ABSTRAK

Persetujuan atau pengesahan terhadap isi dokumen dapat dilakukan menggunakan tanda tangan. Tanda tangan digital telah digunakan untuk mengatasi masalah pemalsuan tanda tangan konvensional terutama pada dokumen PDF. Meskipun tanda tangan digital mencakup aspek keamanan *data integrity* dan *authenticity*, namun tanda tangan digital tetap dapat dipalsukan karena hanya memverifikasi melalui keterkaitan pasangan kunci publik dan privat. Selain itu, tanda tangan digital rentan terhadap serangan Man-In-The-Middle (MITM) terutama pada pertukaran kunci publik. Oleh karena itu, dibutuhkan solusi yang dapat meningkatkan keamanan tanda tangan digital pada penggunaanya untuk menandatangani dokumen PDF.

Penelitian ini membahas implementasi sertifikat digital X.509 pada dokumen elektronik PDF menggunakan format PKCS#10. Sertifikat digital X.509 hanya dapat diterbitkan oleh pihak terpercaya yang disebut *Certificate Authority* (CA). Penggunaan sertifikat digital X.509 yang mengandung kunci publik penandatangan digunakan untuk menambah lapisan keamanan pada proses verifikasi. Tujuan penelitian ini adalah untuk menganalisis keamanan integritas data (*data integrity*) dan otentikasi penandatangan (*authenticity*) sertifikat digital pada dokumen PDF.

Pengujian pada aspek keamanan *data integrity* dilakukan dengan membandingkan *digest* dokumen PDF asli dan *digest* dari tanda tangan digital. Pengujian aspek kemanan *authenticity* dilakukan dengan memverifikasi tanda tangan digital dan sertifikat digital setelah memanipulasi pasangan kunci pada proses penandatanganan dokumen PDF, penggunaan sertifikat digital X.509 yang telah kedaluwarsa, dan pengujian MITM untuk memverifikasi tanda tangan digital. Persentase ketercapaian hasil analisis *data integrity* dan *authenticity* secara keseluruhan mendapat hasil 87,5%.

Kata Kunci: Tanda Tangan Digital, PDF, Kriptografi Kunci Publik, Infrastruktur Kunci Publik, Sertifikat Digital X.509, SHA256, RSA2048, MITM.

ABSTRACT

Approval or validation of the contents of a document can be done using a signature. Digital signatures have been used to overcome the problem of forging conventional signatures, especially on PDF documents. Even though digital signatures include security aspects of data integrity and authenticity, digital signatures can still be forged because they are only verified through the linkage of public and private key pairs. Additionally, digital signatures are vulnerable to Man-In-The-Middle (MITM) attacks especially on public key exchanges. Therefore, a solution is needed that can increase the security of digital signatures when used to sign PDF documents.

This research discusses the implementation of X.509 digital certificates in PDF electronic documents using the PKCS#10 format. X.509 digital certificates can only be issued by a trusted party called a Certificate Authority (CA). The use of X.509 digital certificates containing public signing keys is used to add a layer of security to the verification process. The aim of this research is to analyze the security of data integrity and authentication of digital certificates on PDF documents.

Testing on the security aspect of data integrity is carried out by comparing the essence of the original PDF document and the essence of the digital signature. Authenticity security aspect testing is carried out by verifying digital signatures and digital certificates after manipulating key pairs in the PDF document signing process, using expired X.509 digital certificates, and MITM testing to verify digital signatures. The percentage of achievement of the overall data integrity and authenticity analysis results was 87.5%.

***Keywords**: Digital Signature, PDF, Public Key Cryptography, Public Key Infrastructure, Digital Certificate X.509, SHA256, RSA2048, MITM*.