Preventing fraud in ePassports and eIDs

Security protocols for today and tomorrow

by Markus Mösenbacher, NXP

Machine-readable passports have been a reality since the 1980s, but it wasn't until after 2001, in the wake of the terrorist attacks of September 11 in the US, that development of ePassports really shifted into high gear. Today, there are more than 100 countries with ePassport systems in place or in the works, and the contactless technology they use is also being introduced to other types of government-issued ID documents.

One of the main advantages of ePassports is their high level of security, which makes them hard to counterfeit and thereby reduces the risk of fraud. But identity thieves and other criminals are determined and cunning, so security is always an evolving standard. At the same time, ePassports are becoming more sophisticated. They can store more information and can even work with biometric data such as fingerprints and iris scans. This higher level of sophistication also adds to the demand for better security. These factors have lead to the creation of multiple security mechanisms, each with its own set of features and advantages.

Having different security mechanisms in use worldwide can create a challenge for the ID infrastructure, especially since government-issued IDs are typically valid for many years. The average lifespan of an ePassport, for example, is five to ten years. That means the infrastructure has to keep current with the latest standards but also support legacy standards while the cards that use them are still in circulation.

This paper looks at the security mechanisms currently in use or on the immediate horizon, and summarizes the design considerations for each.

The basic landscape

As shown in Figure 1, there are three generations of security mechanisms either in use or coming soon. The first ePassports, officially introduced in 2005, used a first-generation security mechanism called Basic Access Control (BAC), defined by the International Civil Aviation Organization (ICAO) in DOC 9303. In 2009, the German Federal Office for Information Security (BSI) introduced a second-generation security mechanism, Extended Access Control version 1 (EACv1), which has since been upgraded to version 2 (EACv2). And, in 2014, the third generation is scheduled to launch: the Supplemental Access Control (SAC) mechanism, a new mechanism defined by the ICAO in 2010 and based on Password Authenticated Connection Establishment (PACE), a protocol for generating keys for secure messaging.

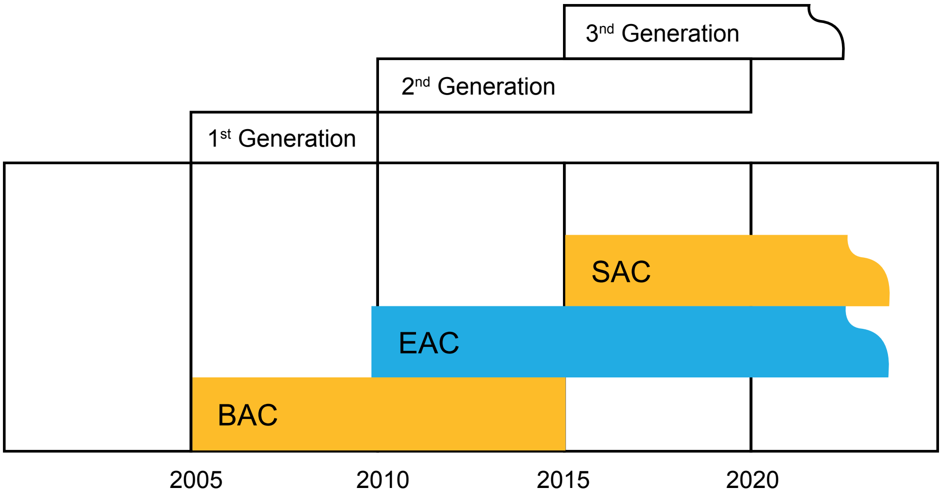

Figure 1 Evolution of ePassport security mechanisms

ePassports are equipped with a standardized logical data structure (LDS) that is used to program the chip and store data. The simplest LDS stores a facial image and very basic data. As the LDS has evolved over time, it has grown more sophisticated, and today can store a range of items, from biometric data like fingerprints and iris scans, to card-reader data and other travel information.

1st Generation - BAC (2005 – 2009)

The majority of ePassports in use today use the BAC security mechanism. The BAC LDS supports storage of a high-res facial image; it does not support biometric data.

The BAC protocol

The BAC protocol is specified in ICAO DOC 9303. BAC prevents reading the passport without the physical access to the travel document. The information stored in the passport is protected against eavesdropping (the act of secretly listening to the conversation between chip and terminal) because the communication is secured by a symmetric key. First, a symmetric key is derived from the machine-readable zone (MRZ) for mutual authentication, then a session key is generated out of the MRZ. The terminal uses an optical character recognition (OCR) reader to read the MRZ and derive the keys. The session key is used to encrypt the data exchange between passport and reader. BAC does not secure the chip against cloning. Another limitation of this technology is that the entropy of the key source (MRZ) is low, and it does not change. No PKI infrastructure is required for BAC.

