Moving to the third generation of electronic passports

A new dimension in electronic passport security with Supplemental Access Control (SAC)

FINANCIAL SERVICES & RETAIL

ENTERPRISE

GOVERNMENT > WHITE PAPER

TELECOMMUNICATIONS

TRANSPORT

gemalto
security to be free

Gemalto in brief

Gemalto is the world leader in digital security with 2010 revenues of €1.9 billion and 10,000 employees operating out of 87 offices.

In the public sector, Gemalto provides secure documents, robust identity solutions and services for governments, national printers and integrators in more than 60 government programs worldwide.

Gemalto contributes to over 25 ePassport programs around the world. The company serves its clients with secure travel documents, solutions and managed services, covering enrolment, issuance and complementary applications like e-Verification.

Executive Summary

Recognizing that electronic passports (ePassports) need to be protected for at least the next 10 to 20 years, the International Civil Aviation Organization (ICAO) is introducing Supplemental Access Control (SAC), an additional security mechanism for the next generation of documents.

The ICAO and the European Union (EU) have recently decided to enforce the use of this mechanism for all travel documents issued as of December 2014. As the industry moves forward, it is clear that countries have to start thinking about how to manage the approaching SAC migration in travel documents and associated systems.

Overall, new benefits for governments and citizens are tangible and the impact on the whole process from issuance to border control is minimal. SAC brings additional benefits to citizens and authorities by improving the security level thanks to asymmetric cryptography and by harmonizing security processes for electronic documents (ePassport, eResident permit but also eID). The Card Access Number (CAN) is also something brand new and very powerful. It allows reading the data with a six-digit number (potentially printed on the datapage) and is an alternative to the Machine Readable Zone (MRZ) reading. CAN opens the door to a much cheaper way to control documents as MRZ readers are no longer necessary. The inspection officer has just to key-in the six digits and to present the document to the contactless reader.

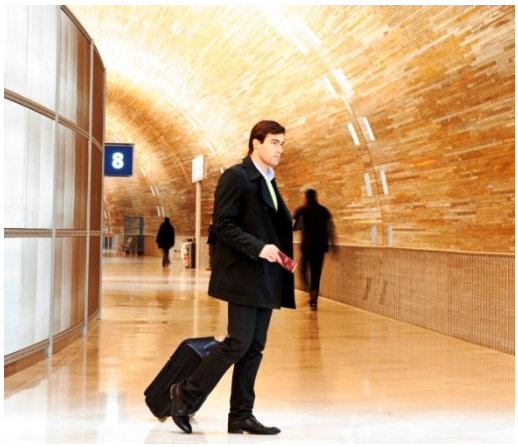
However, passport issuers must be vigilant when searching for the right partner. To guarantee a smooth migration to SAC and ensure full interoperability compliance, it is important to select partners and suppliers with long-standing experience of the travel market and a proven track-record in ePassport migrations.

Gemalto is one such supplier, active in the ePassport market since 2005. The company provides technologies and services to over 25 national ePassport programs around the world and is geared up to help you succeed in your migration project.

ePassport evolution

ePassports are biometrics-enhanced machine-readable travel documents (MRTDs) based on specifications defined by the ICAO. They were introduced with the aim of strengthening international border security by preventing illegal immigration and trans-border crime as well as reducing the threat of identity theft.

ePassports incorporate a contactless microprocessor chip, on which information about the passport holder is stored. This may include their biographic data such as their name, date and country of birth, as well as their biometrics including facial image, fingerprints and iris pattern. This data can be read from the passport using a contactless reader.



A travel document has a lifespan of 5 to 10 years

While contactless technology is well suited to border control and international interoperability, contactless communication is inherently vulnerable to threats such as skimming and eavesdropping. Since the first generation of ePassports was issued, several security schemes have been developed to protect passport holder privacy, anonymity and personal data.

