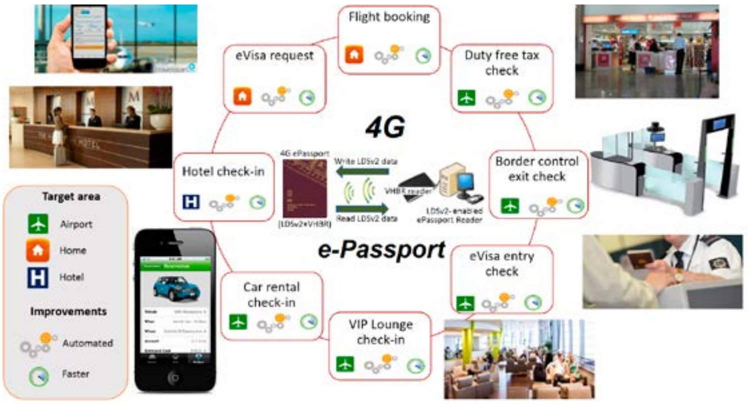
NewP@ss

Next Generation e-Passport

NewP@ss targeted the development of advanced secure platforms (microelectronics and embedded SW) suitable for 3rd and next generation 4th e-Passport currently under discussion at ICAO, which could also be used for hosting dedicated governmental applications; these include e-visa, and boarding tickets among others. Such disruptive new technologies are expected to be introduced in 2015-2020



Main Project Team	
Jonathan Rodriguez	**MS IT-Av**
Joaquim Bastos	MS IT- Av
José Carlos Ribeiro	MS IT- Av
George Mantas	MS IT- Av
Funding Agencies	
QREN - COMPETE	**79,500€**
Start Date	01/07/2012
Ending Date	30/06/2015
Indicators	
Journal Papers	1 (pending review)
Conference Papers	2

Two Main Publications

J. Bastos, G. Mantas, J. C. Ribeiro, J. Rodriguez, T**owards an Advanced PKI-based Security Solution for Next Generation e-Passport and Associated Applications: The NewP@ss Approach**, 8th International Wireless Internet Conference - Symposium on Wireless and Vehicular Communication (WiCON 2014), Lisbon, Portugal, November, 2014

E. Alireza, A. Nascimento, J. Rodriguez, J. C. Neves, **An Efficient MAC-Signature Scheme for Authentication in XOR Network Coding**, 19th IEEE Symposium On Computers And Communications (ISCC 2014), Funchal, Madeira, Portugal, June, 2014

PROJECT WEBPAGE URL
http://newpass.av.it.pt/index.html

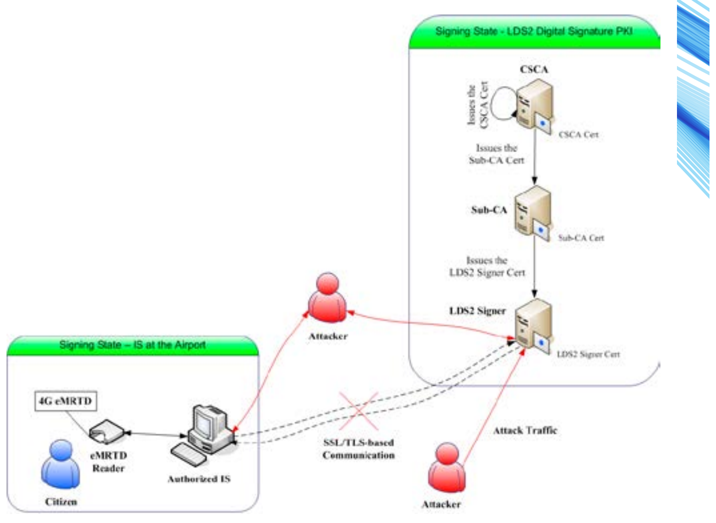


Fig. 1 SSL/TLS-based communication between the IS and the LDS2 Signer under MITM attacks and DoS attacks.

