RESUMEN

Este trabajo busca ayudar en la comprensión de los conceptos que están detrás del pasaporte electrónico, regulado por la Organización de Aviación Civil Internacional y su Doc 9303. Con este fin se describen sus características lógicas y físicas, y se hace una revisión de los estándares ISO/IEC 14443 (que define su comunicación por radio frecuencia) e ISO/IEC 7816-4 (que define los comandos Smart Cards para intercambio) así como de la especificación PC/SC que facilita la interoperación de Smart Cards y dispositivos lectores correspondientes a diferentes fabricantes en el entorno PC. También se explican los principales mecanismos de seguridad aplicables a los ePassports y que sirven para proteger su Autenticidad (por medio de la Autenticación Pasiva que hace uso de una Infraestructura de Clave Pública), Confidencialidad (por medio del Control de Acceso Básico) y Originalidad (por medio de la Autenticación Activa). Esto sirve de preámbulo para plantear una metodología que permita hacer una validación electrónica del pasaporte, basada en tres resultados posibles. Por último se ha desarrollado, en el lenguaje de programación Java, una herramienta como instrumento para la aplicación de la metodología, que ha servido para realizar la validación de un conjunto de pasaportes, cada uno con características de entrada pre-establecidas, y que cubren las principales alternativas que pueden presentarse. El resultado de las pruebas ha demostrado que la metodología propuesta es útil para validar pasaportes electrónicos.

PALABRAS CLAVE:

- **PASAPORTE ELECTRÓNICO**
- **RFID**
- **SISTEMA DE INSPECCIÓN**
- **PKI**

ABSTRACT

This work tries to help in the comprehension of the concepts behind the electronic passport, regulated by International Civil Aviation Organization and his Doc 9303. With this aim, its logical and physical characteristics are described, and a revision of the ISO/IEC 14443 (which defines its communication through RF) and ISO/IEC 7816-4 (which defines the commands used in Smart Cards for exchange) standards is made, as well as the PC/SC specification that facilitates Smart Card and reader's interoperation corresponding to different manufactures, in the PC environment. It also explains the main security mechanisms applicable to ePassports and that serve to protect their Authenticity (through Passive Authentication that makes use of a Public Key Infrastructure), Confidentiality (through Basic Access Control) and Originality (through Active Authentication). All this serves as a preamble to propose a methodology that allows to perform an electronic validation of the passport, based on three possible results. Finally, in the Java programing language, a tool has been developed as an instrument for the methodology's application, which has served to validate a set of passports, each with pre-established input characteristics, and which cover the main alternatives that can be presented. The result of the test has shown that the proposed methodology is useful for validating electronic passports.

KEY WORDS

- **EPASSPORT**
- **RFID**
- **INSPECTION SYSTEM**
- **PKI**