Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense nationale

Direction centrale de la sécurité
des systèmes d'information

Paris, the 24 october 2008

N°2415/SGDN/DCSSI/SDR

Référence : NOTE/09.1

APPLICATION NOTE

E-PASSPORT : UNDERSTANDING THE EAC PROTECTION PROFILE

Object	:	E-passport : understanding the EAC protection Profile
Application	:	Date of publication
Diffusion	:	Public document, published on DCSSI Internet website (www.ssi.gouv.fr)

Courtesy Translation

SÉCURITÉ CERTIFICATION

Document Releases

Révision	Date	Modifications
1.0	24/10/2008	Creation

TABLE OF CONTENT

1. Context and purpose of the document

The protection profiles [PP BAC] and [PP EAC] were developed to specify the evaluation of e-passport product (Machine Readable Travel Document – in short : MRTD).

This application note aims to give adequate understanding of some particularities of the protection profiles, in order to ease the work of Security Target writers, and also aims to enforce homogeneity among all e-passport evaluations.

It also focuses on the points which are identified in [PP EAC] as requiring a decision from the certification body.

1.1. References

- [PP BAC] : Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application", Basic Access Control, reference : BSI-PP-0017, Version 1.0, 18th August 2005, BSI. Published on www.commoncriteriaportal.org[1] web site
- [PP EAC] : Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application", Extended Access Control, référence : BSI-PP-0026, Version 1.2, 19th November 2007. Published on www.commoncriteriaportal.org[2] web site
- [ICAO 9303 v1] : 9303 part 1 volume 1, Sixth edition, 2006, Passports with Machine Readable Data Stored in Optical Character Recognition Format. Obtainable on www.icao.int[3] web site
- [ICAO 9303 v2] : 9303 part 1 volume 2, Sixth edition, 2006, Specifications for Electronically Enabled Passports with Biometric Identification Capability. Obtainable on www.icao.int[4] web site
- [REF CRYPTO] : Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level version 1.10, 14th of September 2007, No. 1904/SGDN/DCSSI/SDS/LCR. Published on www.ssi.gouv.fr[5] web site
- [PUBLI] : Security and Privacy Issues in E-passports, By Ari Juels, David Molnar, and David Wagner
- [PP9911] : Protection Profile Smart Card Integrated Circuit With Embedded Software , version 2.0, June 1999. Certified by DCSSI under the reference PP/9911. Published on www.ssi.gouv.fr[6] web site

1.2. Life Cycle definition

The evaluation perimeter defined in the [PP BAC] and [PP EAC] protection profiles covers a large range of the product life cycle, starting from the design of the microcontroller and the e-passport application, and ending at the passport booklet manufacturing. This perimeter covers a large range of actors and trades, from microelectronics to paper production.

[1] http://www.commoncriteriaportal.org/files/ppfiles/PP0017b.pdf

[2] http:// www.commoncriteriaportal.org/files/ppfiles/PP0026_ma1b.pdf

[3] http://www.icao.int/icao/en/sales/index.html

[4] http://www.icao.int/icao/en/sales/index.html

[5] http://www.ssi.gouv.fr/fr/politique_produit/catalogue/pdf/mecanismes_cryptographique_v1_10_standard_uk.pdf

[6] http://www.ssi.gouv.fr/site_documents/pp/pp9911.pdf

The goal of the chapter 2 is to define what is the scope of flexibility when performing MRTD evaluation with a conformance claim to the protection profiles, in order to keep a relevant view of the MRTD security but also to make the evaluation practicable.

1.3. Intrinsic resistance of the BAC mechanism – Entropy of the MRZ data

ICAO specifications (reference [ICAO 9303 V2] § III LDS(Logical Data Structure) and §IV PKI(Public Key Infrastructure)) regarding e-passport product (MRTD) describe access control mechanisms to protect the data contained in the MRTD, including the personal data of the MRTD holder (biographical data and image of the holder's face digitally stored).

There are several levels of access control mechanism, begining with the named « Basic Access Control » (BAC) which allows the mutual authentication of the MRTD and the inspection system[7]. The authentication process is the following:

- The MRTD holder shows his passport to the inspection system;
- The inspection system reads optically the MRZ data printed on it;
- The inspection system computes, by derivation, the authentication key of the MTRD;
- The inspection system authenticates itself to the MRTD (contactless mode);
- If the authentication succeeds, the inspection system and the MRTD calculate a shared session key that will allow protecting further communications (secure messaging) during which the data contained in the MRTD are transfered.

The access control function protects the product from eavesdropping and skimming.

