World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:9, No:11, 2015

NFC Communications with Mutual Authentication Based on Limited-Use Session Keys

Authors : Chalee Thammarat

Abstract : Mobile phones are equipped with increased short-range communication functionality called Near Field Communication (or NFC for short). NFC needs no pairing between devices but suitable for little amounts of data in a very restricted area. A number of researchers presented authentication techniques for NFC communications, however, they still lack necessary authentication, particularly mutual authentication and security qualifications. This paper suggests a new authentication protocol for NFC communication that gives mutual authentication between devices. The mutual authentication is a one of property, of security that protects replay and man-in-the-middle (MitM) attack. The proposed protocols deploy a limited-use offline session key generation and use of distribution technique to increase security and make our protocol lightweight. There are four sub-protocols: NFCAuthv1 is suitable for identification and access control and NFCAuthv2 is suitable for the NFC-enhanced phone by a POS terminal for digital and physical goods and services.

Keywords : cryptographic protocols, NFC, near field communications, security protocols, mutual authentication, network security
Conference Title : ICOCN 2015 : International Conference on Optical Communications and Networking
Conference Location : Kyoto, Japan
Conference Dates : November 12-13, 2015