RFID chips and EU e-passports: the end of privacy?

By Nikita Maria, PhD Candidate, Applied Informatics, University of Macedonia

Abstract

Radio Frequency Identification (RFID) technology is in wide deployment and has been used to many applications for decades. The principal advantage of this technology is that it automatically identifies objects using electromagnetic waves to communicate with a reader without requiring contact and line of sight.

As the technology evolved and offered large memory capacity it was used as a storage medium for electronic passports (e-passports). The e-passport is the digital version of the paper passport and its goal is to provide stronger identity authentication than the classic one. It was believed that it was able to ease identity checks, lessen the amount of human errors, protect against manipulation of travel documents and improve border security. But the fact that biometric data can be stored to the e-passport; privacy and security risks are posed for the holders. So, this new passport turned out to be much more intrusive than the traditional one.

RFID chips used in e-passports are equipped with protection mechanisms but they still have lots of technical flaws and they are vulnerable to skimming and eavesdropping. The main problem stems from the fact that the data contained on the e-passport are transferred wirelessly, so it is vulnerable to anyone having the necessary equipment.

This paper focuses on the use of RFID technology in EU e-passports. Particularly a short description of the technology and its advantages are given and even more attention is given to the threats that are posed to the holder's privacy. Finally, data protection issues and the proposed EU Regulation are presented.