One particularity of this mechanism is that the key is static and can be derived from the MRZ data printed on the passport booklet. The protection profiles [PP BAC] and [PP EAC] both include this mechanism. The [PP BAC] is targeting a VLA.2 level (resistance to attacker with low attack potential), whereas the [PP EAC] is claiming a VLA.4 level (resistance to attacker with high attack potential). The problem is that the intrinsic resistance of the BAC mechanism, which is included in both PP, is weak due to the entropy of the BAC key, and therefore can not reach resistance level required for VLA.4.

The chapter 3 gives some technical elements to understand the resistance level of the BAC mechanism, and explains how the [PP EAC] addresses this point.

[7] inspection system is a system used at border control to read passports and to identify its holder .

2. Life Cycle definition

2.1. Comparison between [PP BAC]/[PP EAC] and [PP9911]

The life cycle described in both protection profiles [PP BAC] and [PP EAC] is clear and without ambiguity, and defines four phases, compared to some PP such as “Smart Card Integrated Circuit With Embedded Software Protection Profile” (see reference [PP9911]) which were identifying more phases with more steps corresponding to the different trades and actors involved in smartcard manufacturing.

Here is a comparison between [PP BAC]/[PP EAC] and [PP9911]:

[PP BAC] / [PP EAC]	[PP9911]
Phase 1: - Design of the IC and dedicated software, and associated guidance, - Development of the embedded application and associated guidance.	Phase 1: development of the embedded application and associated guidance.
	Phase 2: design of the IC and dedicated software, and associated guidance. Photomask fabrication.
Phase 2: - Production of the chip, chip identification data, - MRTD manufacturing, including: ▪ Pre-personalization: patch, activation of the application, loading authentication data for the personalization agent, ▪ Inlay manufacturing (antenna), ▪ Booklet manufacturing.	Phase 3: manufacturing and pre-personalization (transport key).
	Phase 4: IC packaging, testing.
	Phase 5: smartcard product finishing process, testing.
Phase 3: personalization of the MRTD (enrolment and loading of the holder characteristics).	Phase 6: personalization, testing.
Phase 4: operational use.	Phase 7: smartcard product end-usage, end of life process.

Considering the [PP9911] life-cycle, the evaluated product is the chip at the end of its manufacturing phase (end of phase 3 of the [PP9911] life cycle). Further phases are covered by guidance and testing.

Considering the [PP BAC]/[PP EAC] life-cycle, the evaluated product is by default the MRTD at the end of its manufacturing phase (end of phase 5 of the [PP9911] life cycle).

This is a major change compared to what is done within “usual smartcard” evaluation approach that was built in order to be consistent with business organisation in the fields of smartcard. By default, for the [PP BAC]/[PP EAC], that means to perform tasks such as analysis of the procedure and site audits of several actors (among which antenna suppliers and booklet manufacturer), though some of them may have no real impact on the security of the product. However, we may notice that in the updated version of the [PP EAC], version 1.2, the editor introduced more flexibility on the following points, and can be considered applicable for the [PP BAC] as well.

2.2. Considerations on e-passport application and pre-personalization

Regarding e-passport application, the protection profiles [PP BAC] and [PP EAC] consider that, from a technical point of view, phase 2 corresponds to:

- Loading any possible patch for the application in EEPROM,
- Creating MRTD application, which is not clearly defined besides,
- Loading MRTD chip with pre-personalization data (i.e. authentication key for the personalization agent).

All actors involved in these technical activities have to be covered by the evaluation task (i.e. ACM, ALC, ADO and AGD) however the "application note 5" on page 9 of [PP EAC] allows the following adaptations:

1. Depending on the e-passport development process, the “creation of the MRTD application” can be covered by guidance and analysed through ADO /AGD tasks, as long as the procedures describe exactly how to configure the application, and that this configuration process cannot decrease the security level of the product;
2. The actor responsible for patching the product has to be covered by the evaluation task (while evaluating the security of development environment). If patches are only loaded by the IC manufacturer, this may be already covered by the IC evaluation and then, there is no need to perform it again;
3. The actor, responsible for loading the key that ensures the product’s self-protection from the delivery until its use by the personalization agent, shall be covered by the analysis (while evaluating the security of development environment).

2.3. Considerations on the booklet

The booklet manufacturing (i.e. including the insertion of the inlay into the cover of the passport) has obviously no security impact on the information technology part of a MRTD, as long as the electronic chip is already self-protected during this phase (with an authentication key for instance).

With respect to the "application note 5" on page 9 of [PP EAC], there is therefore no need to include this part of the life cycle in the scope of evaluation (tasks related to the development environment).

2.4. Considerations on the antenna

The antenna of the chip has an impact on the electromagnetic field used to supply the chip with power, and to establish a communication channel between the chip and the terminal. This impact concerns in particular the analysis tasks in terms of “side channel”.

Some technical analysis show that the antenna behaves like a filter that can distort the desired information in the RF field, or even mask it in the worst case. The sensor used to measure the “side channel” effect has also an impact on the RF field.

