Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 25 ; Nomor 1 ; Februari 2026 ; Page 111-118
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

# Implementasi Digital Signature Pada Faktur Elektronik Dengan Menggunakan Algoritma RSA

**Fadil Fauzi[1], Abdullah Muhazir[2], Egi Affandi[3]**
[1,2,3] Sistem Informasi, Stmik Triguna Dharma
Email: [1]fadilfauzi@outlook.co.id, [2]muhazir@gmail.com, [3]egi.afandi46@gmail.com
Email Penulis Korespondensi: fadilfauzi@outlook.co.id

**Article History:**
Received Jan 16th, 2026
Revised Feb 10th, 2026
Accepted Feb 27th, 2026

**Abstrak**

Digital signature atau tanda tangan digital adalah bentuk pengesahan elektronik yang digunakan untuk mengamankan keaslian dokumen elektronik, pada PT. Escoplus Mitra Indonesia adalah salah satu perusahaan penyedia jasa konsultasi energi yang biasanya menggunakan faktur sebagai bukti biaya pembayaran perusahaan tersebut. Dimana faktur tersebut bisa saja dimanipulasi isinya oleh orang yang tak bertanggung jawab dan bisa berdampak negatif pada perusahaan tersebut. Dari masalah tersebut maka dibuatlah sebuah sistem faktur elektronik dengan digital signature menggunakan kriptografi asimetris yaitu algoritma RSA (Rivest-Shamir-Adleman). agar dapat meningkatkan keamanan dan kemudahan verifikasi dari faktur tersebut. Hasil dari penelitian ini menunjukan bahwa sistem yang dibangun dengan berbasis web dapat membantu perusahaan dalam meminimalisir manipulasi dari faktur elektronik dengan digital signature dengan metode RSA.

**Kata Kunci :** Digital Signature, RSA, Kriptografi, Faktur Elektronik, Keamanan Digital

***Abstract***

*Digital signature is used to secure the authenticity of electronic documents, PT Escoplus Mitra Indonesia is one of the energy consulting service providers that usually uses invoices as proof of the company's payment costs. Where the invoice can be manipulated by irresponsible people and can have a negative impact on the company. From this problem, an electronic invoice system with a digital signature using asymmetric cryptography, namely the RSA (Rivest-Shamir-Adleman) algorithm, was created in order to increase the security and ease of verification of the invoice. The results of this study show that a web-based system can help companies minimize manipulation of electronic invoices with digital signature using the RSA method.*

***Keyword :*** *Digital Signature, RSA, Cryptography, Electronic Invoice, Digital Security*

## 1. PENDAHULUAN

Faktur adalah dokumen yang dibuat oleh penjual kepada pembeli sebagai bukti bahwa suatu barang atau jasa telah dibeli dan telah dibayar[1]. Faktur biasanya berisi informasi tentang barang atau jasa yang dibeli, jumlah yang harus dibayar, tanggal pembelian, dan informasi lainnya seperti nomor faktur, nama dan alamat penjual dan pembeli, serta metode pembayaran. Faktur biasanya dikeluarkan oleh penjual setelah barang atau jasa telah dikirim atau diberikan kepada pembeli, dan seringkali faktur ini digunakan sebagai bukti transaksi oleh kedua belah pihak.

Seiring berkembangnya teknologi informasi, pemalsuan terhadap faktur dapat dengan mudah dilakukan oleh orang-rang yang tidak bertanggungjawab. Bentuk pemalsuan faktur pada umumnya dilakukan dengan memanipulasi isi faktur dengan membuat faktur baru menggunakan desain dan tampilan yang sama dengan aslinya. Biaya yang digunakan untuk pemalsuan faktur juga semakin rendah, sehingga kerentanan terhadap pemalsuan meningkat. Hal ini mengakibatkan kebutuhan akan kerahasiaan informasi serta penjagaan atas keaslian faktur semakin meningkat. Dalam perkembangan teknologi saat ini verifikasi manual menjadi kurang efektif karena membutuhkan waktu dan upaya yang lebih atau dengan prosedur yang cenderung rumit [2].

