ISSN: 1391-8796
Proceedings of 7th Ruhuna International Science & Technology Conference
University of Ruhuna, Matara, Sri Lanka
January 22, 2020

Building an identity verification system with high security using elliptic curve digital signature algorithm

De Silva P.D.D.C. and Yapage N.*

Department of Mathematics, University of Ruhuna, Wellamadama, Matara, Sri Lanka

We construct a web based Identity Verification System called AuthC which is built upon ECDSA with SHA256 (Elliptic Curve Digital Signature Algorithm with Secure Hashing Algorithm 256 bit versions), which uses ECDSA as a method of verifying the source of the requests. The main reason to introduce AuthC is to fulfill the trust gap, when one faces the identity verification problems. AuthC may be very useful when authentication is the main requirement.

AuthC is a web based application with high security which fulfills the trust gap between two strangers. Basically, AuthC ensures the identity of an identification card holder by providing basic information such as name, address, birth date, general appearance, and any other identification or individual information of the holder, which are provided by authorized parties. These can be related to educational status, crime history, civil status, etc. AuthC can help society by verifying identification card of an individual easily and accurately, and also by updating and linking all personal information of the holder in real time. Moreover, the proposed cryptosystem has the potential of implementing as a commercial product with high fidelity.

Technically AuthC is developed using RESTful service, which is built on the REST (REpresentational State Transfer) architecture, SpringBoot (https://spring.io/projects/spring-boot), VueJS (https://vuejs.org), and Bootstrap (https://getbootstrap.com) Frameworks. RESTful service is a web service, which is used to communicate between applications, services or any other softwares.

Keywords: cryptography, elliptic curve cryptography, elliptic curve digital signature algorithm, authentication and identity verification

*Corresponding author: nihal@maths.ruh.ac.lk