However, in order to characterize the “side channel” through the contactless interface, it is always possible to probe the signal directly on the RF pad of the chip (with an appropriate test bench). The antenna is then emulated and the possible “side channel” effect is measured at the source without any modification of the raw signal by the sensor or the antenna. It is therefore the best case to make this characterisation.

So, if the product is resistant in such a situation, that means it will also be resistant with any antenna.

In such a case, as long as the evolution of the state of the art does not question itself that point, and with respect to the "application note 2" on page 6 of [PP EAC], we can assess the product without identifying a specific antenna (i.e. including the antenna in the TOE). So, there is no use verifying the conformance of antenna supplier to criteria dealing with development environment (DVS, ACM…).

3. Intrinsic resistance of the BAC mechanism – Entropy of the MRZ data

3.1. Analysis of the BAC intrinsic resistance level

The BAC key is derived from the MRZ data printed on the passport booklet with the following format (example taken from [ICAO 9303 V2], Appendix 7):

```
               P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
               L898902C<3UTO6908061F9406236ZE184226B<<<<<14
Colours:       RRRRRRRRRBVVVRRRRRRBVRRRRRRBVVVVVVVVV
```

The BAC keys of the MRTD is determined from the data in red in this document[8] (personalized data) and those in blue (“check digit”, with determined value), and allows calculating a common session key shared by the MRTD and the inspection system to encrypt their communication (secure messaging).

The first block of personalized data gives the passport number. The second block gives the date of birth of the holder and the third group gives the expiration date of the passport.

The possible values for these parameters and its associated entropy are described below for each group:

- According to ICAO specifications (cf. [ICAO 9303 V2]), passport number is made of 9 symbols taken from the alphanumeric set [a-z, A-Z, 0-9] that provide $9\times\log_2[(26 + 26 +10)]$=53,5 bits. But according to [ICAO 9303 V1] specifications[9], only upper-case letter shall be used and therefore, the entropy is only $9\times\log_2[(26 +10)]$ = **46,5 bits**;
- The date of birth of a person of at most 75 years provides: $\log_2(365*75)$=**14,7 bits**, but just observing the holder of the MRTD allows to reduce the entropy of the value;
- The expiration date is at most within the next ten years: $\log_2(365*10)$=**11,8** bits.

The total reaches a maximum of **73 bits**. This is **not** compatible with a **VLA.4** level according to the French rules about cryptography (cf. [REF CRYPTO]) which state that 80 bits at least is required until 2010 (and 112 bits beyond).

For some examples on how it is implementated in some countries, see Annexe A.

3.2. Consequences and conclusion for the [PP EAC]

In one hand, the [PP EAC] claims VLA.4 resistance level and, on the other hand, it also identifies logical MRZ data as assets to be protected, but these assests are only protected by the BAC mechanism.

However, an application note was introduced (see “application note 1” on page 6 of [PP EAC]) in order to interpret the PP and make evaluation task practicable.

As the logical MRZ data are printed on the MRTD booklet, for interoperability reasons, and as its entropy is quite low, they cannot be protected upper than VLA.2, even if the [PP EAC] targets a VLA.4 level.

[8] For the reader that doesn’t have a colour printed version of this document, the line « colour » gives the colour of each character (R=Red, B=Blue, V=green).

[9] see [ICAO 9303 V1], appendix 8, §9.4.1 page IV-14

The evaluation at VLA.4 level can then focus only on the sensitive biometric reference data and EAC mechanism (including Chip authentication).

Annexe A Passport number format in several countries

According to the study found in the referenced publication [PUBLI], the entropy of the BAC key for US passport is closer to 52 bits: the passport issued since 1981 have 9 digit numbers where the first two digits encode one of fifteen issuing offices and the remaining seven digits are assigned arbitrarily (although some offices presumably issue more passports than others). This gives a total entropy of at most log(15 x 10)+14+11 ~ 53 bits.

Other countries of the European Union, like Spain or Italy, seem to use a single capital letter and six digits. In this case, the total entropy is log(26 x 106)+14+11 ~ 51 bits.

In France, passport numbers are presently made of:

- two digits giving the year of the set, i.e. 10 possibilities. This gives $\log_2(10)$ = 3,3 bits. But as the year of passport manufacturing should be not far from the issuing date, this reduces the 10 years possibility to something like two year to guess the expiration date.
- two capital letters for the lot (excluding G, J, M, N, O, Q, S, U, W), i.e. 17 possibilities, providing $2*\log_2(17)$ = 8,2 bits,
- five digits with numeric character, providing : $5*\log_2(10)$ = 16,6 bits.

The expiration date provides then: $\log_2(365*2)$ = 9,5 bits.

Therefore, added with the date of birth that remains the same, the total entropy for French passport is 52 bits.