As a travel document has a lifespan of 5 to 10 years, one of the major challenges for the whole industry is to protect the holder's data with reliable security mechanisms for the full length of its intended operational life. There is continual investment being made into producing secure identification that combats the ever-growing threats of international terrorism, illegal immigrating and organized crime.

> The ePassports generations

The first generation of ePassports appeared in November 2004. This followed the publication of a set of technical requirements by the ICAO, which defined the cryptographic protocols to be used to ensure an ePassport's data integrity and authenticity.

The EU Council's December 2004 regulation n° 2252/2004 delivered the roadmap for passport and travel document security features and biometrics. Since August 2006, all 27 EU member states have used this new technology and issued passports containing an embedded security microcontroller with a contactless RF interface (ISO/IEC 14443) combined with at least one biometric feature: the facial image of the holder.

First generation ePassports are based on Basic Access Control (BAC), a mechanism that was introduced to prevent skimming and eavesdropping and to ensure that the data stored in the ePassport microprocessor chip is read in a secure way. BAC protects the biographic data and facial image – the same data that is visible on the ePassport data page and which is thus considered less sensitive.

BAC is based on a symmetric protocol and the authentication relies on the data provided in the MRZ on the data page. Before access to the chip is granted, the chip and the reading device mutually authenticate themselves using a specific authentication key that is derived from the MRZ. The MRZ is also used to generate the session keys used to encrypt the data exchange between the chip and the reading device.

Today, BAC is used in almost every ePassport in the world (more than ninety countries now issue ePassports), and it is an ICAO-recommended feature for privacy protection.

In 2006, the EU asked all member nations to include on their ePassports additional digital biometric information, in particular, fingerprint biometric data. This ushered in the second generation of ePassport by mid-2009. It was clear that a new security mechanism, Extended Access Control (EAC v1.11), was necessary to protect this data. EAC restricts access to highly sensitive biometric data (fingerprints and iris) to authorized parties only and adds functionality to verify the authenticity of the chip (chip authentication) and the reading device (terminal authentication). EAC is based on an asymmetric protocol and uses stronger encryption.

The advent of the third generation of ePassports sees the introduction of a new security mechanism, Supplemental Access Control (SAC), which aims to overcome the limitations of BAC. While BAC is still considered an adequate access control mechanism, it is clear that the randomness of the keys that are dependent on the MRZ no longer sustains modern threats for very long. It is therefore important to anticipate and prepare for a new generation of ePassports that combat the ever-increasing attempts at fraud to ensure long-term security.

Why SAC, what for and its impacts

> Supplemental Access Control (SAC)

SAC is an evolution of BAC aimed at ensuring future-proof security in electronic travel documents. It is similar in function to BAC and ensures that the contactless chip cannot be read without physical access to the travel document and that the data exchange between the chip and the reading device is encrypted.

Due to its simplicity, BAC turned out to be a very successful protocol and it is now used in almost every ePassport.

Unfortunately, BAC's level of security is limited by the protocol's symmetric (secret key) cryptography design and there is no straightforward way to strengthen it. A cryptographically strong access control mechanism must also use asymmetric (public key) cryptography.

While BAC is still a safe way to protect data, as security levels are ramped up to meet the evolving threat posed by eavesdroppers and hackers with access to greater computing resources, SAC offers dramatic advantages over first-generation techniques.

One security option considered was simply to increase the key parameter size to a level appropriate for another decade of use. The other option was to take advantage of the past 30 years of public key research and analysis and move away from first generation symmetric cryptography and on to elliptic curve cryptography.

Elliptic curve cryptography is a public key encryption technique based on elliptic curve theory (an equation with specific properties). It is used to create faster, smaller, and more efficient cryptographic keys. Elliptic curve cryptography generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

According to some researchers, this method can yield a level of security with a 164-bit key that other systems such as RSA require a 1,024-bit key to achieve. Because this cryptography helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. Many manufacturers, including 3COM, Cylink, Motorola, Pitney Bowes, Siemens, TRW and VeriFone, have included support for elliptic cryptography in their products. source: www.whatis.com

The major advantage of SAC is that the security level is independent of the strength of the password used to authenticate the terminal and generate the keys for secure messaging.

