Sistem desain: implementasi tandatangan digital untuk otentikasi dokumen keuangan menggunakan metode modified-ECDSA

by Ivan Firmansyah

Submission date: 20-Nov-2019 10:34PM (UTC+0700)
Submission ID: 1217878983
File name: Revisi_Ivan2.pdf (321.72K)
Word count: 1467
Character count: 9520

Sistem desain: implementasi tandatangan digital untuk otentikasi dokumen keuangan menggunakan metode *modified*-ECDSA

Abstract— **Tulisan ini membahas tentang desain sistem untuk mengimplementasi tandatangan digital pada dokumen keuangan sebagai otentikasi dokumen menggunakan Bahasa pemrograman Java. Tandatangan digital adalah salah satu layanan keamanan pada bidang kriptografi yang memiliki fungsi untuk mengamankan dokumen dari serangan *man in the middle attack* atau serangan dari pihak ketiga. Tulisan ini dibuat karena dokumen keuangan merupakan sebuah dokumen yang sangat vital yang perlu dijaga keasliannya. Saat ini pertukaran informasi melalui jalur internet sangat aktif digunakan. Disisi lain, komunikasi yang dilakukan menggunakan jalur internet juga sangat rentan terhadap kejahatan siber. Sehingga untuk mengamankan sebuah dokumen keuangan sekaligus menjaga keaslian datanya dilakukanlah implementasi tandatangan digital dengan menggunakan metode modified-ECDSA. Hasil dari penelitian yang dilakukan berupa prototipe dan rancangan sistem tandatangan digital berupa aplikasi desktop.**

Keywords;Digital Signature,Kriptografi,ECDSA

I. PENDAHULUAN

Dalam era digital,ada proses legalisasi suatu berkas konvensional menjadi berkas digital.Dalam proses legalisasi berkas dibutuhkan bukti yang dapat digunakan untuk acuan bahwa berkas tersebut dikirim dan diakui oleh pihak yang membuat tanda tangan.Tanda tangan telah lama digunakan untuk membuktikan autentikasi dan keabsahan dari suatu dokumen.Proses legalisasi ini bisa diterapkan dengan menggunakan tanda tangan digital(digital signature) [1].

Saat ini aktifitas pertukaran data dan informasi melalui jalur Internet sangatlah tinggi, seiring dengan perkembangan teknologi yang digunakan. Selain itu, terjadi pula peningkatan kejahatan siber. Terdapat berbagai macam bentuk pertukaran data dan informasi yang dikirimkan melalui jalur Internet, diantaranya dokumen, foto, audio, video, dan lainnya. Hal yang rentan adalah pada saat dokumen keuangan dikirimkan melalui jalur Internet. Kemungkinan kejahatan-kejahatan siber bisa saja terjadi, sehingga perlu dijaga keotentikan data dan informasi yang terdapat pada sebuah dokumen keuangan.

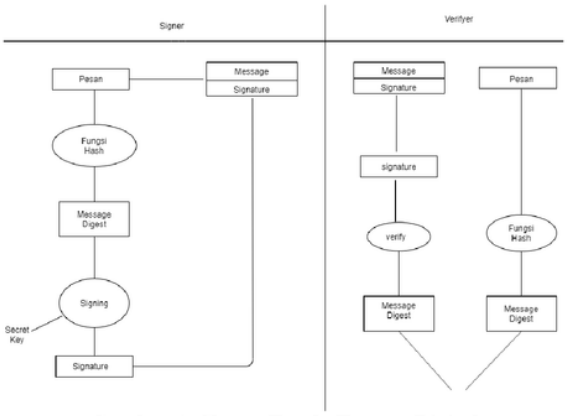
Berdasarkan pada permasalahan tersebut, maka untuk menjaga keotentikan dan mengamankan dokumen digunakanlah teknik tandatangan digital. Penggunaan digital signature untuk autentikasi dokumen keuangan dilakukan agar dokumen tersebut tidak dimodifikasi oleh pihak-pihak tertentu untuk mendapat keuantungan pribadi.Modified ECDSA adalah salah satu algoritma yang digunakan untuk membuat digital signature [5],modified ECDSA memiliki kelebihan dibanding dengan algoritma lain: (1) memberikan keamanan yang lebih besar dengan ukuran kunci yang lebih kecil, (2) Menawarkan implementasi yang berguna dan ringkas untuk operasi kriptografi yang membutuhkan lebih banyak chip kecil (3) Karena chip yang lebih kecil menghasilkan panas lebih sedikit dan konsumsi daya lebih sedikit. Maka dari itu penelitian ini disulkan menggunakan metode modified ECDSA

