Security of electronic passports

Many countries have been issuing electronic passports for about a year, and the introduction of electronic passports started some controversial discussions. Let us consider some of the security features of electronic passports.

Worldwide standardization of the passports falls under the competence of the International Civil Aviation Organization (ICAO), a UN agency. Passports are described in the ICAO document 9303. The sixth edition of Doc 9303 introduces also electronic passports. Although the electronic part of the passport remains optional at the worldwide level, US have asked all its Visa Waiver Program partners to introduce electronic passports and the European Council decided that the introduction of electronic passports will be mandatory in EU member states (to be exact, this decision is not mandatory for the UK and Ireland and two non-EU countries – Norway and Iceland – decided to participate).

The difference between a traditional passport and an electronic passport (ePassport) is an embedded contactless chip (and the electronic passport logo on the front cover). The chip with an antenna is integrated into the cover or a page of the passport. The chip is a contactless smart card compliant to the ISO 14443 standard (both variants – A and B – are allowed). Technology based on ISO 14443 is able to communicate over distance of 0-10cm and supports also relatively complex cryptographic cards and permanent memory of kilobytes to megabytes. Herewith it differs from other RFID technologies that are capable to communicate over longer distances, but do not support more complicated operations other than sending a simple identification string. Higher communication layer is based on classical smart card protocol ISO 7816-4 (i.e., SELECT AID, SELECT FILE a READ BINARY).

The data in electronic passports are stored as files (elementary files in the smart card terminology) in a single folder (dedicated file). Up to 16 data files named as DG1 to DG16 (DG for Data Group) can hold the data. DG1 contains the data from the machine-readable zone (i.e. nationality, first name, surname, passport number, issuing state, sex, birth date, validity date, and optional data – for example a personal ID number), DG2 contains the photo of the passport holder (in JPEG or JPEG2000 and some additional metadata). DG3 is dedicated for fingerprints, DG4 may contain iris image. Remaining data groups contain information about the holder, issuing institution or passport itself. Two additional files with metadata are also present. The file EF.COM contains list of available data groups (and the information about versions used) and file the EF:SOD contains the digital signature of the passport data. The files EF.COM, EF.SOD, DG1 and DG2 are mandatory for all electronic passports. The data group DG3 will be mandatory in the EU states (see above) after 28th June 2009 (and will be protected by an additional mechanism). All other data groups are optional.

Data integrity (passive authentication)

The stored data integrity is protected by a digital signature stored in the file EF.SOD. The file structure is the usual SignedData of the CMS (Cryptographic Message Syntax) standard. The PKI hierarchy has a single level. Each country establishes its own CSCA (Country Signing CA), which certifies bodies responsible for issuing the passports (e.g. the state printers, embassies etc.). These bodies are called Document Signers. Data in the passport are then signed by one of these Document Signers.

To verify signatures, the CSCA certificates of the issuing country must be available and their integrity must be guaranteed. The certificate of the Document Signer is either directly stored

in the passport (in the certificates part of the SignedData structure – and this is mandatory in the EU) or must be obtained from other sources (the issuing country, the ICAO public key directory, etc.).

The signed data is a special structure containing hashes of all present datagroups in the passport. Integrity of each file can be verified separately (i.e., first the digital signature in EF.SOD is verified and then integrity of each file is checked by verifying its hash with the hash stored in the EF.SOD file).

The digital signature is one of the key security mechanisms of electronic passports – if not the most important one. Every country can choose a signature scheme (allowed schemes are RSA PKCS#1 v1.5, RSA PSS, DSA and ECDSA in combination with SHA-1 or any of the SHA-2 hash functions), that best fits its needs from the implementation and security perspective. Every inspection system (InS – a system that is able to retrieve information from the electronic passport and check/display/use the data) must naturally support all these schemes to be able to verify any valid passport. The signature verification is a relatively simple process, yet complications may arise due to a relatively high number of signature schemes that have to be supported, retrieval of the correct root certificates (CSCA) from all countries and CRLs (each country must issues one at least every 90 days).

