ISSN : ISSN 2962–5688
Website :
jurnal.umj.ac.id/index.php/TripleA
Email : triplea@umj.ac.id

TRIPLE A
Jurnal Pendidikan Teknologi Informasi

IMPLEMENTASI PERANCANGAN INFRASTRUKTUR KUNCI PUBLIK PADA PEMBUATAN SURAT ORGANISASI DIGITAL MENGGUNAKAN DIGITAL SIGNATURE

Fajar Tri Laksana[1*)], Sari Palestina[2*)], Eldiyas Nur Anfa[3*)]
[1,2,3)]Pendidikan Teknologi Informasi, Fakultas Ilmu Pendidikan, Universitas Muhammadiyah Jakarta, Jl. K.H. Ahmad Dahlan, Cireundeu, Kec. Ciputat Timur., Kota Tangerang Selatan, Banten 15419

[*] *fajartri306@gmail.com*

ABSTRACT

Internet is defined as an interconnected network which can literally be interpreted as a connected network. Simply put, the Internet is Simply put, the Internet is a assembly of interconnected computers. Part of the Internet is the World Wide Web (WWW), or what is now commonly known as web technology. Information on the Web is one of the means of communicating information quickly, up-to-date, and efficiently. As web usage grows and diversifies, there are other things to consider. It's the security of the website itself. Often referred to as web security or web security, it basically means protecting a website or web application by detecting, preventing, and responding to cyberthreats. The research uses Secure Socket Layer as one of the security protocols that protects transactions on websites with advanced data encryption techniques.
Keywords*: Public Key Infrastructure, Digital Signature*

ABSTRAK

Internet didefinisikan sebagai interconnected network yang secara harfiah dapat diartikan sebagai jaringan yang terhubung. Sederhananya, Internet adalah kumpulan komputer yang terhubung satu sama lain. Bagian dari Internet adalah World Wide Web (WWW) atau yang sekarang biasa dikenal dengan teknologi Web. Informasi melalui web merupakan salah satu sarana untuk menyampaikan informasi dengan cepat, terbaru dan efisien. Disamping penggunaan web yang terus meningkat dan beragam ada hal lain yang perlu diperhatikan yaitu mengenai keamanan situs web itu sendiri. Keamanan dunia maya, atau sering disebut dengan cyber-secure, pada dasarnya berarti melindungi situs web atau situs web dengan mengidentifikasi, mencegah, dan menanggapi ancaman dunia maya.
Kata Kunci: *Infrastruktur Kunci Publik, Tanda Tangan Digital*

DOI:https://

PENDAHULUAN

Pada era sekarang, kebutuhan terhadap teknologi semakin meningkat. Hal ini disebabkan karena teknologi membantu kita dalam berbagai hal, mulai dari menghemat waktu dan tenaga hingga meningkatkan efisiensi dan produktivitas. Teknologi juga memungkinkan kita untuk berkomunikasi dan bertransaksi dengan lebih cepat dan mudah, serta membantu kita untuk mengakses informasi dan pengetahuan yang lebih luas.

Salah satu penerapan teknologi yang saat ini berkembang ialah kriptografi yang merupakan ilmu pengetahuan serta seni yang bertujuan untuk melindungi kerahasiaan pesan (data atau informasi) dengan teknik merahasiakan ke dalam bentuk kode yang tidak memiliki arti.

Dalam perkembangan teknologi informasi, terdapat sebuah sistem yang menggunakan prinsip kriptografi yaitu Public Key Infrastructure (PKI) yang merupakan sistem dasar dengan sebuah portal yang khusus diciptakan untuk tujuan pengelolaan penerbitan, pendistribusian, identifikasi serta pencabutan public key sertifikat. Sistem dalam PKI ini antara lain ialah serangkaian kebijakan serta prosedur yang di percayakan pada pengguna sertifikat. Sistem ini memastikan public key hanya dapat digunakan atau dibaca oleh pengguna sertifikat digital yang sudah diterbitkan saja. Informasi yang tertera pada dashboard PKI akan dienkripsi serta ditransmisikan dengan aman. Terdapat juga sebuah bentuk dari tanda tangan digital yang merupakan tanda tangan yang dibuat menggunakan fungsi hash dan algoritma kriptografi kunci publik. Sehingga dengan adanya digital signature dapat dimanfaatkan untuk penandatangan sebuah dokumen dengan valid.

Public Key Infrastructure (PKI) dan digital signature merupakan dua konsep yang saling terkait dalam teknologi kriptografi. PKI menyediakan sebuah sistem yang menggunakan pasangan kunci publik-privat untuk mengenkripsi dan mendekripsi informasi. Digital signature adalah sebuah tanda tangan elektronik yang digunakan untuk memverifikasi identitas pengirim dan integritas pesan.