PT. Escoplus Mitra Indonesia adalah salah satu perusahaan penyedia jasa konsultasi energi. Dalam proses konsultasi mereka biasanya menggunakan faktur sebagai bukti biaya pembayaran konsultasi jasa perusahaan tersebut. Dimana faktur tersebut bisa saja dimanipulasi isinya oleh orang yang tak bertanggung jawab dan bisa berdampak negatif pada perusahaan

tersebut. Dari kondisi tersebut disarankan untuk menerapkan faktur elektronik dengan digital signature agar dapat meningkatkan keamanan dan kemudahan verifikasi dari faktur tersebut.

Dalam penelitian ini akan memanfaatkan dan mengimplementasikan faktur elektronik dengan digital signature. Penerapan digital signature dapat menggunakan kriptografi asimetris yaitu algoritma RSA (Rivest-Shamir-Adleman). Algoritma RSA merupakan jenis kriptografi asimetris yang sangat populer dan aman dengan penggunaan angka kunci yang semakin besar. Algoritma RSA dapat digunakan untuk pembentukan digital signature sehingga dapat melakukan validasi faktur dengan efektif dan efesien [3]. Algoritma hash yang digunakan dalam penelitian ini adalah MD5 (Message-digest 5). Algoritma MD5 merupakan salah satu algoritma fungsi hash yang dapat menerima input dengan panjang sembarang dan akan menghasilkan output berupa message digest dengan panjang 128 bit [4].

Cara kerjanya adalah dengan pembentukan kunci privat dan kunci publik untuk algoritma RSA. Lalu membuat hash dari data yang ingin di sign menggunakan algoritma MD5, setelah itu gunakan kunci publik yang sudah dibentuk untuk mengenkripsi hash yang sudah dibuat. Dengan tahapan tersebut jadilah digital signature yang bisa dimasukan didalam faktur. Untuk memverifikasi keaslian faktur tersebut dapat dilakukan dengan membuat hash dari data original dengan algoritma MD5 lalu mendekripsikan digital signature tersebut menggunakan kunci privat dan lakukan perbandingan antara digital signature yang sudah di dekripsi dengan nilai hash originalnya, jika nilainya sama maka signature tersebut valid dan data tidak diubah atau dimanipulasi.

## 2. METODOLOGI PENELITIAN

### 2.1 Tahapan Penelitian

Tahapan penelitian adalah proses dimana sebuah penelitian dapat distruktur secara logis dan sistematis sehingga mendapatkan hasil dari penelitian yang sesuai dengan yang diharapkan. Adapun dalam tahapan penelitian dilakukan beberapa teknik pengumpulan data sebagai berikut:

a. Observasi
b. Wawancara
c. Penerapan *digital signature* pada faktur elektronik menggunakan metode RSA

Wawancara yang dilakukan kepada bapak Ibrahim Alwie Damanik, ST selaku direktur PT. Escoplus Mitra Indonesia adalah untuk menanyakan apa yang menjadi masalah selama ini. Data yang dikumpulkan merupakan data primer yaitu merupakan faktur yang akan digunakan dalam proses penelitian.

### 2.2 Faktur Elektronik (*E-Invoice*)

Faktur elektronik, juga dikenal sebagai *E-Invoice*, adalah metode pembuatan dan pengiriman faktur secara digital antar bisnis atau antara bisnis dengan pelanggan. Tidak seperti faktur berbasis kertas tradisional, faktur elektronik dibuat, dikirim, dan diterima secara elektronik melalui sistem komputer, sehingga tidak memerlukan kertas dan pemrosesan manual. Sistem faktur elektronik dapat diintegrasikan dengan perangkat lunak akuntansi atau perencanaan sumber daya perusahaan untuk menyederhanakan proses pembuatan faktur, mengurangi kesalahan dan meningkatkan efisiensi. Faktur elektronik juga dapat memberikan pelacakan real-time terhadap pengiriman faktur dan status pembayaran [5][14].

