World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

BAN Logic Proof of E-passport Authentication Protocol

Authors : Safa Saoudi, Souheib Yousfi, Riadh Robbana

Abstract : E-passport is a relatively new electronic document which maintains the passport features and provides better security. It deploys new technologies such as biometrics and Radio Frequency identification (RFID). The international civil aviation organization (ICAO) and the European union define mechanisms and protocols to provide security but their solutions present many threats. In this paper, a new mechanism is presented to strengthen e-passport security and authentication process. We propose a new protocol based on Elliptic curve, identity based encryption and shared secret between entities. Authentication in our contribution is formally proved with BAN Logic verification language. This proposal aims to provide a secure data storage and authentication.

Keywords : e-passport, elliptic curve cryptography, identity based encryption, shared secret, BAN Logic
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020