Passive Authentication (mandatory in ICAO)
This step verifies the authenticity of the data stored in the security IC. The data is digitally signed by the issuing country. This mechanism does not prevent cloning of the chip. A PKI infrastructure is required. However, asymmetric cryptography is not required on the ePassport itself. Digital signature verification is done by the background system of the inspection device.

Active Authentication (optional in ICAO)
Protects the data against cloning. Each chip has stored a diversified key which is not accessible by the reader. The security IC contains a public key. The chip signs the challenge with its secret key which is then verified by the terminal by using the public key of the chip. No PKI infrastructure is required since the public key is accessible by the reader and the secret key is stored in a secure area which cannot be cloned.

Combination of measures for data transaction:

- Basic Access Control - generates keys for secure messaging
- Secure Messaging
- Passive Authentication – checks if data of passport has been manipulated
- Active Authentication (optional) – checks authenticity of passport
- Reading of data groups – terminal is enabled to access to data groups

2nd Generation – EACv1 (2009 – 2014)

The Extended Access Control (EAC) security mechanism introduces the ability to support biometric data such as fingerprints and iris scans. Developed in Germany by BSI, it was approved by EU Article 6 in June 2006. According to ICAO, EAC is not mandatory but is recommended to protect biometric data.

EAC does not replace the BAC scheme. EAC is an additional mechanism for securing biometric data. The facial image can be still retrieved via BAC. The EAC mechanism includes chip authentication and terminal authentication.

Chip Authentication:
Like active authentication, chip authentication is used to protect against cloning attacks. Additionally, chip authentication establishes a secure connection between chip and terminal. The chip of an ePassport stores an individual static RSA key pair. The private key cannot be accessed by the terminal. The terminal generates an ephemeral key pair. The chip individual key pair is used for key agreement on the session key, which transfers the biometric data. During key agreement the chip is implicitly authenticated.

Terminal Authentication:
Terminal authentication ensures that only authorized terminals can access the biometric data. The ePassport chip stores the Country Verifier Certification Authority (CVCA) certificate. The CVCA certificate is generated and stored in the ePassport chip when the ePassport is personalized by the issuing country.

During terminal authentication, the terminal sends a terminal certificate to the ePassport chip, along with the CVCA certificate and any other certificates in the hierarchy. This enables the chip to verify the terminal certificate. If all certificates of the certificate chain are verified up to the CVCA certificate, the terminal is trustworthy to the chip. The terminal certificate is a certificate which is provided by the Document Verifier Certification Authority (DVCA).

To ensure that the certificate sent by the reader is genuine, the chip sends a random number to the terminal. The terminal signs the number and returns it to the chip. With the public key of the terminal (which is part of the terminal certificate), the chip can check the signature over the random number to prove that the terminal certificate belongs to the terminal with the corresponding private key. This complex mechanism requires a PKI infrastructure.

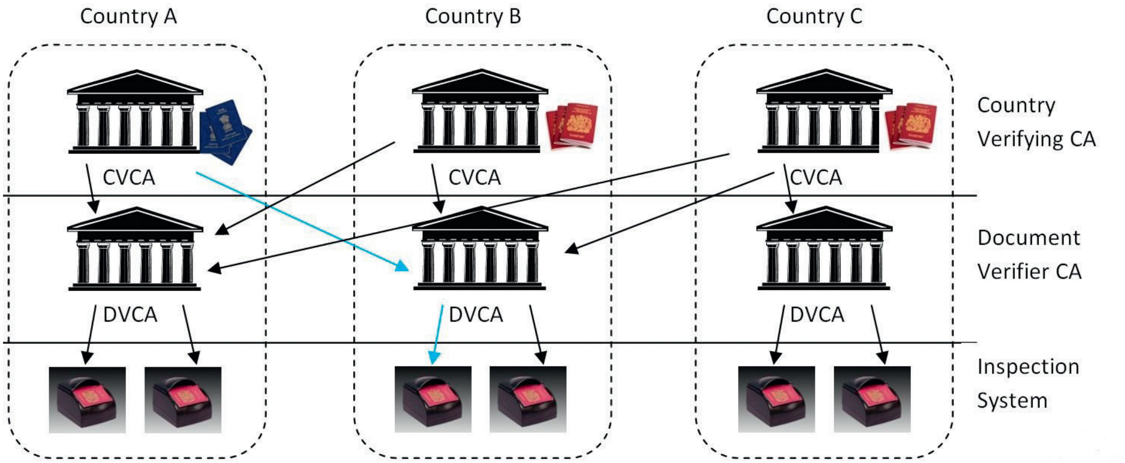

Figure 2 Example of PKI infrastructure (example: arrows in color)