### 2.3 Kriptografi

Kriptografi adalah ilmu yang mempelajari mengenai hal keamanan pada pesan atau dokumen agar tidak dapat dibaca maupun diubah oleh seseorang yang tidak memiliki hak [6]. Tujuan utama kriptografi adalah menjaga kerahasiaan, integritas, dan autentikasi informasi. Terdapat dua jenis algoritma kriptografi berdasar jenis kuncinya yaitu [7] [13] :

a. Algoritma simetri disebut juga sebagai algoritma konvensional adalah algoritma yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Algoritma simetri sering juga disebut sebagai algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci.
b. Algoritma asimetri didesain sedemikian sehingga kunci yang digunakan untuk enkripsi berbeda dari kunci yang digunakan untuk dekripsi.

### 2.4 Digital Signature

Digital signature adalah mekanisme kriptografi yang digunakan untuk memverifikasi keaslian dan integritas dokumen atau pesan elektronik [8]. Digital signature adalah bentuk tanda tangan elektronik yang didasarkan pada kriptografi kunci publik, yang memastikan bahwa tanda tangan hanya dapat dibuat oleh pemilik kunci privat yang terkait dengan kunci publik yang digunakan untuk tanda tangan.Tanda tangan digital digunakan dalam berbagai macam aplikasi, termasuk kontrak elektronik, perbankan online, dan layanan e-government. Digital Signature yang aman tidak dapat di ubah oleh penandatangan dikemudian hari dengan menyatakan bahwa tanda tangan itu dipalsukan. Dengan kata lain, Digital Signature dapat memberikan jaminan keaslian dokumen yang dikirim secara digital, baik jaminan tentang identitas pengirim dan kebenaran dari dokumen tersebut [9][15].

### 2.5 Message Digest 5 (MD5)

MD5 merupakan algoritma perbaikan dari MD4 yang dikembangkan oleh Ronald L. Rivest pada tahun 1991 yang dimana MD4 sudah tidak aman lagi. Algoritma MD5 memiliki panjang kode *hash* 128-bit yang dihasilkan

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 25 ; Nomor 1 ; Februari 2026 ; Page 111-118
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

melalui fungsi hash dari input panjang yang tak terbatas. MD5 adalah hasil pengembangan dari algoritma sebelumnya yaitu MD, MD2, MD3 dan MD4 yang telah digunakan diberbagai bidang sebagai pengamanan keaslian data [10][17].

MD5 adalah fungsi kriptografi satu arah yang digunakan di berbagai bidang untuk menjaga integritas data [11]. Algoritma ini memanfaatkan serangkaian algoritma non-linear untuk melakukan operasi melingkar, sehingga cracker tidak dapat mengembalikan data asli. Dalam kriptografi, dikatakan bahwa algoritma ini sebagai algoritma yang ireversibel, secara efektif dapat mencegah kebocoran data yang disebabkan oleh operasi invers. Baik secara teori maupun praktiknya algoritma ini memiliki keamanan yang baik, karena penggunaan algoritma MD5 tidak memerlukan pembayaran royalti, waktu, dan biaya yang lebih murah yang membuatnya digunakan secara luas dalam aplikasi non-rahasia secara umum.

### 2.6 Algoritma RSA (Rivest–Shamir–Adleman)

Pada tahun 1978, Ron Rivest, Adi Shamir, dan Leonard Adleman memperkenalkan sebuah algoritma kriptografi, yang pada dasarnya untuk menggantikan algoritma National Bureau of Standards (NBS) yang kurang aman. Yang paling penting, RSA mengimplementasikan kriptosistem kunci publik, serta tanda tangan digital. RSA termotivasi oleh karya-karya Diffie dan Hellman yang telah dipublikasikan beberapa tahun sebelumnya, yang menggambarkan ide algoritma tersebut, tetapi tidak pernah benar-benar mengembangkannya [12][16]. Adapun prosedur dalam algoritma RSA adalah sebagai berikut[17]:

a. Pembentukan kunci RSA
   Pilihlah dua bilangan prima $p\ dan\ q$ (1)
   $n = p * q$
   $\phi(n) = (p-1)(q-1)$
   $2 < e < \phi(n)\ dan\ gcd(e, \phi(n)) = 1$
   $d \equiv e^{-1}\ (mod\ \phi(n))$
b. Enkripsi pesan RSA
   $c = m^e\ (mod\ n)$ (2)
c. Dekripsi pesan RSA
   $m = c^d\ (mod\ n)$ (3)

