Introducing the PACE solution

Countries need to be aware of the need to replace BAC

by Dr. Jens Bender
& Dr. Dennis Kügler

In the early days of the e-passport, access control was a controversial issue. At the time, discussions didn't centre on the type of access control mechanisms to implement but on the need for access control at all. They culminated in the inclusion of an optional Basic Access Control (BAC) mechanism in the Technical Report PKI for Machine Readable Travel Documents offering ICC Read-Only Access, which was eventually included in Doc 9303 [1]. While every modern e-passport includes BAC, the time has come for a better, more secure solution.

Chips are included in travel documents for two reasons. First, they enhance the security of the actual document (a chip is a security feature in its own right). Second, they allow the passport holder's identity to be verified. To facilitate this functionality, ICAO opted for a contactless chip that complies with ISO 14443 requirements. These chips combine sizeable storage capacity with durability and interoperability; a combination that places contactless technology ahead of other storage devices such as bar codes or contact-chips. However, the use of a contactless system also entails an element of risk. The following risks need to be addressed:

- Skimming - retrieving data from the chip without being in possession of the passport and without the holder's approval. Skimming is an online attack (the attacker must communicate with the chip for the duration of the attack).
- Eavesdropping - data is intercepted while the passport chip communicates with the reader. As the data is analysed after the attack has taken place, eavesdropping is an offline attack.

To resolve the above threats, Doc 9303 includes the BAC protocol (see box 1) which was designed to protect less sensitive data. The level of protection offered by BAC is adequate but not overwhelming. The protocol was primarily developed with ease of implementation in mind. As such, BAC uses symmetric key device authentication, a technique that was readily available on ISO 14443 compliant chips when the e-passport was introduced. Chips offering asymmetric cryptography at a suitable speed were not available at the time. Neither was a standardized protocol.

In recent years, BAC has become the de facto standard for nearly all e-passports.

BAC weaknesses

Even though BAC is easy to implement and still offers suitable protection, if used correctly, it is a dated technique. Due to the use of symmetric cryptography, the strength (entropy) of the keys used to encrypt and authenticate the contactless communication, is held back by the limited strength of the MRZ-derived password.

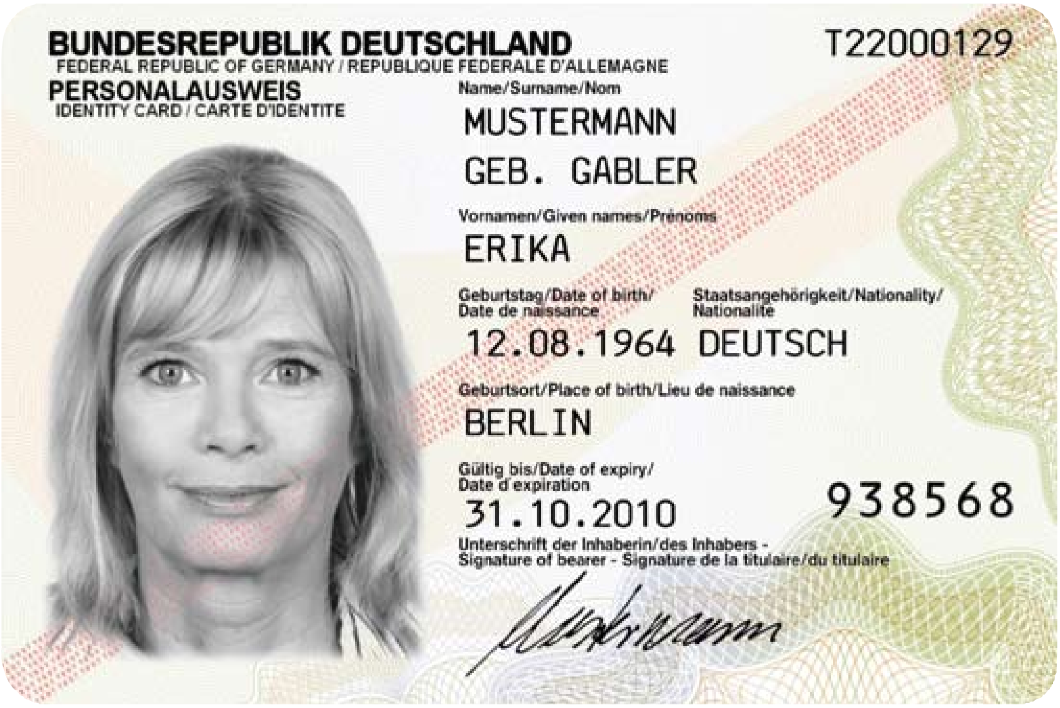
To overcome the above shortcomings, the BAC execution process should be slowed down, prolonging the time an attacker needs to be in contact with the passport chip. This countermeasure is already implemented in some passports. While it makes skimming harder, it obviously does not resolve the problem of eavesdropping. The time an offline attacker needs to launch a successful attack depends on the computing power at his or her disposal and the MRZ fields in use[1]. As explained in the separate box 2 entitled 'Entropy of the MRZ' there is no easy way to improve the strength (entropy) of the keys.

