Sealys eTravel Operating System

For a seamless migration to the 3rd generation of ePassport (SAC)
Recognizing that electronic passport should be secure for the long term, the International Civil Aviation Organization (ICAO) has introduced Supplemental Access Control (SAC), a new security mechanism for the next generation of ePassport. The ICAO and the European Union will enforce the use of this mechanism for all travel documents to be issued as of December 2014.

The first generation ePassports appeared in 2004. It used Basic Access Control (BAC), a mechanism protecting the biographic data and facial image, against skimming and eavesdropping. BAC leverages the machine readable zone (MRZ) with symmetric cryptography.

In 2006, the European Union requested its member nations include fingerprint biometry. This second generation ePassport is protected with Extended Access Control (EAC), which restricts access to biometry to authorized parties only.

SAC third generation ePassport ensures long-term privacy by providing future-proof anti-skimming and anti-eavesdropping beyond BAC. SAC leverages the MRZ with PACE v2 (Password Authenticated Connection Establishment) optimized for asymmetric cryptography and stronger elliptic curve based algorithms.

Gemalto turn-key 3rd generation ePassport offer includes SAC-ready Sealys eTravel application and Coesys issuance and eVerification solutions. It uniquely brings the following key benefits:

• Full compliancy to standards
• Seamless migration
• Trusted and future-proof

Gemalto’s SAC solution is truly compliant with the ICAO standards thanks to Gemalto’s deep involvement in the international standards and government bodies. Gemalto is an active contributor to SAC’s specifications, security proofs and conformance requirements.

Gemalto’s consistent first ranking in ICAO and European interoperability tests proves its track record in standard compliancy.

Sealys eTravel can flexibly be used in BAC, SAC and EAC modes, enabling smooth migration with highly efficient supply chain and stock management as security configuration is only updated at the issuance stage.

Gemalto’s dedicated migration support includes a coordinated update of turn-key solutions for Issuance as well as eVerification. Gemalto’s experience in multiple BAC to EAC migrations leverages international best practices.

Sealys eTravel guarantees long-term viability through widest security features set supporting RSA and elliptic curve cryptography and an extensive set of key lengths. This enables smooth evolution to higher security levels during passport life time of up to 10 years. Sealys eTravel features international Common Criteria certification.

The supply chain is end-to-end secured and optimized thanks to microprocessor multisourcing: the microprocessor platforms are seamlessly interchangeable within issuance and verification systems. Such flexibility leverages microprocessor innovations while reducing delivery risks.

Gemalto has extensive experience in the public sector, having contributed to over 60 national electronic identity projects worldwide. These include passport, national ID, driving license, and eHealth programs with the delivery of enrolment, issuance, eGovernment and eVerification solutions including turn-key solutions and operated services.

Gemalto delivered the world’s first ICAO and European Union-compliant ePassport in 2005. As of today, Gemalto is contributing to over 25 national ePassport programs including Côte d’Ivoire, Denmark, Estonia, France, India (diplomatic), Korea, Malta, Morocco, Norway, Portugal, Qatar, Singapore, Sweden and the USA.

www.gemalto.com