It is based on Password Authenticated Connection Establishment (PACE v2). During the authentication phase, it implements asymmetric cryptography and bases data encryption on a shared key between the reading device and the chip. Data confidentiality is thus enhanced and eavesdropping becomes impossible.

Thanks to SAC the data is strongly protected both when stored on the chip and when transmitted to the reading device, and provides a superior level of security compared to BAC.

Resident cards and ePassports will both benefit from SAC

Key challenges for passport manufacturers and border control authorities

With the December 2014 ICAO/EU deadline for implementing SAC in travel documents fast approaching, it's important to examine the effects this will have on the documents themselves and related infrastructure. To be effective, SAC impacts on passport manufacturing, personalization and border control systems. Enrolment will remain untouched with the same data needing to be captured.

SAC implementation will require action from governments and border control authorities. However, for the traveler the SAC upgrade will be completely seamless and the experience at the border control will remain the same as today.

> The impact on passport manufacturing

Governments must get ready for the forthcoming SAC migration and plan the sourcing of SAC-enabled ePassport applications carefully.

The ICAO Technical Report on SAC defines various implementation options, such as the mappings, algorithms and passwords (six-digit CAN in additional to MRZ) available within the SAC framework. This means that each application developer may offer different sets of features. From the ePassport issuer's point of view, an extensive feature set allows maximum flexibility and the possibility of migrating to higher security levels during the passport's lifespan of up to 10 years.

Furthermore, it is advisable to use an ePassport application that is designed to be used in BAC, SAC and EAC modes thus enabling smooth migration from one security mechanism to another. Issuers do not need to worry about areas such as supply chain and stock management when the configuration is updated at the issuance stage.

> The impact on personalization

Personalization of the SAC authentication mechanism has an impact on the issuance system at three levels:

- The data preparation system needs to be updated to handle SAC. This new information for SAC is the security data that will be used subsequently at border controls when the document is authenticated. It is mainly algorithms eg key agreement, symmetric cipher and MAC, domain parameters eg Diffie-Hellman or Elliptic Curve Diffie-Hellman) and the password. The password can either be generated based on data in the MRZ (already exists for current BAC-compliant ePassports) or a six-digit CAN.

- SAC data have to be personalized on the document. This consists of the password (MRZ or CAN) graphical personalization and the SAC security information (mainly algorithm, domain and password) electrical personalization. Password graphical personalization has a very limited impact on issuance as the MRZ is already printed and CAN printing is typically configurable. SAC security information electrical personalization involves creating an elementary file and data object in the chip to store SAC information securely. This is handled usually by a personalization program in the personalization device. If personalization equipment does not need upgrading, the personalization script needs to be updated to handle this new chip file and object creation.

- The post-personalization quality controller operating at the issuance level may need to be updated as well to perform SAC authentication between it and the document. This is the most significant and sensitive modification required. Indeed, several authentication algorithms based on Elliptic Curve Diffie-Hellman could be implemented to verify that the personalized document can be authenticated successfully. Nevertheless, it will only impact the software component, meaning that there is no need to change readers. Standard readers will still read SAC eDocuments.

The post-personalization quality control stations will need to be updated as well to perform SAC authentication

What about issuance system performance?

- The implementation of SAC does not have a major impact on the overall issuance process. If state-of-the-art personalization technologies are being used, no significant impact is noticed at data processing level.
- For electronic personalization, programming the SAC information into the chip costs about 10% more than BAC. Equally for quality control operations, it will take 10% longer to perform SAC-enabled ePassports compared with BAC-only ones as both mechanisms are tested.
- Thus introducing SAC will not have noteworthy impact on the ePassport delivery lead time to citizens.