Pada tulisan ini, pembahasan penulisan dibagi menjadi tiga bagian. Pembahasan mengenai teori dan kajian terhadap penelitian terkait dengan tandatangan digital dibahas pada bagian sesi dua. Pembahasan mengenai metode yang digunakan pada penelitian tandatangan digital dibahas pada bagian sesi tiga. Perancangan dan desain sistem yang akan direkomendasikan dibahas pada bagian sesi empat. Sehingga kesimpulan dari keseluruhan tulisan ini dibahas pada bagian sesi lima.

II. KAJIAN PUSTAKA

A. Tanda Tangan Digital

Tanda tangan digital merupakan langkah otentikasi untuk memperbolehkan pemilik berkas menambahkan kata sandi [4]. Tanda tangan yang dimaksud bukan tanda tangan yang didigitalkan dengan scanner,melainkan nilai kriptografi yang berdasar pada pesan dan kunci.Tanda tangan digital memiliki 3 proses yaitu pembangkitan kunci,pembubuhan tanda tangan digital dan konfirmasi keabsahan tanda tangan digital [1]



Gambar 1. Skema Tanda Tangan Digital

B. ECDSA

ECDSA merupakan salah satu algoritma yang diaplikasikan untuk pembuatan tanda tangan digital dengan analogi kurva elips. ECDSA dikenalkan pada tahun 1992 oleh seseorang bernama Scott Vanstone ,lalu pada tahun 1998 memperoleh standar ISO14888-3.Tahun 1999 ditetapkan menjadi standar ANSI X9.62 Pada tahun 2000 ECDSA ditetapkan sebagai standar IEEE (Institute of Electrical and Electronics Engineers) IEEE 1363-2000 serta standar NIST (National Institute of Standards and Technology) yaitu FIPS 186-2. [2]

Perbandingan Panjang kunci RSA dan ECDSA

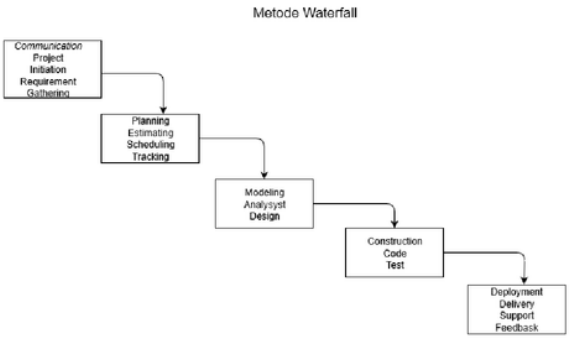
RSA	ECDSA
1024	192
2048	256

C. Modified ECDSA

Modified-ECDSA adalah sebuah modifikasi metode dari EDCSA untuk mempercepat proses algoritma ECDSA biasa. Modified-ECDSA mengubah waktu verifikasi algoritma reguler dari lambat ke cepat. Ukuran kunci yang lebih kecil dari ECDSA berpotensi memungkinkan perangkat yang ringan dan sistem nirkabel yang kurang mampu menggunakan kriptografi untuk transmisi data yang aman, verifikasi data dan lebih sedikit membutuhkan daya.Memori dan bandwidth yang dioptimalkan dan pembuatan tanda tangan yang lebih cepat.

III. METODOLOGI PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah metode waterfall.Metode Waterfall adalah sebuah metode pengembangan aplikasi dimana setiap fase tergantung dari hasil yang sebelumnya dan sesuai dengan tugasnya masing masing.[6]Langkah-Langkah dalam metode waterfall yaitu requirement analisis (Analisis Kebutuhan Pengguna), System Design (Desain Sistem), Implementation (Coding), Integration & Testing (Pengujian Sistem), Operation & Maintenance (Pemeliharaan Perangkat Lunak).