Deep Crack - a $ 250,000 computer built for the sole purpose of breaking the symmetric cipher DES - was able to process 88,000,000,000 DES keys per second when it was introduced in 1998 [2]. Another machine, COPACOBANA, achieved similar speeds of 48,000,000,000 DES keys per second and 65,000,000,000 DES keys per second in 2006 and 2008 respectively (at the cost of only $ 10,000) [3,4].

The above closely mirrors Moore's Law, which states that computing power per dollar doubles approximately every 18 months [5]. If we extrapolate the above data, a machine with the same computing power as Deep Crack or COPACOBANA will cost approximately USD 100 in 2019 (when a passport with a validity period of 10

__Dr. Jens Bender__ is a member of the section Official Electronic ID Documents of the German Federal Office for Information Security (BSI), working on e-passports and the German electronic ID-card, especially on specifications and international standardization.

__Dr. Dennis Kügler__ is the head of the working group responsible for developing security specifications related to electronic identity documents at the Federal Office for Information Security (BSI). Since 2003 he is participating in the International Civil Aviation Organization and contributing to international standardization at ISO.



BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE

T22000129

Name/Surname/Nom
MUSTERMANN
GEB. GABLER

Vornamen/Given names/Prénoms
ERIKA

Geburtstag/Date of birth/ Date de naissance
12.08.1964

Staatsangehörigkeit/Nationality/ Nationalite
DEUTSCH

Geburtsort/Place of birth/Lieu de naissance
BERLIN

Gültig bis/Date of expiry/ Date d'expiration
31.10.2010

938568

Unterschrift der Inhaberin/des Inhabers - Signature of bearer - Signature de la titulaire/du titulaire

Figure 1
A Card Access Number (938568) is printed on the frontside of the ID-1 size card.

years will expire, assuming it is issued today). It was already shown that COPACOBANA can be programmed to break MRZ-derived Triple DES keys with 33 bit entropy in only 18 seconds. Thus, in 2019, keys with entropy of 35 bit will be breakable in a few seconds at almost no cost.

Given the above, all issuing states should ensure that their e-passports contain BAC keys with an entropy of at least 40 bits (see box 3). As the BAC entropy is primarily affected by the document serial number, most countries will have to introduce randomly selected alphanumeric serial numbers to achieve sufficient security. Unfortunately most countries still use serial numbers that are assigned sequentially and therefore fail to provide sufficient entropy. Even if the numbering convention is changed, the maximum BAC entropy is approximately 50 to 60 bits. In other words, BAC still has to be replaced in about 5 years time, at most.

The solution: PACE

Asymmetric cryptography offers a viable alternative. To convey its introduction, the German Federal Office for Information Security (BSI) published the Password Authenticated Connection Establishment (PACE - see box 4) protocol in 2007 [6]. The protocol uses a weak password (possibly of low entropy), verifies the password, and generates cryptographically strong session keys.

