

SAC : 3rd generation of ePassport.

A new dimension in electronic passport security

In addition to the information that is already visible on its pages, e-Passports authenticate the holder's identity thanks to a microchip that integrates personal information and hypersensitive biometric data. One of the issues of our time as far as ID is concerned is protecting this data to prevent any capture, identity thefts, targeted terrorist attacks and ensure the holder's privacy.

Ensuring a growing and more secure personal data protection therefore becomes vital.

Electronic passports have now been issued worldwide. Their use aims at, increasing the level of confidence in the ID documents used for travel and easing the flow of passengers whilst authorizing an advanced automation of controls.

Many security schemes have been developed to protect the passport holders' privacy, anonymity and personal data, since the first generation of e-passports was issued by the governments and various organizations at the time.

The ePassports generations:

In November 2004, the first generation of e-Passports ap-

peared. It followed the publishing of a set of technical requirements by the ICAO (International Civil Aviation Organization), which defined the cryptographic protocols to be used to ensure the e-passport's data integrity and authentication.

First generation e-Passports are based on the Basic Access Control (BAC) protocol, which enables access to the data registered on the microchip through the numbering of the communications between that chip and the reader. The BAC protocol relies on an access key derived from the Machine Readable Zone (MRZ), which contains data that can be read on the passport itself or partially known (ex: date of birth).

An additional protocol was suggested in 2006 regarding EU passports, or "2nd Generation passports". Extended Access Control (EAC) protocol relies on advanced cryptology and aims at highly securing biometric data access, especially digital prints (viewed as more sensitive data by the EU). It still uses BAC for 'normal data' access.

It is therefore important to anticipate and prepare for a new generation of passports that challenges an ever progressing fraud, so as to ensure long term security.



Supplemental Access Control (SAC)

The SAC protocol introduces new supplemental security features when compared to BAC. During the authentication phase, it implements asymmetric cryptography when BAC only uses symmetric cryptography. In addition, during the authentication phase, data encryption is based on a shared key between the reader and the chip when BAC only generates a key based on some of the Machine Readable Zone (MRZ) data. Data confidentiality is enhanced and eavesdropping is then impossible.

This new mechanism brings superior security features when compared to BAC and guarantees a high level of privacy.

SAC protocol is:

➔ Unlinkable:

if two data flows are recorded, it is impossible to know if they are coming from the same document.

➔ Non transferable:

The travel document leaves no electronic hints (signature) that can be transferred to third parties.

➔ Untraceable:

A recorded exchange between a reader and a travel document gives no information about the travel document.

This protocol brings additional benefits to existing potential weaknesses in travel documents.

A migration to plan now

As travel document's life spans up to ten years, migrating to this new generation of ePassport should be planned now. In order to organize harmonious migration and to allow BAC readers to keep on verifying travel documents in the coming years, BAC and SAC protocols will be working together even after 2014.

The International Civil Aviation Agency (ICAO) and the European Union have recently decided to enforce the use of this protocol for all travel documents to be issued as of 2014.



Specifications immediately available:

The SAC mechanism has been totally defined by ICAO (SACTR). Documents defining SAC-based travel document interoperability are available, as well as the protection profile to be used for Common Criteria certification (EAL4+). Last but not least, a software reader tool supporting SAC, but also BAC, AA and EAC is available at no cost.

This software can be downloaded from:

➔ **SAC protection profile:** http://www.commoncriteriaportal.org/files/ppfiles/ANSSI-CC-cible_PP-2010-06fr.pdf

➔ **Test plan:** http://www2.afnor.org/espace_normalisation/structure.aspx?commid=3131&lang=french

➔ **Additional tools:** www.gixel.fr