## 3. HASIL DAN PEMBAHASAN

### 3.1 Deskripsi Pengujian Data

Adapun tahapan-tahapan dalam pengujian data dengan metode RSA dan MD5 yang sesuai dengan sub bab sebelumnya dan dengan menggunakan data sampel No. Faktur yang memiliki pesan teks “21”, berikutlah langkah-langkahnya:

a. Pesan di ubah kedalam bentuk hash MD5
   No. Faktur yang memiliki pesan teks “21” dibuah menjadi hash MD5 :
   H(m) = 3c59dc048e8850243be8079a5c74d079
b. Pembentukan kunci publik dan privat (1)
   1. Pilih nilai $p$ dan $q$ yang dimana keduanya merupakan bilangan prima
      $p = 89$ dan $q = 113$
   2. Hitung $n$ yang merupakan modulus untuk kunci publik dan privat, yang dimana $n = p * q$
      $n = 89 * 113$
      $= 10057$
   3. Pilih bilangan desimal $e$ yang dimana $2 < e < \phi(n)\ dan\ gcd(e, \phi(n)) = 1$. $e$ dan $\phi(n)$ bisa juga disebut sebagai relatif prima
      $e = 3$
   4. Tentukan $d$ dimana $d \equiv e^{-1}\ (mod\ \phi(n))$
      $d = 6571$
c. Proses *digital signature*
   1. Pesan yang telah diubah menjadi hash akan di ubah menjadi integer:
      H(m) = 3c59dc048e8850243be8079a5c74d079
      H(m) = [51, 99, 53, 57, 100, 99, 48, 52, 56, 101, 56, 56, 53, 48, 50, 52, 51, 98, 101, 56, 48, 55, 57, 97, 53, 99, 55, 52, 100, 48, 55, 57]
   2. Lalu pesan di enkripsi menggunakan rumus sebagai berikut:
      $c(m) = m^e\ (mod\ n)$
      $c(51) =$ 51 ^ 3 $mod$ 10057 (2)
      $c(51) =$ 1910
      Keseluruhan pesan yang di enkripsi sebagai berikut :
      $c(m) =$ 1910,4827,8079,4167,4357,4827,10022,9867,4647,4487,4647,4647,8079,10022,4316,

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 25 ; Nomor 1 ; Februari 2026 ; Page 111-118
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

9867,1910,5891,4487,4647,10022,5463,4167,7543,8079,4827,5463,9867,4357,10022,5463,4167

d. Verifikasi *digital signature*
   1. Hash pesan dari faktur yang ingin diverifikasi , “21” menggunakan metode MD5 sebagai berikut :
      h(m) = 3c59dc048e8850243be8079a5c74d079
   2. Setelah itu chiper yang diterima didekripsi menggunakan kunci privat dan kemudian di konversikan ke huruf ascii:
      $m(c) = c^d \ (mod\ n)$
      $m(1910) = 1910^{6571} \ (mod\ 10057)$ (3)
      $m(1910) = 51$
      $ascii(56) = 3$
      Keseluruhan pesan yang di dekripsi sebagai berikut:
      m(c) = 3c59dc048e8850243be8079a5c74d079
   3. Bandingkan nilai hash dari pesan di faktur h(m) dengan pesan yang telah di dekripsi, apabila hasilnya sama maka pesan tersebut terjaga integritasnya dan datanya tidak diubah sama sekali.

### 3.2 Implementasi Program

Hasil tapilan antarmuka adalah gambaran dari tampilan keseluruhan menu dari sistem yang telah dibangun beserta penjelasan dari setiap menu dan fungsinya. Berikut merupakan tampilan dari implementasi *digital signature* dengan metode RSA:

1. Halaman *Login*
   Halaman *login* merupakan tampilan awal dari sistem yang merupakan area di mana pengguna diminta untuk memasukkan informasi kredensial mereka, yaitu nama pengguna dan kata sandi, untuk mengakses akun dari sistem tersebut.

