

ABSTRAK

Surat keterangan sehat sangat dibutuhkan pada masa pandemic covid-19, dengan adanya surat keterangan sehat kegiatan diluar rumah dapat dilakukan, pentingnya surat keterangan sehat tersebut rentan terjadi pemalsuan oleh pihak yang tidak bertanggung jawab. Sehingga dibutuhkan suatu jaminan untuk menguji validitas pada surat keterangan sehat tersebut dengan menerapkan *digital signature*. *Digital signature* yang di rancang dalam penelitian ini menggunakan algoritma kriptografi RSA dan algoritma MD5. Algoritma kriptografi RSA yang di gunakan pada penelitian ini adalah algoritma kriptografi RSA kunci ganda yang pada proses enkripsi dan dekripsinya menggunakan dua pasang kunci rsa yang berbeda. Dan menggunakan algoritma MD5 yang berguna untuk mengantisipasi perubahan data pada surat keterangan sehat yang sudah dibuat, disisipkan juga QR Code pada surat keterangan sehat untuk mempermudah penggunaan *digital signature*nya. Penggunaan algoritma kriptografi RSA kunci ganda untuk proses enkripsinya sebesar 1,98 kali lebih lambat di bandingkan enkripsi menggunakan RSA biasa dan untuk waktu dekripsi proses RSA kunci ganda dan RSA biasa bisa mencapai 2.295,33 kali lebih lambat di bandingkan proses pendeskripsian menggunakan metode RSA biasa. Proses validasi surat keterangan sehat cukup mudah dilakukan dengan menscan QR code pada surat dan memasukkan inputan nik pasien dan tanggal pembuatan surat. Aplikasi yang telah dibuat dengan tingkat kelayakan aplikasi mencapai 90%.

Kata kunci: *Digital signature, RSA dan MD5, Surat Keterangan Sehat*

Abstract

Health certificates are very much needed during the covid-19 pandemic, with a health certificate, activities outside the home can be carried out, the importance of the health certificate is prone to forgery by irresponsible parties. So a guarantee is needed to test the validity of the health certificate by apply a digital signature. The digital signature designed in this study uses the RSA cryptographic algorithm and the MD5 algorithm. The RSA cryptographic algorithm used in this study is a double key RSA cryptography algorithm which in the encryption and decryption process uses two different RSA key pairs. And using the MD5 algorithm which is useful for anticipating changes in data in the certificate that has been made, a QR Code is also inserted in the health certificate to facilitate the use of digital signatures. The use of the double key RSA cryptography algorithm for the encryption process is 1.98 times slower than the encryption uses ordinary RSA

and for the decryption time the double key RSA and ordinary RSA can reach 2,295.33 times slower than the decryption process using the ordinary RSA method. The process of validating a health certificate is quite easy to do by scanning the QR code on the letter and entering the patient's identification number and the date of writing the letter. Applications that have been created correctly for applications are up to 90%.

Key Word: Digital signature, RSA, MD5, Health Certificate