (or in this case the receiving implementation) one must keep in mind that usually the load modulation amplitude is increasing when the generator field is decreasing. Hence, in this document the following basic distances must be considered to cover the worst cases:

- For the activation path: The distance from which the chip in an electronic travel document can be activated
- For the receiving path: The distance from which an eavesdropping can be implemented
- Both parts being implemented separately, but being available simultaneously.

10.2 Reporting of successful (or theoretically possible) activation distances:

In the following table the distances which have been reported to successfully activate a proximity chip (as used in travel documents) are given:

Source	reported activation distance	effort for implementing			Remarks
		in terms of cost	in terms of size	in terms of knowledge	
[1]	0,5 m	no information	no information	knowledge on the communi-cation itself; more mature experience in RF field generation	
[2]	0,27 m	low to medium	medium Antenna size approx. A3	medium knowledge on the communi-cation itself; more mature experience in RF field generation	achieved with 4 W amplifier
[4]	0,25 m	low (100 €)	medium (40 cm loop antenna); 12 V battery	low solutions freely available	Increase of range not easily doable by increasing the power.
[5]	0,25 m	low (300 – 400 €)	medium	medium	
[7]	0,25	low	low	medium knowledge on the communi-cation itself; more mature experience in RF field generation	requires about 50 W antenna power, antenna of 0,2 m loop diameter
[7]	0,4 m	medium	medium	medium knowledge on the communi-cation itself; more mature experience in RF field generation	requires more than 120 W antenna power, antenna of 0,5 m loop diameter
[7]	0,6 m	high	high	medium knowledge on the communi-cation itself; more mature experience in RF field generation	requires more than 350 W antenna power even for an antenna of 1 m loop diameter (not mobile!)

Table 1: Reported Activation Distances

Definition of effort:

	Cost	Size	Knowledge
Low	< 400 €	< shoe carton	technician level
Medium	< 5.000 €	< wheely trash bin	advanced technician level; expert level
High	> 5.000 €	> wheely trash bin	research level; high-grade expert level

Table 2: Definition of Effort

10.3 Reporting of successful (or theoretically possible) eavesdropping distances:

As said before, for this investigation we need to base the eavesdropping distance for assessing the appropriateness of an ePassport/eID card shielding as the activation of the chip could be made either by a legitimate reader or a separately placed activation path. Moreover, this assessment shall take the basic RFID communication into account, rather than a complete cryptographically secured reading of the chip. Therefore, also the separated activation and an eavesdropping reception must be deemed as possible. In the following table the distances which have been reported to successfully listen to a communication between a reader and a proximity chip (as used in travel documents). The list is completed by a figure as found by investigations at CETECOM which have not been published so far.

Source	reported eavesdropping/ communication distance	effort for implementing			Remarks
		in terms of cost	in terms of size	in terms of knowledge	
[1]	5 m (eavesdropping)	medium	medium	medium	
[2]	4 m (eavesdropping)	medium	medium	medium	
[2]	1,45 m (communication)	medium	medium	high	communication must be rebuilt (more complicated than just listening)
[5]	2,7 m	medium	medium	medium	considering the signal-to-noise ratio in normal environments; considering the required signal quality (BER). (see also MARS study of the BSI)
[7]	3,8 m (424 kbit/s) (eavesdropping)	maximum (theoretical limit)	maximum (theoretical limit)	maximum (theoretical limit)	theoretical limit; BER: 1E-3 Business Environment (such as at airports etc.) SNR: 10 dB
[7]	4,5 m (424 kbit/s) (eavesdropping)	maximum (theoretical limit)	maximum (theoretical limit)	maximum (theoretical limit)	theoretical limit; BER: 1E-3 Residential Environment SNR: 10 dB

Source	reported eavesdropping/ communication distance	effort for implementing			Remarks
		in terms of cost	in terms of size	in terms of knowledge	
[7]	8,9 m (424 kbit/s) (eavesdropping)	maximum (theoretical limit)	maximum (theoretical limit)	maximum (theoretical limit)	theoretical limit; BER: 1E-3 Quiet Rural Environment SNR: 10 dB
[7]	47,3 m (Far-Field-Eavesdropping)	high	high	high	theoretical limit; BER: 1E-3; Quiet Rural Environment, antenna gain: 1,8 dB SNR: 10 dB
[7]	< 5m (Far-Field-Eavesdropping)	high	high	high	theoretical limit; BER: 1E-3; Residential or Business Environment (airports, etc.); SNR: 10 dB
CETECOM	7 m	high	high	medium	measured in a clean environment (anechoic chamber) with best achievable signal-to-noise ratio; not considering the signal quality (BER) as the chip was not read out but only the presence of the communication was monitored.

Table 3: Reported Monitoring Distances

Definition of effort:

	Cost	**Size**	**Knowledge**
Low	< 400 €	< shoe carton	technician level
Medium	< 5.000 €	< wheely trash bin	advanced technician level; expert level
High	> 5.000 €	> wheely trash bin	research level; high-grade expert level

Table 4: Definition of Effort