It is clear that a digital signature cannot prevent making identical copies (including EF.SOD file with digital signature, so-called cloning). Therefore it is not possible to rely only on the data stored in passport, but it is necessary to inspect also the classical security features (security printing, watermarks, holograms, etc.) and namely the correspondence between the printed data and the data stored on the chip.

Active authentication (AA)

Cloning of passports can be prevented using a combination of cryptographic techniques and reasonable tamper resistance. A passport-specific asymmetric key pair is stored in the chip. Whereas the public key is freely readable (stored in DG15 and its hash digitally signed), the private key is not readable from the chip and its presence can be only verified using a challenge-response algorithm (based on ISO 9796-2). This process is called *active authentication* and it is an optional security feature of electronic passports (also for EU countries it only remains an optional feature).

The point of the active authentication is to verify whether the chip in the passport is authentic. The inspection system generates an 8-byte random challenge and using the INTERNAL AUTHENTICATE command asks the chip to authenticate. The chip generates its own random string and cryptographically hashes both parts together. The chip's random string and the hash of both parts (together with a header and a tail) are then signed by the private key. The result is sent back to the inspection system, which verifies the digital signature. If the digital signature is correct the chip is considered authentic. Possible attacks might try to focus on the tamper resistance of the chip or the analysis of side-channels.

An interesting privacy attack exists against the active authentication. If the challenge sent to the chip is not completely random, but rather specifically structured (for example encoding place and time), the inspection systems can store the challenge and response pair as a proof that the passport in question was at the given place at the given moment. In reality, such a proof would have to face the fact that the passport signs any arbitrary challenge at any place

and the evidence value is therefore very limited. Even so some countries decided not to implement the active authentication in their passports because of this privacy threat.

Passport holders will soon realize that the passport is in fact a powerful smart card. The use of the chip for digital signatures of documents is apparently insecure as the passport will sign anything without additional authentication, e.g., via PIN (moreover the challenge-response protocol is definitely not a suitable signature scheme). The utilization of the active authentication for user authentication (e.g., a computer logon) can be much more promising.

Basic Access Control (BAC)

Basic access control is a mechanism that prevents reading of the passport data before the authentication of the inspection system. The authentication keys are derived from data printed in the machine-readable zone. In particular, the document number, the holder birth date and the passport expiration date is used. All these items are printed in the second row of the machine readable zone and are protected with a check digit (OCR characters recognition is not error-free; hence the preference of fields with check digits). These three entries are concatenated in an ASCII form (including their respective check digits) and are hashed using the SHA-1 function. The hash value is then used to derive two (112-bit 3DES) keys for encryption and MAC authentication. The command GET CHALLENGE is consequently used to obtain the challenge from the chip. Then the inspection system and the chip mutually authenticate using the MUTUAL AUTHENTICATE command. A session key is established and further communication is secured using Secure Messaging.

BAC is based on a standard mutual authentication technique, which is considered to be secure as long as the keys are kept secret. In the case of electronic passports the keys are not secret in the classical sense as they are derivable from the data printed in the passport, but even so could prevent the random guess of the key. This is, however, slightly problematic as the data used to derive the key do not have enough entropy. Although the theoretical maximum is 58 bits and in case of alphanumerical document number even 74 bits, real values are significantly lower. Let us inspect the particular entries in more details:

- Holder's birth date: one year has 365 or 366 days, theoretical maximum is 100 years, i.e. around 36524 days total (15.16 bits of entropy). But the holder's age can be realistically estimated, say with a precision of 10 years (3652 days, 11.83 bits entropy), but often even more accurately.
- Day of expiry: maximal validity of passports is 10 years (therefore approximately 3652 days, 11.83 bits entropy). Passports of children can have a shorter validity (typically 5 years). In the nearest future we can exploit the fact that electronic passports have been being issued only for a very short period of time. To reduce the space we can also use the fact that passports are issued only on working days and the expiration date is directly connected with the day of issue.
- Document number: 9 characters are dedicated for the document number. Shorter document numbers must be padded with padding (<) characters and longer document numbers must be truncated. Document numbers consisting of digits only (and the padding character <) allow for the total number of 11^9 combinations (31.13 bits of entropy); if numbers can be alphanumerical then the maximum number is 37^9 combinations (thus 46.88 bits of entropy). These values can be accomplished only when the passport number is completely random. And that is often not the case. If certain information about the numbering policy of the particular country is known, the number of combinations and thus the entropy will decrease. Many countries assign sequential numbers to their passports. If we know the date of issue (or expiration