Penerapan PKI memungkinkan pengirim untuk mengenkripsi pesan menggunakan kunci publik penerima, sehingga hanya penerima yang memiliki kunci privat yang dapat membuka pesan tersebut. Digital signature juga dapat digunakan untuk memverifikasi identitas pengirim dan integritas pesan yang dienkripsi menggunakan PKI. Dengan demikian, PKI dan digital signature saling melengkapi satu sama lain dalam meningkatkan keamanan dan kepercayaan dalam berkomunikasi dan bertransaksi secara elektronik.

Dengan sistem yang disebutkan diatas dan semuanya bermuara kepada kriptografi, diyakini bahwa dapat mengamankan aset ataupun informasi digital yang dimana pada era teknologi seperti sekarang banyak sekali ditemukan kecurangan ataupun tindakan kejahatan dalam dunia digital.

Salah satu tindak kejahatan yang sering terjadi ialah pemalsuan dokumen digital. Dimana terdapat kasus dimana ada pemalsuan sebuah dokumen digital dengan mengubah isi di dalam dokumen tersebut sehingga dipercaya jika dokumen yang dipalsukan tersebut merupakan dokumen yang asli. Ada banyak hal yang dapat diubah seperti penyalahgunaan tanda tangan ataupun pemalsuan nama yang tercantum serta berbagai macam informasi lainnya

yang dapat di manipulasi. Hal ini sangat lah merugikan berbagai pihak dikarenakan keaslian dokumen menjadi sesuatu yang ditakutkan karena tidak diketahui apakah dokumen digital tersebut benar keasliannya. Ini dapat menyebabkan kerugian yang besar serta terdapat berbagai macam bentuk kejahatan yang dimulai dari bentuk manipulasi ini.

Salah satu contoh bentuk dokumen yang dapat dimanipulasi ialah dokumen surat digital yang dikeluarkan oleh sebuah organisasi. Dalam berjalannya sebuah organisasi, ada kala nya mengeluarkan surat dalam bentuk digital sehingga mudah dalam pemberitahuan informasi kepada yang ditujukan. Namun dengan adanya surat digital dapat terjadi penyalahgunaan seperti manipulasi surat. Hal ini dapat menyebabkan misinformasi yang dapat memberikan masalah kedepannya.

Dengan adanya pemanfaatan kriptografi, public key infrastructure serta tanda tangan digital diharapkan bahwa keaslian sebuah dokumen digital dapat terjaga. Namun timbul sebuah pertanyaan apakah benar jika dengan pemanfaatan teknologi tersebut, maka manipulasi tidak dapat dilakukan lagi. Hal ini menjadi sebuah pertanyaan yang harus diuji kebenarannya dan nantinya hasil dari penelitian tersebut dapat diterapkan di kehidupan sehari-hari.

Dalam penelitian ini, akan dijelaskan apakah ketika terdapat sebuah dokumen digital dalam hal ini surat organisasi digital yang dimanipulasi dan sebelumnya telah dilalui proses digital signature dan proses-proses lain apakah keaslian dokumen tersebut masih dapat terjaga atau terdapat perubahan yang menyebabkan dokumen tersebut tidak valid.

METODE PENELITIAN

1. Penandatangan Dokumen Digital

Dalam proses ini, terbagi atas tiga langkah:

a. Proses menghitung nilai hash dokumen.
b. Melakukan proses enkripsi nilai yang di dapat dengan penggunaan kunci privat pemilik tanda tangan.
c. Membubuhkan tanda tangan pada file dokumen.

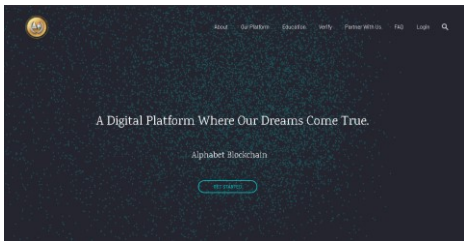
Selanjutnya untuk proses pemeriksaan validitas tanda tangan digital caranya antara lain:

a. Proses pemisahan dokumen asli dan tanda tangan dari file digital.
b. Proses dekripsi tanda tangan yang nantinya menghasilkan nilai hash.
c. Proses perhitungan nilai hash dokumen dan hasil nya ialah nilai hash perhitungan.
d. Perbandingan nilai hash tanda tangan dengan nilai hash perhitungan. Dalam proses ini jika nilai hash sama maka dokumen tak pernah diubah sejak ditandatangani.