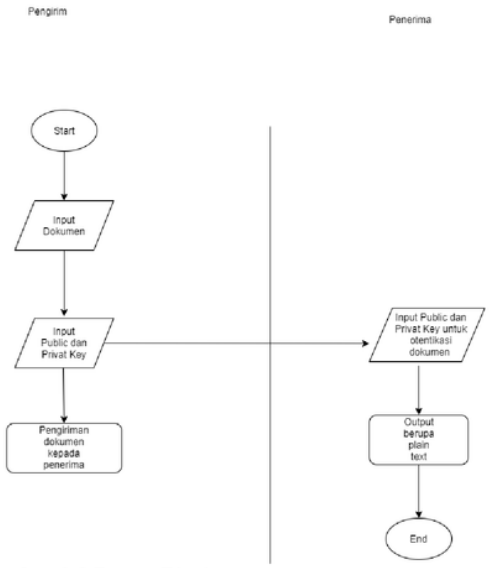
Gambar 2 2 Metode Waterfall

Pada penelitian ini tahapan yang akan dikerjakan adalah tahapan analisis kebutuhan dan desain sistem, hal ini dikarenakan pada penulisan ini hanya membahas tentang desain sistem.

A. Analisis Kebutuhan

Ketika pengirim akan mengirimkan suatu pesan, sistem akan meminta pesan berbentuk dokumen yang harus disiapkan oleh pengirim.Selanjutnya dokumen tersebut akan melalui proses enkripsi oleh sistem dengan menggunakan tekhnik enkripsi ECDSA.Proses ECDSA melakukan enkripsi pada dokumen .Setelah dokumen selesai dienkripsi, pengirim akan menerima overview dokumen yang telah dienkripsi tersebut dan dokumen dapat langsung dikirim ke penerima

Penerima dapat melakukan verifikasi tanda tangan digital. Verifikasi tanda tangan digital dapat dijalankan otomatis saat memilih berkas yang akan dibaca.Hasil verifikasi akan ditampilkan oleh program apakah valid atau invalid.telah dienkripsi tersebut dan dokumen dapat langsung dikirim ke penerima.



Gambar 2 2 Proses Bisnis

Pada sistem tandatangan digital ini terdapat satu aktor yang akan menjalankan sistem yaitu user. Aplikasi yang akan dibuat terdiri dari dua jenis. Aplikasi yang berada disisi pengirim dan penerima. Kemudian kebutuhan sistem akan dibagi menjadi tiga bagian yakni: input, proses, dan output. Penjabaran analisis kebutuhan sistem dibahas sebagai berikut:

Aplikasi dari sisi pengirim:

a. Analisis kebutuhan input
   -input dokumen
   -input public key & privat key untuk dikirimkan kepada penerima dokumen
b. Analisis kebutuhan proses
   Pada tahap ini metode ecdsa akan melakukan enrkipsi terhadap dokumen keuangan yang akan dikirim.Setelah melakukan enkripsi kepada dokumen keuangan selanjutnya dokumen akan dikirimkan kepada penerima
c. Analisis kebutuhan output
   -plaintext

Aplikasi dari sisi penerima:

a. Analisis kebutuhan input
   -input dokumen
   -input public key untuk validasi
b. Analisis kebutuhan proses
   -Tahap ini metode ecdsa akan melakukan otentikasi untuk membuktikan apakah dokumen yang dikirim adalah asli ataupun tidak.Jika dokumen yang dikirim tidak asli maka aka nada pemberitahuan.
c. Analisis kebutuhan output
   -plaintext

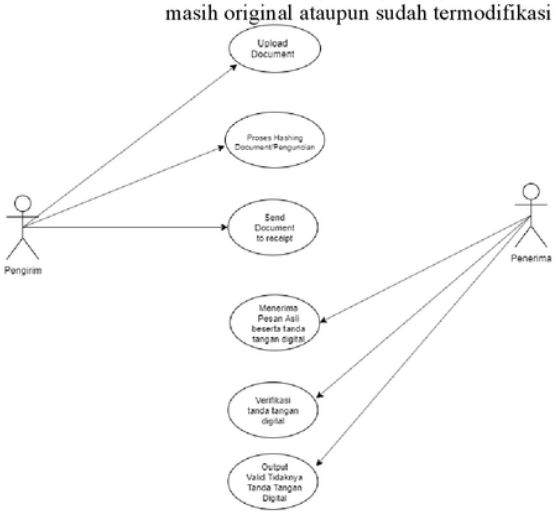
Adapun fitur-fitur dari aplikasi ini adalah