> The Impact on border control and verification systems

Although the border control inspection system for SAC-enabled travel documents is similar to BAC, it does need updating. When a travel document is presented, the inspection system must choose whether to use SAC or BAC. BAC will still be supported for global interoperability and backward compatibility reasons and the two security mechanisms will coexist for some time. However, the reading device should always use SAC if it is enabled on the passport.

The first data group – DG1 – contains the textual information about the passport holder that is printed on the data page and coded in the MRZ. It contains facts such as the name, date of birth, gender of the holder, and as well as the document number, the issuance and expiry dates.

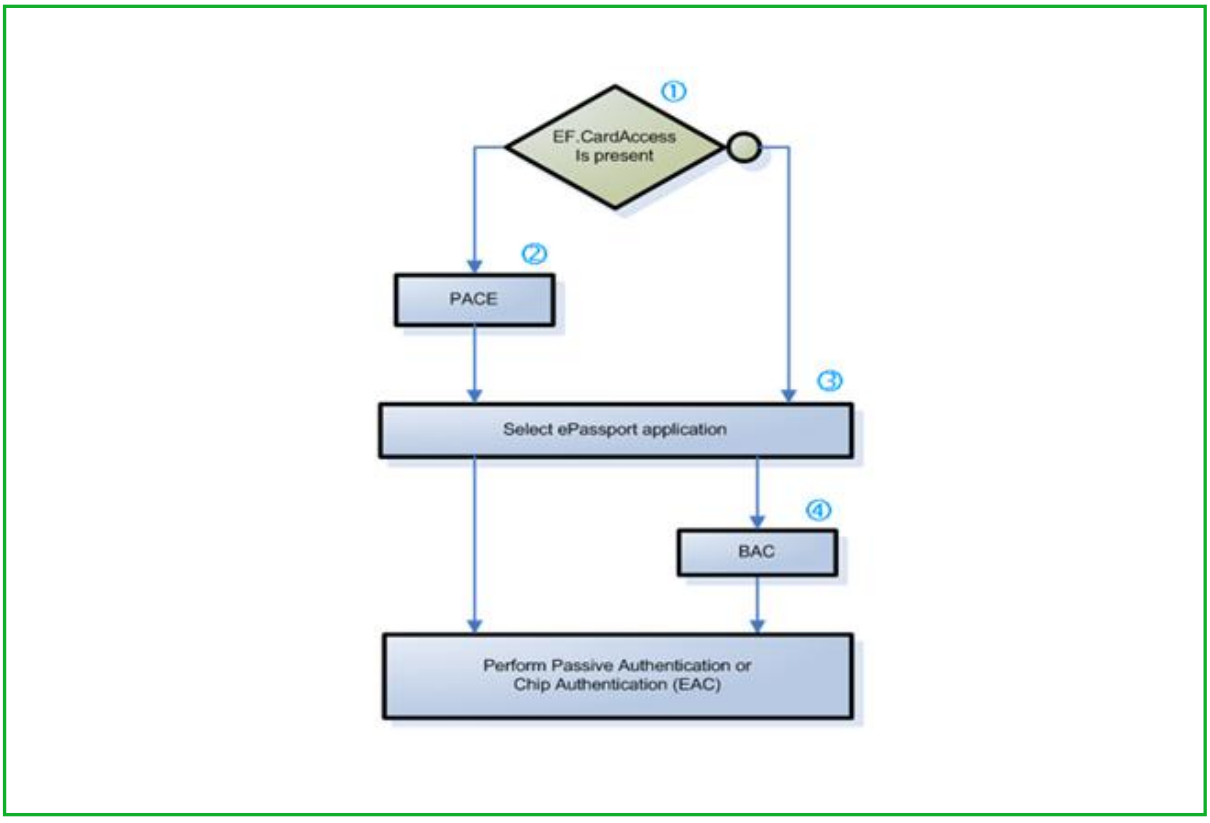
The second data group – DG2 – contains the holder's encoded photo, the same as printed on the data page.