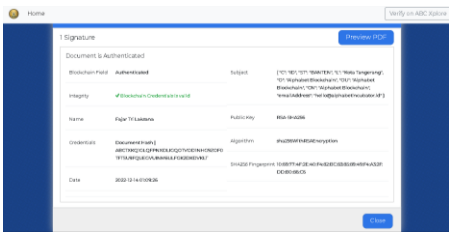
2. Pembuatan Surat Digital

Dalam proses ini, permintaan pembuatan sertifikat dari berbagai media, dalam hal ini penulis menggunakan Alphabet Blockchain, sebuah website yang dapat melakukan proses kriptografi kepada sebuah dokumen dengan menggunakan blockchain. Alphabet Blockchain memfasilitasi aktivitas kriptografi sebuah dokumen sehingga dalam prosesnya akan menghasilkan nilai hash dan dapat melakukan proses penandatangan dan pembuatan surat digital. Dalam hal ini, penulis melakukan proses penandatangan dokumen digital dan pembuatan surat digital menggunakan Alphabet Blockchain. Sehingga akan dihasilkan sebuah

dokumen yang telah melalui proses penandatangan digital.



Gambar 1. Tampilan website Alphabet Blockhain



Gambar 2. Verifikasi keaslian dokumen yang sudah di tanda tangan digital di Alphabet Blockhain

3. Gambaran Umum Alur Kerja Sistem

Sistem yang dibangun dalam penelitian ini merupakan suatu bentuk layanan infrastruktur kunci publik yang bersifat sederhana serta menjadi pondasi utama layanan surat organisasi digital. Studi kasus dalam penelitian ini adalah pengembangan sistem surat organisasi digital.

Metode Pengumpulan Data

Dalam melakukan pengumpulan data, penulis melalui proses analisis data dan membuat informasi yang akan digunakan untuk mengetahui permasalahan yang dihadapi.

a. Studi Lapangan

Metode pengumpulan data dengan melakukan pengamatan atau datang langsung ke lokasi tempat penelitian.

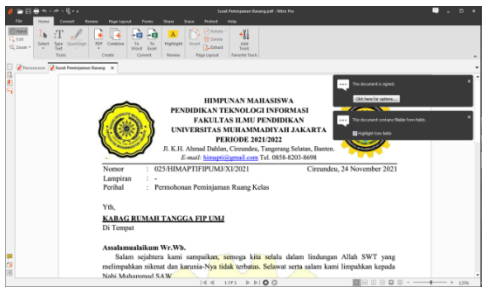
b. Studi Literatur

Metode pengumpulan data melalui perbandingan hasil karya tulis dengan menggunakan tema yang sama, namun berbeda maksud dan tujuan.

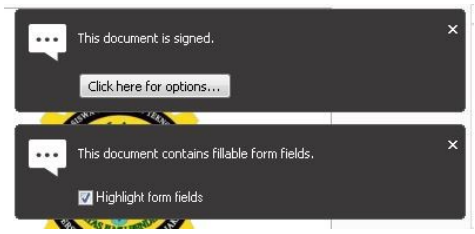
HASIL DAN PEMBAHASAN

1. Hasil Pembuatan Surat Digital

Hasil dari pembuatan surat digital ditunjukan pada Gambar 3, dalam proses ini penulis menggunakan aplikasi NitroPDF sebagai penampil file dokumen bertipe *.pdf* yang sudah melalui proses penandatangan digital sebelumnya. Tampilan dari dokumen yang telah ditandatangan digital ialah muncul notifikasi di samping kanan atas.



Gambar 3. Tampilan Dokumen yang telah melalui proses tanda tangan digital



Gambar 4. Notifikasi dokumen yang telah melalui proses tanda tangan digital

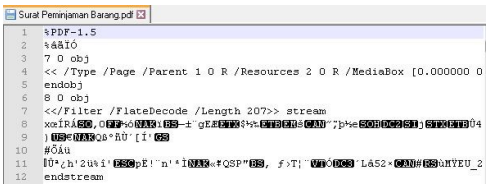
Selanjutnya ketika dilihat bukti tanda tangan digital, akan menampilkan tampilan seperti Gambar 5 disertai dengan berbagai keterangan. Dengan

nilai hash : ABCTXKQ1GLQFPNXDLIGQOTVOD1NHG9ZOF0TFTSU9FQUEGVUINM6ULFGK2DKDVKLT
Nilai hash yang tercantum di dalam dokumen ini sama dengan ketika melakukan verifikasi di Alphabet Blockchain.

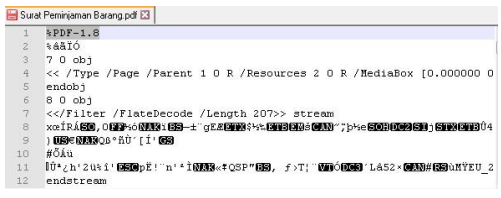
Gambar 5. Tampilan Keterangan Tanda Tangan Digital Dokumen

2. Percobaan Manipulasi Dokumen

Proses pertama yang dilakukan peneliti ialah manipulasi dokumen menggunakan Notepad++ dengan mengubah isi dokumen untuk melihat nantinya apakah dokumen masih dapat dideteksi keaslian nya.

