ABSTRAK

Tanda tangan elektronik telah menjadi komponen penting dalam era digital, menggantikan tanda tangan konvensional yang membutuhkan kertas dan pena. Dengan kebutuhan utama untuk memastikan keamanan dan keabsahan dokumen elektronik dalam berbagai transaksi bisnis dan pemerintahan terdapat masalah utama yang dihadapi yaitu cara untuk memastikan integritas dan keautentikan informasi elektronik dari dokumen elektronik yang ditandatangani secara digital. Di PT Pos Indonesia (Persero), penggunaan tanda tangan konvensional masih banyak digunakan untuk dokumen-dokumen penting yang membutuhkan validitas atas keasliannya. Kriptografi asimetris digunakan untuk menghasilkan pasangan kunci publik dan kunci pribadi, dimana kunci pribadi digunakan untuk menandatangani dokumen dan kunci publik digunakan untuk memverifikasi tanda tangan tersebut. Algoritma Base64 diterapkan untuk memastikan bahwa data tanda tangan dapat disimpan dan dikirim dalam format yang aman dan efisien. Teknik ini digunakan untuk memastikan bahwa data tanda tangan elektronik dapat dengan mudah disimpan dan ditransmisikan. Dengan mengkonversi data menjadi format teks, Base64 memastikan bahwa tanda tangan elektronik dapat diterima dan diinterpretasikan dengan benar oleh penerima. Studi kasus yang dilakukan memperlihatkan bahwa sistem tanda tangan elektronik ini mampu memastikan keabsahan dokumen dan memastikan bahwa dokumen tersebut telah diverifikasi oleh pejabat yang berwenang.

Kata Kunci : tanda tangan elektronik, kriptografi, algoritma base64, keamanan dokumen.

ABSTRACT

Electronic signatures have become a crucial component in the digital era, replacing conventional signatures that require paper and pen. With the primary need to ensure the security and validity of electronic documents in various business and government transactions, a major issue faced is the method to ensure the integrity and authenticity of electronic information in digitally signed documents. At PT Pos Indonesia (Persero), conventional signatures are still widely used for important documents requiring authenticity validation. Asymmetric cryptography is employed to generate pairs of public and private keys, where the private key is used to sign documents and the public key is used to verify the signatures. The Base64 algorithm is applied to ensure that signature data can be stored and transmitted in a secure and efficient format. This technique ensures that electronic signature data can be easily stored and transmitted. By converting the data into text format, Base64 ensures that electronic signatures can be correctly received and interpreted by the recipient. The case study conducted demonstrates that this electronic signature system can ensure the validity of documents and verify that the documents have been authenticated by authorized officials.

Keywords: *electronic signature, cryptography, Base64 algorithm, document security.*