date), the number of possible passport numbers is small. For example a country with 10 million inhabitants issues around a million of passport a year. If the year of the issue and the range of the passport numbers are known, then the entropy drops to 20 bits. If the month of issue and its range of numbers are known, then the entropy further drops to 17 bits. We could go on to single days, but so detailed information probably will not be available to an average attacker. However, not only insiders but also hoteliers and doorkeepers may know a lot about the numbering policy (and such information will eventually be published on the Internet). The guess is a bit more complicated in practice, as we must first guess the issuing country and eventually also the passport type as different types may have separate numbering sequences.

- Every entry is followed by the check digit. The algorithm is publicly known and the check digit des not introduce any new information.

For estimation of the total entropy, we might sum the entropies of entries listed above. But that is correct only when entries are independent. We may debate about the expiration date vs. birth date as the people apply for the document at their 15th year and then almost regularly renew. This holds for personal identification cards, but does not have to be case for passports and thus we omit this influence. The same holds for the relationship between the birth date and the document number. But dependency between the document number and the expiration date typically will be present. There is no dependency only for completely random document numbers and then we can sum the entropies. Otherwise some dependency will be present and it is only the question of how much information about the numbering policy is known to the attacker. When the attacker has a significant knowledge, the total entropy can remarkably decrease. In theory, for sequential document numbers, country with the size of around 10 million people, uniformly distributed passports over whole year and detailed knowledge of the document numbers issued on particular day the entropy of document number can decrease only to 12 bits. Total entropy then decrease from 58 respectively 74 bits to approximately 32 bits. The brute-force key search can be then mounted against significantly smaller number of possible keys.

We can distinct two types of brute-force attack. Either the complete successful communication is eavesdropped and we try to decrypt it or we try to authenticate against the chip and then communicate with it. The advantage of eavesdropping relates to the possibility to store the captured data and then perform a quick off-line analysis. If the whole communication is eavesdropped, we can eventually obtain all transmitted data. The disadvantage is the difficulty of eavesdropping (i.e. the communication must actually be in progress and we must be able to eavesdrop on it).

The derivation of a single key from the authentication data, data decryption and the check of challenge take around 1 microsecond on a common PC. The brute-force search of the space of authentication data with a size of 2^{32} thus takes slightly more then one hour. The practical demonstration of such attack against Dutch passports was published by Marc Witteman in [5]. His attack utilized an additional knowledge about the dependency between document number and the expiration date and the knowledge of a next check digit within the document number. Similarly in UK the postmen who deliver electronic passports could remotely read the content of the electronic passport in an closed envelope as they might know the birthday of the recipient and can easily guess the document number and expiry day (because the passport is new).

As we already mentioned, eavesdropping of the ongoing communication is not an easy task. Intended communication range of devices compliant with ISO 14443 is 0-10cm. This does not necessary mean that an eavesdropping on longer ranges is not possible, but an attacker soon encounters a problem with low signal to noise ratio. Whereas the signal from the inspection system (reader) is strong and detectable on longer distances, eavesdropping of the data sent from the chip (transmitted using load modulation) gets harder with every foot of distance.

An on-line attack against the chip can search the key space in the same way, but a single verification of the authentication data is significantly slower – we must communicate with the smart card first and then we have to compute the MAC key and MAC code as well. A single verification then takes approximately 20 milliseconds for commercially available contactless readers and thus the attack is about 10 000x slower than an off-line attack.

While the entropy of keys' derivation data is significantly lower than the length of resulting keys, practical attacks are restricted by the difficulty of eavesdropping the data for off-line attacks and by the slow speed of the communication for on-line attacks.