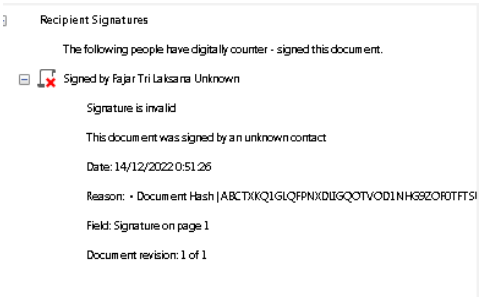


Gambar 6. Bentuk asli dokumen di Notepad++



Gambar 7. Manipulasi dokumen di Notepad++ pada line 1

Setelah di cek melalui NitroPDF seperti pada Gambar 8, notifikasi dokumen tetap ditampilkan, namun keterangan tanda tangan digital menampilkan hasil yang berbeda. Walaupun terdapat nilai hash namun tidak diketahui siapa yang menandatangani.



Gambar 8. Tampilan Keterangan Tanda Tangan Digital Dokumen yang telah dimanipulasi

Manipulasi kedua ialah dengan mengubah isi tanda tangan yang ada di dokumen *.pdf* dengan cara mengkonversi nya ke bentuk *.word* lalu di konversi ulang ke *.pdf* dengan tanda tangan baru.

Gambar 9. Bentuk Tanda Tangan Digital pada dokumen asli

Gambar 10. Bentuk Tanda Tangan Digital pada dokumen yang dimanipulasi

Dalam percobaan ini, ketika dokumen di ubah isinya. Maka tidak muncul notifikasi tanda tangan digital, sehingga ketika dilakukan proses manipulasi seperti tadi tanpa proses

kriptografi akan menampilkan sebuah dokumen biasa. Dalam hal ini keaslian dokumen dapat dilihat dengan cara seperti melihat keterangan dari tanda tangan digital dokumen tersebut dilakukan oleh organisasi yang bersangkutan atau tidak.

SIMPULAN

Simpulan yang diperoleh pada implementasi perancangan infrastruktur kunci publik pada pembuatan surat organisasi digital menggunakan digital signature ialah bahwa ketika sebuah dokumen digital telah melalui proses public key infrastructure dan digital signature maka dokumen tersebut telah tervalidasi dan sertifikasi sehingga ketika dibuka di aplikasi pembaca PDF seperti dalam penelitian ini ialah NitroPDF akan muncul notifikasi bahwa dokumen telah di tanda tangan digital dan disertifikasi. Ketika terjadi manipulasi dalam file dokumen digital tersebut maka ketika dilihat kembali di aplikasi NitroPDF, tanda tangan digital dan sertifikasi dokumen tersebut akan bersifat *invalid* sehingga bisa dipastikan bahwa dokumen tersebut telah melalui proses manipulasi dan bukan dokumen yang asli dikeluarkan oleh pihak yang berwenang.

DAFTAR PUSTAKA

Carnley, Renee, and Sikha Bagui. "A Public Infrastructure for a Trusted Wireless World." *Future Internet* 14.7 (2022): n. pag.

Dakhi, Oskah et al. "Analisis Sistem Kriptografi Dalam Mengamankan Data Pesan Dengan Metode One Time Pad Cipher." *INVOTEK: Jurnal Inovasi Vokasional dan Teknologi* 20.1 (2020): 27–36.

Hepp, Thomas et al. "Exploring Potentials and Challenges of Blockchain-Based Public Key Infrastructures." *INFOCOM 2019 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2019* April (2019): 847–852.

Melo, Wilson et al. "Public-Key Infrastructure for Smart Meters Using Blockchains." *2020 IEEE International Workshop on Metrology for Industry 4.0 and IoT, MetroInd 4.0 and IoT 2020 - Proceedings* June (2020): 429–434.

Nouf Aldahwan, and Daniyal Alghazzawi. "Use of Blockchain in Public Key Infrastructure (PKI): A Systematic Literature Review." *International Journal of Computer Science and Information Security* 18.6 (2020): n. pag.

Sinaga, Theresia Elina. "Sertifikat SSL Dan Public Key Infrastructure (PKI)." *SSLIndonesia.com*. N.p., 2022. Diakses pada 13 Desember 2022.

Yuniati, Trihastuti, and Muhammad Fajar Sidiq. "Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital Sebagai Alternatif Pengesahan Dokumen Di Masa Pandemi." *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)* 4.6 (2020): n. pag.