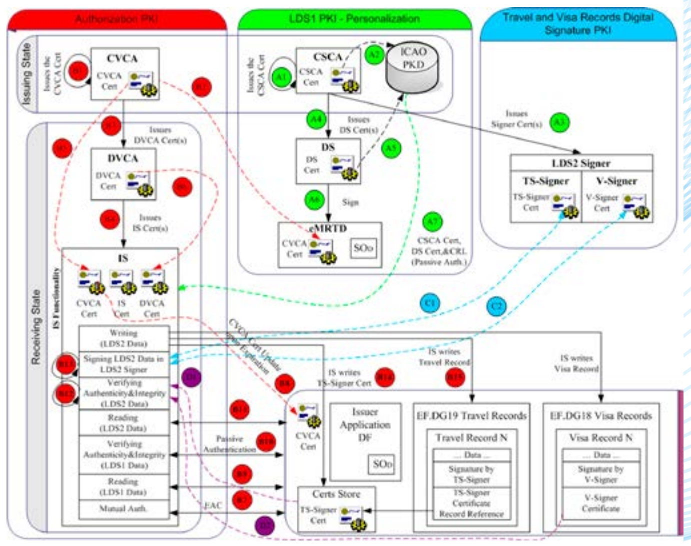


Fig. 2 PKI Architecture for 4th generation e-Passport, with processing steps considering e-travel stamps.

GENERAL MOTIVATION AND OBJECTIVES

The NewP@ss project focus on the design and development of advanced secure HW and SW platforms suitable for the coming new e-Passport generations, usable and recognized as approved travel document at European and International level, but which could also be used for hosting dedicated e-services applications of both government and/or private nature. Essentially, the project will targeted the following objectives:

- Develop all necessary HW/SW technologies needed for supporting the next e-Passport generations. These new generations will in particular support the new LDS1+/2 (Logical Data Structures) under discussion at ICAO, which will enable a fundamental conceptual shift on e-Passport usage, enabling it to become a true multi-application device;

- Develop all necessary technology bricks that will be needed for reaching the performance and functionality levels requested by ICAO and EU or International regulatory bodies (new cryptographic protocols, e.g. SAC, high-speed contactless interfaces, e.g. VHBR, and efficient biometry);

- Develop complete proofs of concepts for new e-Passport implementation, resulting on a combination of advanced secure 32 bit microcontrollers, advanced embedded SW platforms based on small footprint multithread OS, and secure compact fixed or mobile readers;

- Develop all necessary security and privacy concepts needed for guarantying the target life-time (5-10 years) of the envisaged e-Passport platforms as well as the proper level of isolation between applications;

- Provide functional test suites and reference implementations suitable for further interoperability testing;

- Validate the proofs of concepts of the e-Passport platforms on use cases pertaining to e-government, as well as private nature use cases. The setting up of some of these cases also involve the development/validation of the necessary security mechanisms for the proper handling of security credentials (certificates, PKI schemes).

CHALLENGE

It is key to identify all requirements and define the specification that is needed for the NewP@ss platforms, and especially for the future generations of e-Passport compliant with the LDS1+/LDS2 logical data structures that have been under definition at the ICAO. Also, it is important to develop all embedded SW needed, based on existing e-Passport technology and new LDS1+/LDS2+, which implement all basic functions needed for supporting third or fourth generation of e-Passport. A specific focus was needed to keep the SW layout enable to support full interoperability (at application level) of the target platforms and ensuring the multi-application nature of the platform. Moreover, it was vital to perform horizontal studies to ensure that the NewP@ss platforms would reach the highest level of security required by the ICAO, EU and other international regulatory bodies for supporting the target applications, which in the case of IT related to 3rd and 4th generation e-Passport threats modelling and respective analysis and mitigation, as well as PKI design and development for 4th generation e-Passport.

WORK DESCRIPTION AND ACHIEVEMENTS

The IT team involved in NewP@ss has carried out, among other things, a thorough security analysis of the communication between the Inspection System (IS) reading an electronic machine readable travel document (eMRTD/e-Passport) and the LDS2 Signer of the LDS2 Digital Signature PKI. Also, a complete PKI architecture was designed, and implemented for demonstration, following the requirements and current specifications of future 4th generation e-Passport.

The project has been widely disseminated, also by the IT team, including in public media, e.g. at RDP Antena1 public national radio (http://www.rtp.pt/play/p384/e144301/click). Moreover, the NewP@ss consortium has won the "Most Innovative Project" award at the 2015 European Nanoelectronics Forum, as the jury recognized that its work on a new generation of e-Passports and associated e-services will dramatically improve security and convenience for travellers.