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

Abstrak

Dalam situasi WFH ditengah Pandemi COVID-19 dimana beberapa hal dikerjakan dengan pemanfaatan internet, aktivitas seperti mengirim dokumen secara online dengan scan tanda tangan sudah menjadi hal yang standar. Namun, tanda tangan yang dipindai dapat dengan mudah dipalsukan, dicuri, dan disalahgunakan. Penelitian ini bertujuan untuk membuat dan mengimplementasikan aplikasi tanda tangan digital dokumen perusahaan menggunakan RSA dan SHA256 sehingga sistem WFH di era pandemi COVID-19 dapat terselenggara dengan efektif dan aman. Sebagai bukti konsep, aplikasi dummy untuk perusahaan dibuat. Aplikasi ini merupakan sebuah sistem terdistribusi yang dapat berbagi dokumen untuk pemegang dokumen (pemohon), pemegang tanda tangan (signer), dan pemverifikasi tanda tangan dan dokumen (verifier). Dua skenario tanda tangan digital dibuat untuk perbandingan, satu menggunakan enkripsi RSA 2048 bit dan yang lainnya menggunakan enkripsi RSA 4098 bit. Dari hasil pengujian overhead RSA 4096 bit membutuhkan waktu kurang lebih 4 kali dari waktu overhead RSA 2048 bit untuk proses signature dan proses verifikasi. Namun, melalui perhitungan simulasi brute force, RSA 4096 bit membutuhkan sekitar 10^{616} kali lebih lama untuk diretas dibandingkan dengan RSA 2048 bit. Selain itu, melalui uji integritas, verifier dapat mendeteksi jika dokumen atau kunci tanda tangan apabila dipalsukan.

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