World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:10, No:09, 2016

Secure Cryptographic Operations on SIM Card for Mobile Financial Services

Authors : Kerem Ok, Serafettin Senturk, Serdar Aktas, Cem Cevikbas

Abstract : Mobile technology is very popular nowadays and it provides a digital world where users can experience many value-added services. Service Providers are also eager to offer diverse value-added services to users such as digital identity, mobile financial services and so on. In this context, the security of data storage in smartphones and the security of communication between the smartphone and service provider are critical for the success of these services. In order to provide the required security functions, the SIM card is one acceptable alternative. Since SIM cards include a Secure Element, they are able to store sensitive data, create cryptographically secure keys, encrypt and decrypt data. In this paper, we design and implement a SIM and a smartphone framework that uses a SIM card for secure key generation, key storage, data encryption, data decryption and digital signing for mobile financial services. Our frameworks show that the SIM card can be used as a controlled Secure Element to provide required security functions for popular e-services such as mobile financial services.

Keywords : SIM card, mobile financial services, cryptography, secure data storage
Conference Title : ICFCDS 2016 : International Conference on Financial Cryptography and Data Security
Conference Location : Rome, Italy
Conference Dates : September 15-16, 2016