It is necessary to realize that BAC does not restrict access to anybody who is able to read the machine readable zone. If you leave your passport at a hotel reception desk, BAC will not protect your data. On the other hand, at the moment there is not much additional information stored in chip than printed in the passport.

There are also other issues related to contactless communication technology where BAC cannot help. First of all it is possible to remotely detect the presence of passive contactless chips. Second even before the BAC it is possible to communicate with the chip (e.g. to start the BAC). Anti-collision algorithms need unique chip IDs to address the chips. These chip IDs are typically randomly generated each time the chip is powered, but some chips of type A use fixed chip IDs, which makes their tracking very simple. Similarly some error codes may leak information about the chip manufacturer and/or model, which might also increase the chances to guess the issuing state.

Extended Access Control (EAC)

EU passports will also store fingerprints (in DG3) at the latest after 28th June 2009. Fingerprints will be stored as images in the WSQ format (lossy compression optimized for images of fingerprints). As fingerprints are considered to be more sensitive data than facial images (their recognition capabilities are much better), reading of DG3 will be protected by an additional mechanism. This mechanism is called the Extended Access Control and its details have been recently finalized, but let us now look on possible theoretical principles of protecting sensitive biometric data in passports to better understand how the European EAC was designed.

Methods based on symmetric cryptography

If access control is based on symmetric cryptography then the data in passport can be either stored unencrypted and the access would be protected by authentication based on symmetric cryptography or the data could be stored encrypted and not protected by any additional access control mechanism.

A symmetric key would have to be different for each passport (to avoid problems when one of passports leaks the key). Keys can be either completely random or derived from a master key by a suitable diversification algorithm (e.g., the passport-specific key could be obtained by

encryption of the document number with the master key). We need at least one master key per country, more probably one key for each passport issuer (i.e., region, embassy, etc.) and the key has to be regularly (e.g., monthly, annually) updated (for the passports being issued). An inspection system then would need access to all keys necessary to access all valid passports (i.e., up to 10 years) for a number of countries. In case of off-line systems that would mean that a large number of highly sensitive keys would have to be stored in each inspection system (InS) and the compromise of a single InS would imply the current and future access to biometric data in all passports valid at time of the compromise. This situation is easier to manage with on-line systems. The keys would be physically secure; instead we would have to protect the access to central system. In case of unauthorized access to central server the recovery is relatively easy – it is sufficient to stop the unauthorized access.

The advantage of symmetric based authentication or encryption is low required computation power of the chip. Basic access control (BAC) is based on shared symmetric keys, we could design a similar protocol based on truly secret keys. When the data on the chip is stored in the encrypted form, there are no computational requirements on chip as the stored data is transparent for the chip and there is no need for any additional access control mechanism. This solution is secure if the secret keys are kept in secrecy (which is not trivial).

The disadvantage of symmetric methods is the high number of keys that have to be kept secret (and in the case of off-line systems even on each InS). Moreover, the secret keys have a long validity period and cannot be revoked. Gaining access to such keys would result in having access to all valid passports which have been issued so far (naturally only for those countries the compromised InS would be able to access). A clear security weakness of encrypting the data, but otherwise not protecting the access is the possibility of off-line brute force (possibly even parallel) attacks. This would be a significantly stronger weapon than an on-line guessing. However, this should still remain a theoretical threat only for a solid the key length and encryption algorithm.

Methods based on asymmetric cryptography

Another way to authenticate the InS is the use of the PKI. The goal is to reduce the number of secret (private) keys on inspection system side and to limit the possibility of misuse in the case of its compromise. Although there could be several alternatives how to implement the Extended Access Control with the help of asymmetric cryptography and PKI, we will follow the proposal of German BSI [8], which became the European EAC protocol.

Each country establishes a CV (Country Verifying) certification authority that decides which other countries will have the access to sensitive biometric data in their passports. A certificate of this authority is stored in passports and it forms the starting trust point (root certificate) for the access control. Other countries wishing to access sensitive biometric data (no matter if in their own passports or in passports of other countries), must establish a DV (Document Verifier) certification authority. This authority will obtain the certificate from all countries willing to grant access to the data in their own passports. This DV CA will then issue the certificates to end-point entities actually accessing the biometric data – the inspection systems.