Figure 2 shows the example of a PKI infrastructure to support EAC. The CVCA certificate of the issuing country A is stored in the chip of all passports of country A during personalization. This certificate is used to verify the terminal during authentication. Country A permits country B to access the fingerprint data of the passport issued by country A. The DVCA of country B provides the suitable terminal certificate (e.g. a certificate signed by the CVCA of country A), to the inspection system of country B. Country B is now enabled to read passports from country A.

Combination of measures for data transaction:

- Basic Access Control - generates keys for secure messaging
- Secure Messaging
- **Terminal Authentication – proves to the security IC that the terminal is allowed to access the IC**
- Passive Authentication – checks if data of the passport has been manipulated
- **Chip Authentication – proves authenticity of security IC (same mechanism as active authentication as defined in ICAO)**
- **Secure Messaging - uses session key generated during chip authentication**
- Reading of data groups – enables terminal to access data

EACv2:

EACv2 ensures that only authorized terminals can access the ICAO-mandatory data groups (DG1 – personal data text, DG2 – encoded face, SOD). ICAO-mandatory data groups must be readable by countries that are not implementing EAC. Therefore, EACv2 is not used for ePassports due to compatibility reasons. EACv2 is primarily used for eID (electronic identification) cards.

3rd Generation (starting with December 2014)

In 2010, to ensure the security of ePassports for the next 10 to 20 years, ICAO introduced the new Supplemental Access Control (SAC) mechanism (ICAO, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, 2010). SAC is based on the version 2 Password Authenticated Connection Establishment (PACE) protocol.

According to the European Commission Decision, which amends Commission Decision C(2006) 2909, PACE v2 methods that meet the ICAO standard (ICAO, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, 2010) must be implemented by EU countries by the end of 2014.

Main changes with SAC

Like BAC, SAC ensures that the passport can only be read when there is physical access to the travel document and generates session keys used for communication between ePassport and terminal. The main difference between SAC and BAC is that SAC uses asymmetric cryptography (Diffie Hellman Key agreement) to generate the symmetric session keys.

Using BAC is still a fairly safe way to secure the communication between electronic passport and inspection systems, but due to increasing computing power and BAC's relatively low entropy, it will become easier for eavesdroppers to hack the encrypted communication information. SAC improves the security of the communication interface so much that it eliminates the disadvantages compared to contact-based solutions.

While BAC derives the session key directly from the MRZ of the passport, SAC uses a password with possibly low entropy (CAN – Card Access Number, 6 bit) to generate the session keys. It uses a Diffie Hellman key agreement based on asymmetric cryptography technology. The quality of the session key of

SAC is independent on the entropy of the CAN, while BAC is dependent on the entropy of MRZ which is rather low. This is the main advantage of SAC. The 6-digit CAN can be derived from the MRZ or it can be printed separately on the holder page of the ePassport.

Changes for OS implementation and personalization

Overall, the changes required for SAC are marginal compared to the security improvements it delivers. The main change is the requirement to use Diffie Hellman key agreement according to the ICAO specification (ICAO, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, 2010).

During the migration phase, it is recommended to use BAC and SAC together, with SAC being the preferred option. During personalization, the CAN and SAC data need to be stored on the ePassport chip. The CAN data must also be printed on the security document.

Combination of measures for data transaction:

- **PACE - generates keys for secure messaging using asymmetric encryption**
- Secure Messaging – using key generated by PACE
- Terminal Authentication – proves to the security IC that the terminal is allowed to access the IC
- Passive Authentication – checks if passport data has been manipulated
- Chip Authentication – proves authenticity of security IC (same mechanism as active authentication as defined in ICAO)
- Secure Messaging - uses session key generated during chip authentication
- Reading of Data Groups – enables terminal to access to data

Certification

The ICAO does not require that ePassports be certified before use, but certification is a highly recommended practice. As shown in Figure 3, each security mechanism is supported by a protection profile for Common Criteria (CC) certification.