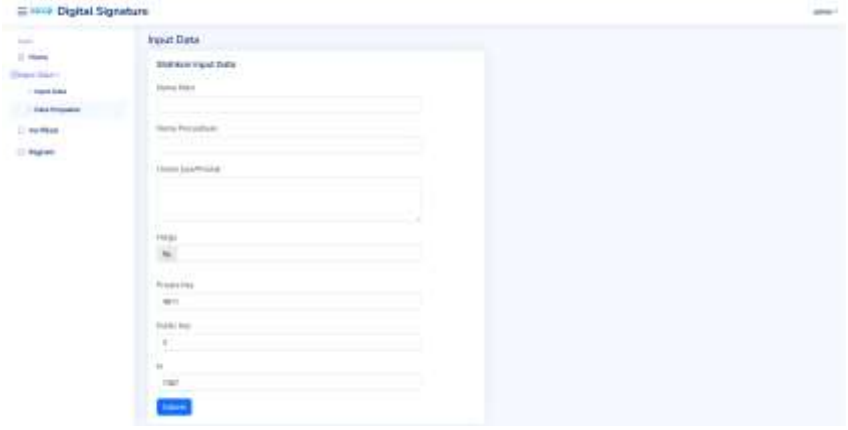

Gambar 1. Halaman Login

2. Halaman *Home*
   Halaman ini merupakan menu utama yang berisi pengenalan terhadap sistem dan juga memiliki area navigasi ke menu-menu yang lainnya.


Gambar 2. Halaman Home

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 25 ; Nomor 1 ; Februari 2026 ; Page 111-118
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

3. Halaman *Input Data*
   Halaman *input data* berfungsi sebagai area dimana *user* bisa menambahkan data penjualan.

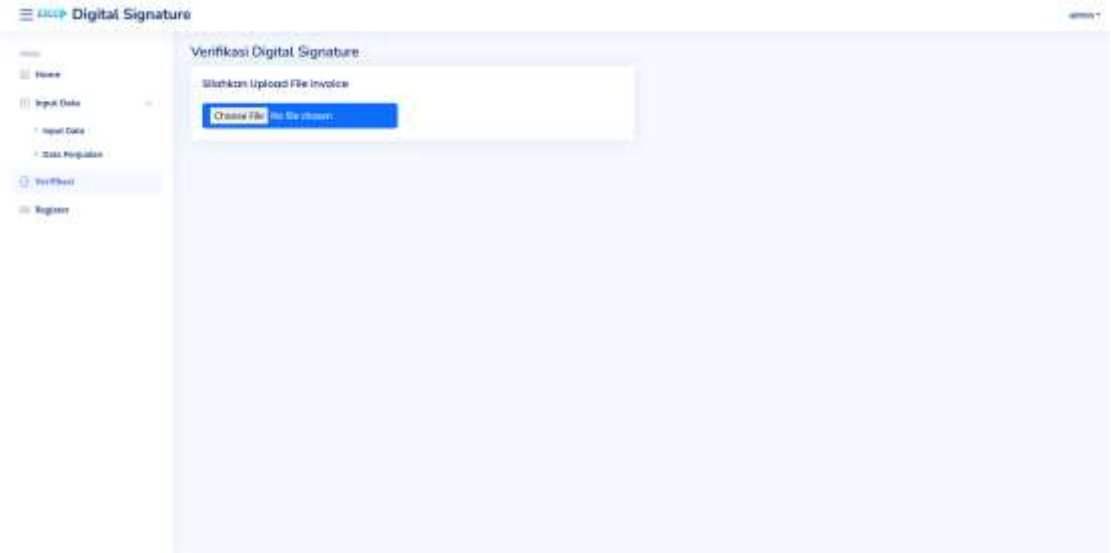



Gambar 3. Halaman Input Data

4. Halaman Data Penjualan
   Halaman data penjualan berfungsi untuk menampillkan seluruh data penjualan yang sudah ditambahakan dan juga untuk mengunduh dan menghapus *data invoice*.