DG1 and DG2 are the first and key data displayed on border control screen and enable the primary document controls and verifications.

The SAC mechanism implements new access rules to improve security for reading these data groups, thanks to symmetric ciphering AES-3DES against skimming and eavesdropping (main threat for contactless application). Additionally SAC allows verifying the ePassport using either MRZ or CAN as a password.

What is the impact on inspection and document verification systems?

- Reading new SAC-enabled ePassports requires an upgrade to border control inspection system software.
- The first phase of ePassport authentication, access control verification, needs to be modified to support SAC procedure in addition to BAC to read, authenticate and then access the DG1 and DG2 data.
- The second phase, which uses Passive Authentication (PA) to prove the authenticity of the data stored in the chip (photo, fingerprint, demographic data, AA Public Key) and to prevent any modification of the information stored in the document, Active Authentication (AA) to check the document has not been cloned and EAC to prevent unauthorized access to fingerprint data and skimming of this sensitive biometric information, will not change.
- This new access control process has no impact on performance and on ePassport verification time at border control.



Will SAC-enabled documents be backwards compatible with BAC ones?

- To ensure global interoperability and backward compatibility, the inspection system must support both SAC and BAC for some time to come. The fact that SAC and BAC mechanisms will be able to work alongside each other even after 2014 will ensure a smooth migration.
- However, to guarantee the most secure access to the chip, SAC should be always used if it is provided by the travel document.

Does SAC improve document inspection system interoperability?

- SAC allows access control either with the MRZ or the CAN.
- Currently, ePassports, eIDs and eResident Permits use a different number of MRZ lines making interoperability difficult to achieve. As SAC and the associated CAN can be supported by all new SAC-compliant electronic documents, access control and inspection systems can select an effective way to apply interoperability and to streamline processes.

> Conclusion: a straightforward migration

For travelers, the migration will be totally seamless from enrolment to crossing borders. SAC offers them greater privacy protection but they use them in exactly the same way as previous ePassports.

For passport issuers, the migration to this enhanced security level should involve minimal effort on their part. It will involve sourcing SAC-enabled passports operating software and some issuance software updates in the areas of data preparation and quality control.

At border control, immigration offers will handle SAC ePassports similarly to BAC documents. The ePassport readers need a straightforward software upgrade to add the SAC mechanism.

Current status of SAC

> The EU and the ICAO

For security reasons, the ICAO decided to enhance the BAC protocol used in the session key calculation to initiate the contactless dialogue between the chip and the reader.

ICAO developed the Technical Report Supplemental Access Control (TR SAC) specifications. Its New Technology working group (NTWG) recommended them to be implemented by December 2014. As time passes, ICAO recommendations generally become mandatory.

In 2010, the European Commission revised its passport and residence permit regulations, which were based on ICAO specifications.

The EU article 6 group within DG JLS (Directorate General on Justice, Freedom and Security) which sets these regulations decided to integrate the ICAO's new TR SAC specification as an amendment to EU passports and residence permits, making it mandatory from the end of December 2014.

> ICAO TR SAC specification

TR SAC specifies an access control mechanism that supplements BAC. It specifies a framework that allows various implementation options, such as mappings, algorithms, passwords. It also defines choices for its implementation in MRTDs.

ICAO Doc 9303, Part 1, as well as Part 3, Volume 2, Section IV, specifies the BAC mechanism, which protects the contents of the Identification Data (IC) against skimming and eavesdropping.

BAC enables the inspection system to authorize itself before granting access to the chip data and establishing a secure (encrypted) communications channel.

It was unveiled in 2004, meaning that by the time e-MRTDs issued now get to the end of their 10-year validity period, they will be being protected by a 15-year-old privacy protection mechanism. Due to ever-increasing computer power, successful eavesdropping attacks will become more and more feasible over this time. Therefore the ICAO started developing an alternative to BAC.