Other protocols are also available, and these are collectively referred to as Password Authenticated Key Exchange (PAKE). Unlike other solutions - such as EKE, SPEKE or SRP - PACE was specifically developed to be suitable for elliptic curve cryptography - a highly efficient technology used by a rapidly growing number of countries - as well as standard cryptography. Moreover, the technology is patent free[2] and provides the highest possible level of security [7]. PACE offers several options which can be chosen upon by the issuing country:

- PACE can be used either with elliptic curve or standard cryptography (asymmetric key agreement method),
- is able to generate session keys for different symmetric ciphers (eg, Triple DES, AES-128/-192/-256) as well as message authentication codes (eg, Triple DES Retail-MAC, AES-CMAC) for secure communication, and
- supports several 'mapping functions', as described below.

Box 1

Basic Access Control

BAC uses the date of birth, the expiry date and the serial number retrieved from the MRZ to verify physical access to the passport and to generate session keys for the protection (encryption and authentication) of subsequent communications. The protocol is based on a mutual challenge-response sequence that relies on symmetric cryptography.

Box 2

Entropy of MRZ

The maximum entropy of the MRZ can be estimated as follows (based on used fields only):

- *date of birth: 365*100, assuming a maximum age of 100. This corresponds to 15 bits;*
- *expiry date: 12 bits, assuming a validity period of 10 years;*
- *serial number: 36^9 possibilities, assuming 9 alphanumeric random digits. This corresponds to 46 bits.*

Based on the above, the MRZ entropy is estimated at 73 bits at most. This theoretical maximum is never reached in practice (certain expiry dates aren't used; a correlation exists between the expiry date and the serial number in case of sequential numbering). Moreover, the age of the holder may be estimated.

Depending on the numbering convention used for the serial numbers, the authors estimate the practical entropy of the MRZ at between 50 bits (using alphanumeric, random serial numbers) and 40 bits (using sequential serial numbers).

Several ways of strengthening the BAC have been discussed over the years. These have centred on the use of additional fields within the MRZ. BAC requires these fields to be correctly read by an OCR system; any reading error will cause the system to fail. When BAC was standardized it was therefore decided to use only fields that contain a check digit and therefore correctly read. As BAC already uses all fields containing a check digit, the only viable alternative is to redefine the optional data field to include a random number plus a check digit.

Unfortunately, some countries already use this field. As a consequence, redefining this or any other field would interfere with the MRZ's backward compatibility.

The problem with strengthening BAC is that all proposed alternatives only improve entropy by small amounts. None addresses the fundamental weakness of BAC: its dependence on the entropy of the MRZ.

Further options could also be added without undermining backward compatibility. One of the core components of PACE is its so-called mapping function, which is used to map a random number to parameters used for asymmetric cryptography. Two mapping alternatives are currently defined:

- Generic Mapping, based on generic group operations. This can be generically adapted to all asymmetric cryptography systems and is easy to implement on smart cards.
- Integrated Mapping, whereby the random number is directly integrated in the parameters used for asymmetric cryptography. While this is easy to implement for standard cryptography, it requires more sophisticated algorithms for elliptic curve cryptography (like the new Hash2Point function developed by Thomas Icart [8][3]).

In contrast to BAC, PACE offers excellent protection against offline attacks.

An unoptimized prototype card[4] and a beta version of the Golden Reader Tool resulted in execution times of roughly one second. Of course, Moore's Law not only helps the attacker, it also benefits the passport chip and reader system. The PACE prototype, for example, can be processed as quickly as the existing German e-passport (2.2 to 2.3 seconds, on average, using the Golden Reader Tool). The PACE data retrieval sequence consists of reading the metadata (EF.COM, EF.SOD), the DG1 data (the electronically stored MRZ) and the DG2 data (the electronically stored image of the holder).

The Integrated Mapping is usually slightly faster than the Generic Mapping (the actual advantage depends on the choice of cryptographic domain parameters and card speed, among other variables). However, as is the case for all PAKE protocols, to protect against online attacks, PACE may require the use of additional countermeasures. Possibilities include slowing down the protocol - assuming it is executed too quickly - or limiting the number of password attempts[5].