Gambar 4. Halaman Data Penjualan

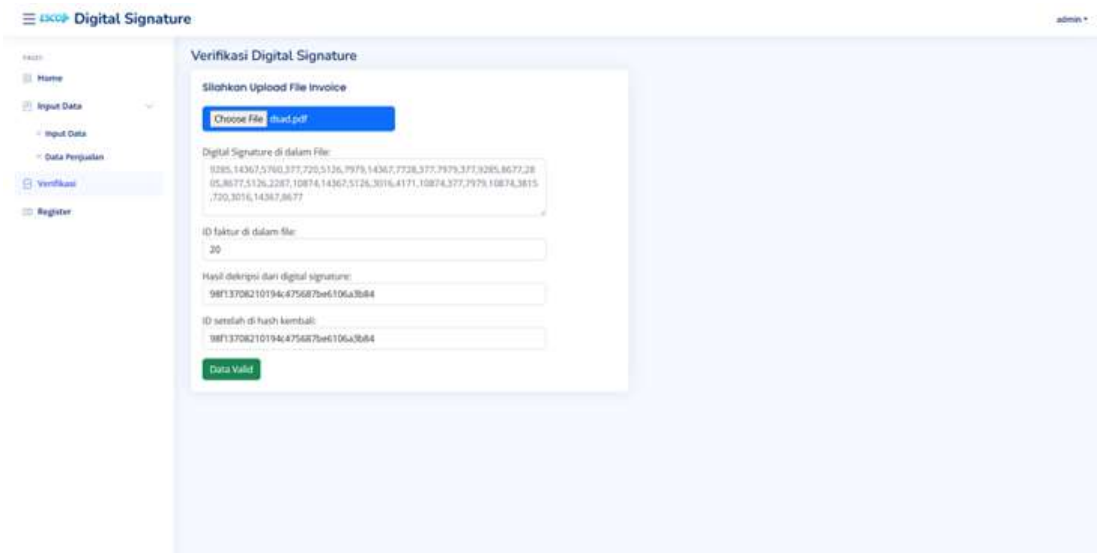
5. Halaman Verifikasi
   Halaman verifikasi berfungsi untuk melakukan proses verifikasi dari *file invoice*.




Gambar 5. Halaman Varifikasi

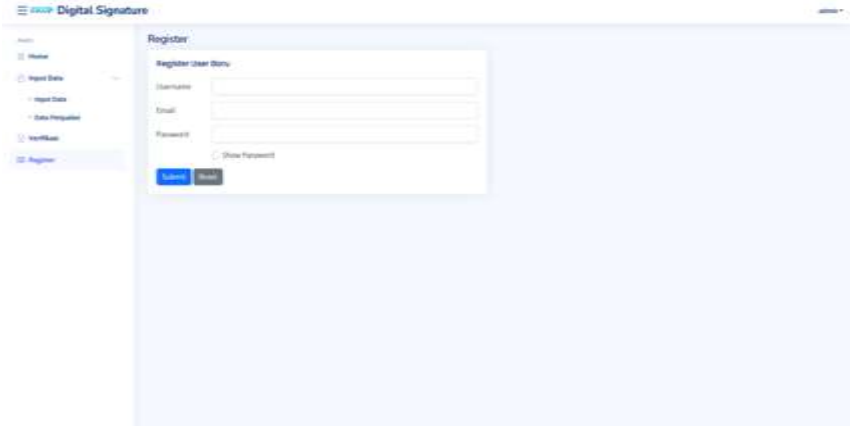
Setelah di verifikasi halaman akan berubah dan akan menampilkan data sebagai berikut:

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 25 ; Nomor 1 ; Februari 2026 ; Page 111-118
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index




Gambar 6. Halaman Verifikasi Setelah File Diunggah

6. Halaman *Register*
   Halaman *register* berfungsi untuk menambahkan *user* baru yang bisa mengakses sistem ini.




Gambar 7. Halaman Register

7. Tampian Faktur Elektronik
   Ketika pengguna mengunduh *file* faktur elekroniknya maka akan mendapatkan *file* sebagai berikut:


Gambar 8. Tampilan Faktur Elektronik

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 25 ; Nomor 1 ; Februari 2026 ; Page 111-118
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

### 3.3 Hasil Pengujian

Hasil pengujian bertujuan untuk mengetahui apakah sistem dapat dijalankan dengan baik dan benar, Berikut tabel 1 adalah hasil dari pengujiannya menggunakan teknik *black box testing*:

Tabel 1. *Black Box Testing*

| No | Nama Pengujian | Test Case | Hasil Pengujian | Keterangan |
|---|---|---|---|---|
| 1. | Form *Login* |  | Sistem akan memproses username dan password, jika sesuai akan muncul halaman home, jika tidak akan muncul "Username/Password Salah" | Valid |
| 2. | Form Tambah Data Penjualan |  | Penambahan data penjualan dengan mengisi form yang ada lau menekan tombol "Simpan", yang dimana data akan tersimpan kedalam data penjualan | Valid |
| 3. | Menu Data Penjualan |  | Sistem menampilkan seluruh data penjualan yang ada, dengan menekan tombol "Download Invoice" akan mengunduh *file invoice* yang sudah memiliki *digital signature* didalamnya. | Valid |

Tabel 1. *Black Box Testing* (Lanjutan)

| No | Nama Pengujian | Test Case | Hasil Pengujian | Keterangan |
|---|---|---|---|---|
| 4. | Menu Verifikasi |  | Mengupload *file invoice* lalu sistem akan melakukan proses validasi dari digital signature yang ada | Valid |
| 5. | Menu *Register* |  | Penabahan user dengan mengisi form yang ada lalu tekan tombol "Submit" dan akan muncul pesan "User Berhasil Ditambahkan" | Valid |

## 4. KESIMPULAN

Berdasarkan hasil analisa penerapan *digital signature* menggunakan algoritma RSA dapat meminimalisir atau bahkan dapat memusnahkan manipulasi dari faktur elektronik di PT. Escoplus Mitra Indonesia oleh orang yang tidak bertanggung jawab yang bisa berdampak negatif pada perusahaan tersebut. Algoritma RSA dapat melakukan proses pembuatan *digital signature* yang berjalan dengan baik. Aplikasi ini dapat digunakan untuk pemberian digital signature pada faktur elektronik dengan berupa file .pdf dan dapat memverifikasi keaslian faktur tersebut.

## UCAPAN TERIMAKASIH

Terima kasih diucapkan kepada Bapak Abdullah Muhazir dan Bapak Egi Affandi atas segala waktu dan ilmunya yang telah memberikan bimbingan selama masa pengerjaan hingga menyelesaikan jurnal ini dan kepada seluruh dosen serta staff pegawai kampus STMIK Triguna Dharma yang telah banyak membantu baik dalam bentuk informasi ataupun dukungan lainnya.

## DAFTAR PUSTAKA

[1] D. Dwiyanti and B. Musri, "Aplikasi E-faktur Dalam Aturan Pemusatan PPN," *Jurnal Pendidikan Akuntansi & Keuangan*, vol. 7, no. 2, pp. 97–110, Jul. 2019, doi: 10.17509/jpak.v7i2.17080.

[2] D. E. Cahyani, "Pengaruh E-Faktur, Penegakan Sanksi Pajak dan Pelayanan Perpajakan terhadap Kepatuhan Pengusaha Kena Pajak dengan Pengetahuan Perpajakan sebagai Variabel Mediasi."

[3] E. V. Waruwu, N. Budi Nugroho, and F. Sonata, "Penerapan Digital Signature Menggunakan Metode RSA Untuk Menvalidasi Keaslian Ijazah SMA Swasta Bina Artha," *Jurnal Cyber Tech*, vol. 1, no. 1, pp. 37–47, 2021.

[4] B. K. Hutasuhut, S. Efendi, and Z. Situmorang, "Digital Signature untuk Menjaga Keaslian Data dengan Algoritma MD5 dan Algoritma RSA," *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan)*, vol. 3, no. 2, pp. 164–169, Mar. 2019, doi: 10.30743/infotekjar.v3i2.1019.