SAC is based on the Password Authenticated Connection Establishment (PACE v2) access control mechanism. Similar to BAC, PACEv2 protocol (TR SAC) also enforces authorized access to the chip contents and establishes secure messaging between an MRTD chip and an inspection system. However, in the PACEv2 protocol the randomness of the password(s) used to authenticate the inspection system has much less influence on the strength of the keys and can therefore be very low.

A key consideration in the development has been preserving global interoperability. Therefore the TR SAC is defined as being supplemental to BAC. It may be implemented in addition to BAC, but not instead of it. Inspection systems should implement and use the new mechanism if provided by the MRTD chip.

BAC will remain the default access control mechanism for globally interoperable MRTDs as long as it provides sufficient security.

Over time, however, SAC will become the default access control mechanism. The approach allows for a gradual change over from BAC to SAC over the next 10 to 20 years.

> Test environment

The technical specifications defining SAC-based travel document interoperability are available as well as the protection profile to be used for Common Criteria certification. In addition a software reader tool supporting SAC, BAC, AA and EAC is publicly available for the whole industry to validate their SAC implementation and it's conformity with the technical specifications.

SAC protection profile can be found here:
http://www.commoncriteriaportal.org/files/ppfiles/ANSSI-CC-cible_PP-2010-06fr.pdf

A free software reader tool supporting SAC, BAC, AA and EAC is also available on the GIXEL website: www.gixel.fr and http://www.soliatis.fr/ (The Universal Reader Tool)

Conclusion

The SAC mechanism has been designed to ensure a higher level of protection against eavesdropping for contactless communication. The mechanism is similar in function to BAC but offers improved and future-proof security with Password Authenticated Connection Establishment (PACE v2) integrating asymmetric cryptography and an option to use a Card Access Number in addition to MRZ.

Overall, the impact of implementing it across the whole process from issuance to border control is minimal.

Passport issuers must be alert when searching for the right partner. To guarantee a smooth migration to SAC, it is important they engage partners and suppliers with long-standing experience of the travel domain.

Suppliers involved in the international standards and government bodies can anticipate compliance as they participate in the definition of the specifications, security proofs and compliancy requirements. Thus they can offer strict compliancy with standards and specifications that form the basis for global interoperability.

Previous experience, especially a proven track-record in BAC to EAC migrations, will ensure a stress-free changeover characterized by best practice. Suppliers dedicated to supporting their client's migration project, including updating issuance and verification solutions, enable them to issue SAC-enabled travel documents seamlessly.

Glossary

AA – Active Authentication

ANTS – Agence Nationale des Titres Sécurisés (French National Agency for Secure Documents)

BAC - Basic Access Control

BIG - Brussels Interoperability Group

BSI - Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)

CAN – Card Access Number

EAC - Extended Access Control V1.11

EC - European Council

EU - European Union

IC - Identification Data

ICAO - International Civil Aviation Organization

MRZ - Machine-Readable Zone

MS - Member states

PACE - Password Authenticated Connection Establishment

SAC - Supplemental Access Control

TR – Technical Report

Bibliography

ANTS Machine readable travel document – SAC/PACE V2

BSI TR 3110 EAC V1.11 – Advanced Security Mechanisms for MRTD – Extended Acess Control (EAC)

ICAO 9303 part 1 & 3 for MRTD booklet and card format

ICAO TR SAC (PACEv2) v1.01

ICAO Supplement 9303 to part 1 and part3 Release 9 Draft

ICAO TAG MRTD 19 WP4 (Decision December 9 2009

EU regulation EC 2252/2004 Dec 13 2004

EU regulation EC 1030/2002 + 3770 (2009) Secret specification

Amendment EU Residence Permit - SPOC 05-nov-2010.doc

Amendment EU passport - Final Proposal 05-11-2010.doc

The world leader in digital security

www.gemalto.com

gemalto
security to be free