Each passport stores a CVCA certificate of issuing country (e.g., the Czech Republic). If the inspection system (e.g., a Spanish one) needs to convince the passport that it is authorized to access sensitive biometric data, it must provide the DV certificate (the Spanish one in our case) signed by the proper issuing CVCA (Czech) and its own InS certificate (for that

particular InS) signed by the DV certification authority (i.e., Spanish in this case). After the passport verifies the whole certification chain it has to check whether the inspection system can access the corresponding private key. That is performed using a common challenge-response protocol. If the protocol runs well, the inspection system can access sensitive biometric data (the DG3 and/or DG4 files). This part of the EAC is called the Terminal Authentication (TA).

The above mentioned process can be slightly more complicated as the CVCA certificates are updated from time to time (by link certificates) and the bridging link certificates have to be provided (and verified by the passport) at first. The terminal authentication can be based on RSA (the PSS as well as PKCS#1 v1.5 padding is possible) or ECDSA, both in combination with SHA-1 or one of SHA-2.

In addition to the terminal authentication, the European EAC also introduces the Chip Authentication (CA) protocol, which eliminates the low entropy of the BAC key and also replaces active authentication, as access to the private key on the chip is checked (the public key is stored in DG14 and is part of the passive authentication). Let us have a look at these protocols in more detail.

Chip authentication

An inspection system reads the public part of the Diffie-Hellman (DH) key pair from the passport (supported are the classic DH described in PKCS #3 and DH based on elliptic curves (ECDSA) according to ISO 15946), together with the domain parameters (stored in DG14). Then the inspection system generates its own ephemeral DH key pair (valid only for a single session) using the same domain parameters as the chip key and sends it to the chip (using the command Manage Security Environment – Set for Computation – Key Agreement Template). The chip as well as the InS can then derive the shared secret based on available information. This secret is used to construct two session keys (one for encryption and the other one for MAC) that will secure the subsequent communication by Secure Messaging (and SSC (Send Sequence Counter – the message counter value utilized for protection against replay attack) is reset to zero). Whether the chip authentication ran successfully or not is only clear after sending and receiving the next command protected with the new session keys.

The result of chip authentication is the establishment of a new secure channel (low entropy BAC keys are no longer used) and check of the chip authenticity (active authentication does not have to be performed, but even so it can be supported by the passport to allow the verification of the chip authenticity to inspection systems that are not EAC specific and only recognize worldwide ICAO standards).

Terminal authentication

The InS must convince the chip at the terminal authentication that it is authorized to access sensitive biometric data on the chip. The starting point is the CVCA certificate, which is uploaded to the passport chip in the phase of (pre-)personalization. During the terminal authentication, the inspection system must provide a certificate chain starting with CVCA stored in passport and ending with a certificate of the InS (sent by commands Manage Security Environment – Set for verification – Digital Signature Template and Perform Security Operation – Verify Certificate). This certificate chain may contain also the linking certificates if necessary and (after their verification) the passport updates the CVCA certificate with a new one (due to a possible overlap of the validity periods of the CVCA certificates, there can be up to two certificates valid at the same time – in such case both are

stored in the passport). Remaining certificates (the DV certificate issued by the CVCA and the DVCA certificate issued for InS) are stored temporarily and serve only for the verification of the whole certificate chain. Once the chain verification succeeds, the passport obtains the public key of the InS and its access rights. Only two access rights are specified at the moment, these are reading access to DG3 (fingerprints) and to DG4 (iris scan).

After obtaining the public key of an InS it has to be verified if the InS has also the access to the corresponding private key. This is done using a challenge-response protocol. At first, the inspection system gets an 8-byte long random challenge (using the GET CHALLENGE command), signs it (in fact the concatenation of the passport number, random challenge and the hash of the ephemeral DH key of the inspection system (from the previous chip authentication) is signed). The signature is then sent to the chip for verification using the EXTERNAL AUTHENTICATE command. If the verification runs correctly, the inspection system is authenticated and may access DG3 or DG4 according to the assigned rights. Terminal authentication is not a mandatory part of the communication with the electronic passport. One can skip the terminal authentication if there is not intent to read the biometric data from the chip.

