PENERAPAN APLIKASI PENGGABUNGAN TANDA TANGAN DIGITAL DENGAN TANDA TANGAN MANUAL UNTUK KEAMANAN BERKAS ELEKTRONIK PADA NISSIN ELECTRIC CO., LTD.

Aminatuz Zuhrah

Abstrak

Pengiriman dokumen melalui e-mail sudah merupakan hal komersiil. Pengamanan dokumen untuk menjaga keotentikannya sampai di pihak penerima dalam perjalanan di jaringan relative tidak aman salah satunya dengan cara memberi tandatangan dijital. Salah satu metode untuk membuat tandatangan dijital adalah tandatangan manual yang dikombinasikan dengan DSA (*Digital Signature Algorithm*). Tujuan dari penelitian ini adalah mengamankan e-dokumen dengan metode penggabungan penggabungan tanda tangan manual dan DSA (*Digital Signature Algorithm*) sebagai salah satu solusi pada masalah manajemen kunci dan memenuhi kebutuhan ketidaktunggalan penandatangan yang dalam penelitian ini disebut *signer*. Biometrik yang digunakan adalah tandatangan manual/ *offline.* Pada penelitian ini keluaran yang dihasilkan adalah berupa Aplikasi Kriptografi dengan tiga tahap proses inti (Pembangkitan Kunci, Pembuatan tandatangan dijital, dan verifikasi). Selanjutnya e-dokumen, tandatangan *digital* dan kunci publik ditransmisikan melalui internet via *e-mail* pada pihak penerima yang selanjutnya dalam penelitian ini disebut *verifier*. Kemudian pihak *verifier* memverifikasi apakah hasilnya valid yaitu e-dokumen tersebut masih otentik dan pengirim adalah *penandatangan yang sah* sebenarnya dari e-dokumen tersebut. Sebaliknya jika hasilnya tidak valid yaitu. E-dokumen tersebut sudah tidak otentik dan atau pengirim bukanlah *signer* sebenarnya dari e-dokumen tersebut.

Kata Kunci: *Signer, verifier,* Tandatangan *off-line,* Tandatangan *digital, DSA (Digital Signature Algorithm*).

APPLICATION OF INTEGRATION BETWEEN OFFLINE SIGNATURE AND DIGITAL SIGNATURE FOR E-DOCUMENT SECURITY AT NISSIN ELECTRIC CO., LTD.

Aminatuz Zuhrah

Abstract

Document transmission through email has been used as a commercial transaction. One of the method to keep the document authentic while it's transmit through insecure network is with embed digital signature. One of method to create digital signature is with merger between offline signatures with digital signature algorithm. . The purpose of this research is to create cryptographic applications with merger offline signatures and DSA (Digital Signature Algorithm) as one of the solution to the problem of management key and meet the needs nonsingular of signer. In this research as an input (key generator) are offline signature with one or more users that able to generate one or more digital signatures for one e-document. Furthermore, e-documents, digital signatures and public key is transmitted over the Internet via e-mail to the verifier. Afterwards the verifier verifies whether its result is valid which means the e-documents are still authentic and the sender is the authorized signer of the e-document. Conversely, if the result is not valid that means the e-document is not authentic and signer is not the authorized sender of the e-document.

Keywords: Signer, Verifier, offline signature, Digital signature, DSA (Digital Signature Algorithm).