Protection Profile	BAC	EACv1	EACv2	PACE2	Comment
PP0055b	X				
PP0056b	X	X			
PP0056 v2		X		X	For PACE this protection profile refers to PP0068 v2b
PP0068 v2b				X	

Figure 3 Overview of Protection Profiles

All the protection profiles can be found on the BSI website:
https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/TRundSchutzprofile/trundschutzprofile_node.html

Conclusion

The infrastructure for ePassports has to be equipped to support evolving standards for security and new kinds of data, including biometrics. At the same time, the infrastructure has to retain its support for previous standards, since ePassports that were issued many years ago may still be in current use. This need to combine next-generation technology with legacy standards can be challenging. Having a clear understanding of security mechanisms – those in use today and those scheduled to come online in the next few years -- is an important first step in meeting this challenge. Partnering with a technology leader, especially one with experience implementing ePassport schemes worldwide, is another way to ensure that the ePassport infrastructure meets short- and long-term needs.

NXP for eGovernment: Leadership & innovation

NXP Semiconductors holds the number-one position in eGovernment. NXP is involved in more than 80 percent of all ePassport schemes worldwide, and of the 103 countries currently using ePassports, 87 of them have deployed NXP's SmartMX chip technology.

Building on its leadership in the market for contactless security ICs, NXP provides governments with a proven security solution that can be used within a variety of eGovernment projects. In addition to ePassports, NXP’s technology is involved in a number of domestic ID projects including national ID cards, health cards, vehicle registration, and driving licenses.

Originally launched in 2004, the biometric passport was intended to improve the level of security at border controls and to provide greater security against counterfeiting and fraud. NXP has a proven track record in offering eGovernment solutions that provide the strongest protection of sensitive private data, and deliver the highest performance in terms of transaction speed, power consumption, interface options as well as convenience for end-users.

In 2005, NXP was the first silicon supplier to have a contactless security chip, the P5CD072, compliant with the ICAO BAC requirements for ePassports and CC certification level EAL5+ by the German Federal Office of Information Security. In 2007, Building on the strength of the original product, the company launched a new IC into the SmartMX family, the P5CD080, which became the first EAL5+ certified chip in the industry fully supporting the ICAO EAC specification. In 2008, NXP launched the successor product EAL5+ certified P5CD081 controller with even higher performance, fully supporting SAC. The latest flagship NXP introduced in 2012 is the SmartMX2.

The SmartMX2 family follows on the proven reliability and interoperability of SmartMX with a further optimized feature set. It introduces the Integral Security™ architecture with over 100 security features as well as combining powerful co-processors for the highest levels of performance. SmartMX2 provides a new level of RF excellence to support contactless and dual-interface solutions. Since SmartMX2 comes with a CC EAL 6+ certificate for the majority of family members, customers can rely on an unprecedented level of security provided with this new secure microcontroller platform.

Glossary

AA	Active Authentication
BAC	Basic Access Control
BSI	Bundesamt für Sicherheit und Informationstechnik (German Federal Office for Information Security)
CAN	Card Access Number
EACv1	Extended Access Control version 1.11
EACv2	Extended Access Control version 2
EU	European Union
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
MRZ	Machine Readable Zone
OCD	Optical Character Recognition
PACE	Password Authenticated Connection Establishment
SAC	Supplemental Access Control

Bibliography

BSI. (March 2012). Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 v2.1 – eMRTDs with BAC/PACEv2 and EACv1. (p. 24). BSI.

BSI. (March 2012). Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2 v2.1 – Extended Access Control Version 2 (EACv2),Password Authenticated Connection Establishment (PACE),and Restricted Identification (RI). (p. 26). BSI.

BSI. (March 2012). Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 v2.1 – Common Specifications. (p. 83). BSI.

BSI. (n.d.). BSI Homepage. Retrieved from https://www.bsi.bund.de

ICAO. (2005). DOC 9303 part 1- volume 2. ICAO (p. 131). ICAO.

ICAO. (2010). Technical Report, Supplemental Access Control for Machine Readable Travel Documents. ICAO (p. 33). ICAO.

Schmeh, K. (2009). Elektronische Ausweisdokumente. Munich: Hanser.

www.nxp.com

Date of release: February 2013
Document order number: 9397 750 17377
Printed in the Netherlands