E-Passports as a Means Towards the First World-Wide Public Key Infrastructure

Dimitrios Lekkas[1] and Dimitris Gritzalis[2]

[1] Dept. of Product and Systems Design Engineering, University of the Aegean
Syros GR-84100
dlek@aegean.gr
[2] Information Security and Critical Infrastructure Protection Research Group,
Dept. of Informatics, Athens University of Economics and Business (AUEB)
76 Patission Ave., Athens GR-10434
dgrit@aueb.gr

Abstract. Millions of citizens around the world have already acquired their new electronic passport. The e-passport is equipped with contactless communication capability, as well as with a smart card processor enabling cryptographic functionality. Countries are required to build a Public Key Infrastructure to support digital signatures, as this is considered the basic tool to prove the authenticity and integrity of the Machine Readable Travel Documents. The first large-scale worldwide PKI is currently under construction, by means of bilateral trust relationships between Countries. In this paper, we investigate the good practices, which are essential for the establishment of a global identification scheme based on e-passports, together with the security and privacy issues that may arise. We argue that an e-passport may also be exploited in other applications as a globally interoperable PKI-enabled tamperproof device. The preconditions, the benefits, and the drawbacks of using e-passports in everyday electronic activities are further analyzed and assessed.

Keywords: Security, Trust, Digital Signatures, Machine Readable Travel Documents, PKI, RFID, Smart card, Passport.

1 Introduction

The citizens of many countries around the world obtained their new electronic passport (e-passport), within the last year or so. Most European countries have already implemented the infrastructure for the issuance of the new passports. The requirements for a new type of passport are imposed by the United States and the International Civil Aviation Organization (ICAO), demanding a higher level of security at the inspection points of the countries borders. The e-passport incorporates three state-of-the-art technologies: Radio Frequency Identification (RFID), Biometrics and Public Key Infrastructure (PKI). While RFID is used for practical reasons in the communication with the inspection systems, Biometrics and PKI are considered capable of reducing fraud and enhancing security in worldwide digital identification.

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 34–48, 2007.

From its side, ICAO published a series of technical reports, describing the technical and procedural details on how a Machine Readable Travel Document (MRTD) must be implemented [1]. Face recognition is specified as the only mandatory globally interoperable biometric for identity verification of travelers. MRTDs including e-passports, are equipped with an Integrated Circuit Chip (ICC), where all digital data, including biometric information are stored. Among several other issues, ICAO technical reports describe the details of the communication between the e-passport and the local inspection points, the specifications for biometric data, the structure of the data stored (called the Logical Data Structure – LDS [2]), and the PKI support.

The ICAO PKI Technical Report [3] is intended to provide standards for a simple worldwide Public Key Infrastructure, which should support digital signatures applied to Machine Readable Travel Documents. These digital signatures are intended to permit authentication of basic data produced by the issuing Country and stored in the chip embedded into the e-passport. The stored signed data include the Machine Readable Zone (MRZ) of the passport plus digitized biometric measurements, as well as other personal data of the passport bearer.

Using the digital signature, the receiving Countries can verify that the stored data is authentic (i.e. generated by the issuing Country, and not been altered), just as the physically readable passport booklet is secured from unauthorized alteration or substitution by strong physical security measures. ICAO has recognized that one of the most effective ways of doing this is using Public Key Cryptography to digitally sign the data stored on the chip. Issuing Countries are requested to implement a PKI, following specific interoperable standards, and to properly manage their own keys, which are used to digitally sign the data stored in the e-passports.

Given that the US and the ICAO initially demanded from the Countries to implement the PKI within a very short period (just a few months), the ICAO Technical Report states that it does not aim at describing a full implementation of a PKI within each Country. ICAO states that PKI does not provide the sole measure for determining the authenticity of the passport and, thus, it should not be relied upon as a single determining factor. The passport still maintains its physical security characteristics, and it should be verified by check-points using conventional manual mechanisms, along with the automated check of its electronic contents. Due to this restrained approach, the ICAO report seems that it sacrifices several security characteristics of a strong PKI implementation, such as the existence of client X.509 certificates, as well as the existence of passport revocation mechanism. Moreover, perhaps due to the increased cost of passports with crypto-processor chip, the active security mechanisms, which could protect the e-passport's data against eavesdropping and cloning, are not mandatory, allowing a weak e-passport implementation.

In this paper we focus on the PKI-related issues of e-passports, proposing a series of good practices in order to implement a Country PKI, conforming to ICAO rules. We examine how the required global interoperability can be achieved by building an appropriate worldwide Trust architecture. We then specify some important security and privacy issues, which are emerged by the use of digitized personal data. As the e-passports infrastructure seems to implement the sole globally interoperable PKI of today, we investigate how we can exploit this infrastructure in different areas and applications, by using the e-passport not only as a digital identity, but even as a