Dari Sisi Pengirim

- Upload dokumen keuangan kepada penerima
- Penyisipan Digital Signature pada dokumen yang akan dikirimkan kepada penerima
- Pengiriman dokumen yang telah disisipi digital signature kepada penerima

Dari Sisi Penerima

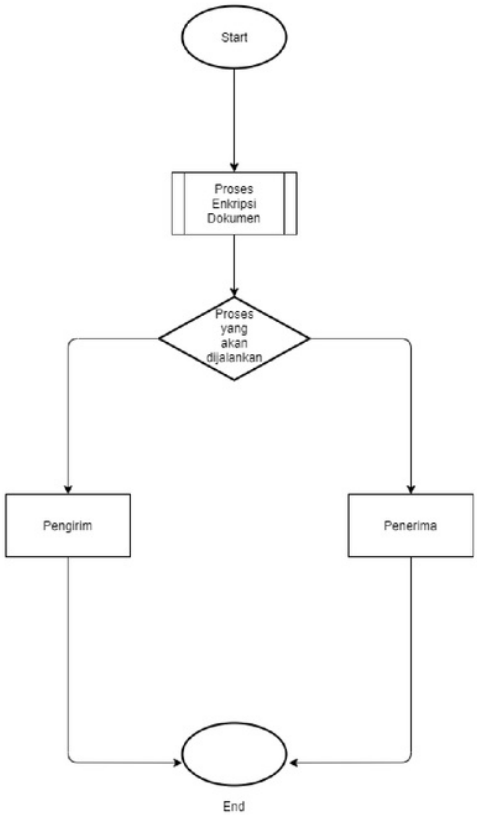
- Penerima menerima pesan dan juga digital signature
- Penerima melakukan verifikasi tanda tangan digital
- Penerima menerima output dari pesan yang dikirim oleh pengirim apakah pesan tersebut masih original ataupun sudah termodifikasi



Gambar 2 3 Use Case Diagram

B. Design

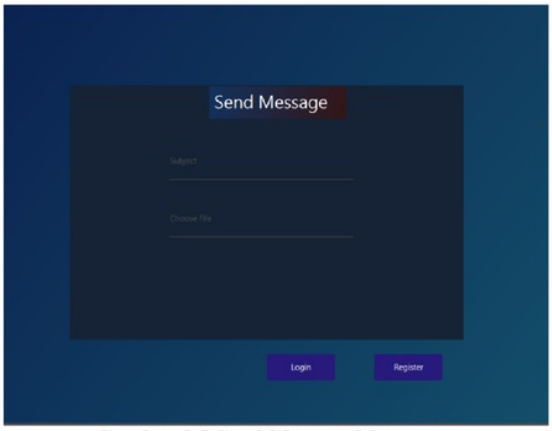
Untuk menerapkan modifed ECDSA harus merancang program terlebih dahulu yang bertujuan untuk meringkas kesulitan agar mudah dalam penerapannya



Gambar 2 4 Use Case Alur Aplikasi

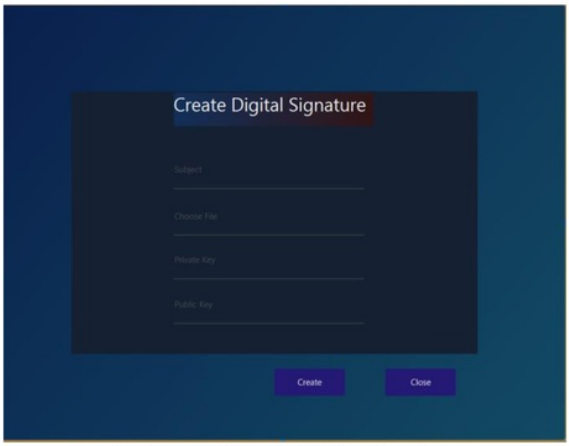
(Interface Aplikasi)

- Send Message
  Pada menu ini pengirim dapat memilih dokumen keuangan mana yang akan dikirimkan kepada penerima



