Aplikasi *Enterprise Document Digital Signature* menggunakan RSA dan SHA256 untuk WFH di Era Pandemi COVID-19

Rafie Afif Andika[1], Aji Gautama Putradana[2], Rizka Reza Pahlevi[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]rafieafifandika@students.telkomuniversity.ac.id, [2] aji@telkomuniversity.ac.id, [3]reza@telkomuniversity.ac.id

Abstract

In a COVID-19 Pandemic situation of WFH with the use of the internet, activities such as sending documents online with scanned signature have become standard. However, scanned signature can be easily forged, stolen, and misused. The aim of this research is to create and implement an application for enterprise document digital signatures using RSA and SHA256 so that WFH in COVID-19 pandemic era can be held effective and securely. For proof of concept, an enterprise-like dummy application is created. The application is a distributed system that can share documents for the document holder (applicant), the signature holder (signer), and the signature and document verifier (verifier). Two digital signature scenarios are created for comparison, one uses RSA 2048 bit encryption and the other uses RSA 4098 bit encryption. From overhead testing results, RSA 4096 bit requires approximately 4 times the overhead time of RSA 2048 bit for the signature process and the verification process. However, through calculation brute force simulations, RSA 4096 bit requires approximately 10^{616} times longer to crack compared to RSA 2048 bit. Also, through integrity test, the verifier can detect if the document or the signature key is falsified.

Keywords: ***digital signature, SHA256, RSA, enterprise, COVID-19, brute force attack***