Additional advantages

As the quality of the session keys does not depend on the complexity of the password, PACE can be used on the basis of passwords that are shorter than the MRZ. One alternative is a short, 6-digit Card Access Number (CAN), which is printed on the document. On ID-1 cards, which are issued by many countries, the MRZ is printed on the back, while the photograph, security features, etc. are located on the face. If the MRZ is used as the password, both sides of the card have to be read. This can be avoided if a CAN printed on the front side of the card is used (figure 1).

PACE can additionally be used to verify a personal PIN known only to the legitimate holder. This feature

Box 3

Future trend

2008	*2011*	*2014*	*2017*	*2020*
33 bit	*35 bit*	*37 bit*	*39 bit*	*41 bit*

MRZ - cracked for USD 10,000 in 20 seconds. The above estimates are based on the results achieved by COPACOBANA in 2008 and Moore's law.

is particularly interesting when combined with multi-purpose ID-cards (a travel document cum personal security token). PACE lifts the security of contactless ID cards to exceed that of contact cards.

The way forward

PACE is currently being standardized by ISO JTC1/SC17/WG3 [9], which supports ICAO in the ongoing development of Doc 9303. The protocol will be submitted to the ICAO TAG MRTD for approval by the end of the year (as soon as technical work has been completed). Once implemented as an ICAO standard, PACE will provide long-term protection against skimming and eavesdropping. That said, a migration period of several years will apply for reasons of compatibility (the actual period will be defined by ICAO).

Box 4

PACE Protocol

The PACE protocol comprises four steps:

1. ***The chip randomly chooses a random number, encrypts it with a password-derived key and sends the encrypted random number to the terminal, where it is recovered.***
2. ***Both the chip and the terminal use a mapping function to map the random number to parameters for asymmetric cryptography.***
3. ***The chip and the terminal perform a Diffie-Hellman protocol based on the parameters generated during step 2.***
4. ***The chip and terminal derive session keys, which are confirmed by exchanging and checking the authentication tokens.***

1 It should be noted, however, that eavesdropping on a legitimate communication without introducing reading errors is not easy.

2 The BSI has not applied for a patent on PACE, but cannot guarantee that no patents of third parties are affected.

3 The Hash2Point-algorithm is patented by Sagem. While Sagem announced to offer a free license in the area of identity projects, the precise conditions of licensing are not yet known to the authors at the time of writing.

4 Card provided by Bundesdruckerei/T-Systems, featuring TCOS Identity Version 1.0 beta 1, personalized with the standard "Mustermann" data set. Strong cryptography (elliptic curves with length 256 bit and AES-128), the Generic Mapping and an Extended Length buffer of 2 kBytes is used.

5 Limiting the number of tries opens the possibility of a DoS-attack and is therefore not possible for a passport.

References

[1] ICAO: Machine Readable Travel Documents - Part 1: Machine Readable Passports - Volume 2: Specifications for electronically enabled passports with biometric identification capabilities, ICAO Doc 9303 part 1, volume 2, sixth edition, 2006.

[2] Electronic Frontier Foundation, Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design. O'Reilly & Associates, July 1998.

[3] S. Kumar, C. Paar, J. Pelzl, G. Pfeiffer, and M. Schimmler: Breaking Ciphers with COPACOBANA - A Cost-Optimized Parallel Code Breaker, Proc. Eighth Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '06), 2006.

[4] T. Güneysu, T. Kasper, M. Novotny, Ch. Paar, Member, IEEE, and A. Rupp: Cryptanalysis.

[5] http://en.wikipedia.org/wiki/Moore%27s_Law, retrieved 02.07.2009.

[6] BSI: Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.01, May 2009.

[7] J. Bender, M. Fischlin, and D. Kügler: Security Analysis of the PACE Key-Agreement Protocol, Information Security Conference '09, Lecture Notes in Computer Science, Springer-Verlag 2009.

[8] Th. Icart: How to Hash into Elliptic Curves, Crypto 2009, Lecture Notes in Computer Science, Springer-Verlag, 2009.

[9] ICAO NTWG: Draft Technical Report: Supplemental Access Control.

If you would like to respond to the contents of this article, please send an email to kjd@keesing.nl