DIGITAL CERTIFICATE MANAGEMENT SYSTEM FOR eHEALTH AND mHEALTH PRACTITIONERS IN SRI LANKA TO SECURE MEDICAL DATA

Jinasena T.M.K.K.[1*], Meegama R.G.N.[1] and Marasinghe R.B.[2]

[1]Department of Computer Science, University of Sri Jayawardenepura, Sri Lanka

[2]Department of Medical Education and Health, University of Sri Jayawardenepura, Sri Lanka

kasunkosala@yahoo.com

ABSTRACT

eHealth and mHealth systems are getting more popular; yet, vulnerabilities are much higher when the sensitive medical data being transferred through public networks. Thus, it is required to have a security mechanism to support encryption, digital signature, digital authentication, and integrity verification. However, in this research we have developed a digital certificate management system to facilitate all these features including creating asymmetric key pairs, generating, signing, chaining and revoking certificates, signing and verifying digital contents. Because it is a Java application, it is portable and platform independent. In backend, it uses Open SSL library. Moreover, it is capable of managing present RSA based certificates as well as the latest Elliptic Curve (EC) based certificates. Thus, it is more robust, future-proof and well-suited for mobile devices. In conclusion, it is a simple, free and open source software for the public to secure their digital data.

Keywords: Computer Security, Digital Certificate, PKI, eHealth, mHealth