[5] N. Sakti and A. Hidayat, *E-Faktur: Mudah dan Cepat Penggunaan Faktur Pajak secara online*. 2016. Accessed: Apr.16,2023.[Online].Available:https://books.google.com/books?hl=en&lr=&id=geWACwAAQBAJ&oi=fnd&pg=PA27&dq=buku+faktur&ots=Qs8pdxnq1r&sig=5p5Ahku9H1nlcliA6urqkc0mJ4s

[6] N. Zaatsiyah, "IMPLEMENTING DIGITAL SIGNATURE WITH RSA AND MD5 IN SECURING E-INVOICE DOCUMENT," 2021.

[7] R. Siringoringo, "Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File 31 Oleh : Rinmar Siringoringo Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File ARTICLE INFORMATION A B S T R A K," 2020.

[8] M. Taufiqurrahman *et al.*, "Perancangan Sistem Tanda Tangan Digital (Digital Signature)," 2020.

[9] W. Krisna, H. J. Muhammad, and D. Puspitaningrum, "Penggunaan Digital Signature Untuk Absensi Pada Universitas Muhammadiyah Purworejo," *Jurnal Sistem Cerdas*, vol. 5, no. 1, pp. 36–45, May 2022, doi: 10.37396/JSC.V5I1.188.

[10] H. Kumar, D. Sarma, B. Bhuyan, and S. Borah, "Lecture Notes in Networks and Systems 99," 2018. [Online]. Available: http://www.springer.com/series/15179

[11] A. Mohammed Ali and A. Kadhim Farhan, "A novel improvement with an effective expansion to enhance the MD5 hash function for verification of a secure E-Document," *IEEE Access*, vol. 8, pp. 80290–80304, 2020, doi: 10.1109/ACCESS.2020.2989050.

[12] J. Jamaludin and R. Romindo, *Kriptografi: Teknik Hybrid Cryptosystem Menggunakan Kombinasi Vigenere CipherdanRSA*.2020.Accessed:Apr.16,2023.[Online].Available:https://books.google.com/books?hl=en&lr=&id=z3ELEAAAQBAJ&oi=fnd&pg=PA41&dq=buku+kriptografi+rsa&ots=fmR3UKGS9n&sig=QUmoJtdD8TK1zAq4-jnDu0f0Xw4

[13] V. Dwi, P. Anggraini, K. Ibnutama, and Z. Panjaitan, "Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer) Implementasi Algoritma AES Pada Qr-Code Untuk Validasi Keaslian Surat Kontrak Kerja Di Pt. Citra Alfa Sasmita," vol. 24, pp. 252–261, 2025,[Online].Available: https://ojs.trigunadharma.ac.id/index.php/jis/index

[14] M. F. Rafli, Z. Panjaitan, and W. Riansah, "Aplikasi Keamanan Sistem Pengiriman Tagihan Pembayaran Online (Invoice) Berbasis Website dengan algoritma RSA-CRT," J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer), vol. 23, no. 1, p. 138, 2024, doi: 10.53513/jis.v23i1.9604.

[15] N. Arwa, A. Aminudin, and S. Arifianto, "Implementasi Tanda Tangan Digital menggunakan ECDSA (Studi Kasus: Jurnal Tipe File pdf)," J. Repos., vol. 3, no. 3, pp. 321–330, 2021, doi: 10.22219/repositor.v2i3.1306.

[16] F. Nuraeni, D. Kurniadi, and D. N. Rahayu, "Implementation of Rsa and Aes-128 Super Encryption on Qr-Code Based Digital Signature Schemes for Document Legalization," J. Tek. Inform., vol. 5, no. 3, pp. 675–684, 2024, doi: 10.52436/1.jutif.2024.5.3.1426.

[17] Arif Indra Irawan, Iman Hedi Santoso, Istikmal, and Maya Rahayu, "Implementation of QR Code Attendance Security System Using RSA and Hash Algorithms," J. Nas. Tek. Elektro dan Teknol. Inf., vol. 13, no. 1, pp. 53–59, 2024, doi: 10.22146/jnteti.v13i1.4395.