Gambar 2 5 Send Message Menu

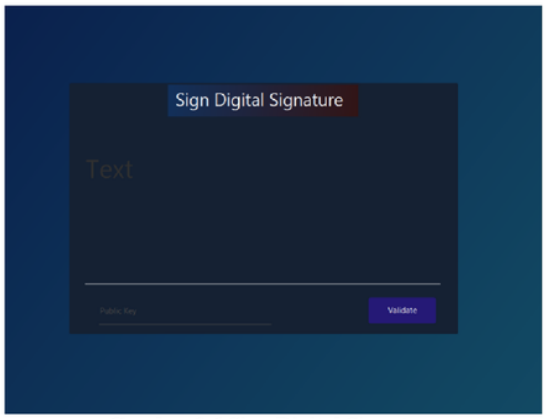
- Create Digital Signature
  Menu ini pengirim dapat memilih ingin menggunakan metode yang akan digunakan untuk mengenkripsi dokumen yang akan dikirim nantinya output dari dokumennya berupa file pdf yang sudah diselipkan digital signature didalamnya



Gambar 2 6 Create Digital Signature

- Validate Digital Signature
  Setelah konten file ditampilkan, maka validasi tanda tangan digital dapat dijalankan dengan menekan tombol Validasi. Jika tombol validasi ditekan maka akan muncul jendela pilihan untuk memilih file yang berisi kunci publik pengirim,. Setelah kunci publik dipilih, untuk menentukan apakah informasi yang dikirim valid atau tidak informasi akan diproses

terlebih dahulu. Jika informasi yang dikirimkan benar, maka status bar akan menampilka pesan Valid; jika tidak, pesan Tidak Valid akan muncul di status bar jika kunci tidak cocok dengan tanda tangan yang disisipkan dalam file



Gambar 2 6 Sign Digital Signature

Kesimpulan

Penggunaan metode Modified ECDSA untuk melakukan enkripsi dan dekripsi terhadapat dokumen terbukti lebih unggul daripada metode digital signature yang lain baik.Pengguna tidak akan menunggu terlalu lama untuk mengenkripsi dan mendekripsi data, Waktu verifikasi antara ECDSA reguler dan RSA berbeda.Karena ECDSA membutuhkan sumber daya yang lebih sedikit dibandingkan dengan RSA.Algoritma (Modified ECDSA) telah memperpendek perbedaan antara ECDSA dan RSA dalam hal waktu penandatanganan dan verifikasi.Waktu yang diperlukan RSA untuk menghasilkan tanda tangan cenderung lebih lambar karena kunci yang lebih besar sedangkan,Waktu yang dibutuhkan untuk menghasilkan tanda tangan pada metode ECDSA cenderung lebih cepat dibandingkan algoritma sejeni

IV. REFERENSI

[1] A. I. Ali, "COMPARISON AND EVALUATION OF DIGITAL SIGNATURE SCHEME EMPLOYED IN NDN NETWORK," p. vol 5, 2015.

[2] K. S. S. Aqeel Khalique, "Implementation of Elliptic Curve Digital Signature Algorithm," p. 7, 2010.

[3] A. Triwinarko, "Elliptic Curve Digital Signature Algorithm (ECDSA) Departemen Teknik Informatika ITB," vol. 6, 2002.

[4] R. Munir, "Tandatangan Digita".

[5] I. W. S. M. R. M. S. M. Pualam Sendi A P, "IMPLEMENTASI ALGORITMA ECDSA UNTUK PENGAMANAN E-MAIL (VERIFIKASI KEASLIAN PESAN)," 2010.

[6] R. e. Al, "Waterfall Metode," 2013.

[7] A. A. Aziz, "IMPLEMENTASI TANDA TANGAN DIGITAL MENGGUNAKAN METODE ONG-SCHNORR-SHAMIR DAN EUCLIDEAN PADA TEKS," 2009.

Sistem desain: implementasi tandatangan digital untuk otentikasi dokumen keuangan menggunakan metode modified-ECDSA

ORIGINALITY REPORT

17%	15%	1%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.eepis-its.edu Internet Source	7%
2	budi.paume.itb.ac.id Internet Source	4%
3	repository.uinjkt.ac.id Internet Source	2%
4	Submitted to Universitas Brawijaya Student Paper	1%
5	docplayer.info Internet Source	1%
6	Submitted to Ilia State University Student Paper	1%
7	text-id.123dok.com Internet Source	1%

Exclude quotes	Off	Exclude matches	Off

Exclude bibliography On