As the computational power of smart cards is limited, simplified certificates (card verifiable (CV) certificates) are used instead of common X.509 certificates. An interesting point is the verification of certificate validity. As the chip has no internal clock, the only available time-related information is the certificate issue date. If the chip successfully verifies the validity of given certificate issued on a particular day, then it knows that this date has already passed (or is today) and can update its own internal time estimate (if the value is newer than the one already stored). It is clear that if some CV CA or DV CA issues (either by a mistake, intentionally or as a result of an attack) a certificate with the issue date in a distant future, the passport will then reject valid certificates and will become practically unusable. For that reason, only the CVCA, DV and domestic InS certificates are used to update the internal time estimate.

Worldwide interoperability is not necessary for the extended access control as the sensitive data should be accessible only when agreements between countries exist. Then it is up to the countries to agree on technical details (naturally within boundaries given by the ICAO standards). The current leader in area of EAC is the EU, which designed (actually it was the German Federal Office for Information Security) a protocol for the EAC. EU discussions on technical details finished just recently, and the final version of the protocol was released in [X].

It is assumed that the protected biometric data will be initially accessible only among the EU member states. There have already been some speculations about involvement of countries like United States of America, Canada and Australia in the European extended access control system. Looking at the PKI structure of the EAC, it is clear that is up to each member state to decide what other countries will have the access to data in the member state passports.

While the chip authentication substitutes active authentication and also improves the security of Secure Messaging, the chip and terminal authentication protocols are not standardized by ICAO. Hence the protocols will be used only when both the passport and inspection systems support these protocols. If the passport (e.g., first generation passport) or inspection system (e.g., non-EU or even some older EU systems) are not supporting the protocol, then it is necessary to fall back and utilize common protocols standardized by ICAO in Doc 9303 (i.e.,

BAC and AA). It is also possible that some other countries (outside EU) will not consider the fingerprints and iris scans as a sensitive data and thus the data groups DG3 and DG4 in their passports will not be additionally protected.

Electronic passports introduce new problems with the means they address some issues, but we know quite well that no technology is completely perfect. It is necessary to take into account that the passport security is not based only on the electronic part, but also on the classical security features (secure printing and other protection techniques). The digital signature of the stored data certainly increases the security of these travel documents, but should not lead to complacency and to overlooking the need to check on other relevant aspects and issues.

Comment

The presented opinions are the private views of the authors and cannot be considered as the official position of European Commission, where one of the authors is currently working in Joint Research Centre (JRC) in Ispra, Italy.

References

[1] ICAO TAG MRTD/NTWG: Biometrics Deployment of Machine Readable Travel Documents, version 2.0. Including appendix A-J, http://www.icao.int/mrtd/download/documents/
[2] ICAO TAG MRTD/NTWG: PKI for Machine Readable Travel Documents offering ICC read-only access v1.1, http://www.icao.int/mrtd/download/documents/
[3] Kirschenbaum, I., Wool, A. *How to Build a Low-Cost, Extended-Range RFID Skimmer,* http://www.eng.tau.ac.il/~yash/kw-usenix06/index.html
[4] MiniMe (pseudonym), Mahajivana (pseudonym): RFID-Zapper, http://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN)
[5] Witteman, M. *Attacks on Digital Passports,* WhatTheHack, http://wiki.whatthehack.org/images/2/28/WTH-slides-Attacks-on-Digital-Passports-Marc-Witteman.pdf
[6] ICAO NTWG: PKI for Machine Readable Travel Documents Offering ICC Read-Only Access V1.1, http://www.icao.int/mrtd/download/technical.cfm.
[7] ICAO NTWG: Development of a Logical Data Structure – LDS for Optional Capacity Expansion Technologies, V 1.7, http://www.icao.int/mrtd/download/technical.cfm.
[8] BSI: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.0, TR-03110, http://www.befreite-dokumente.de/eingereichte-akten/tr-03110-eac-1.0/.
[X] Expected to be published in the nearest future