



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



**APLIKASI WEB UNTUK DIGITAL SIGNATURE
DENGAN PENERAPAN METODE PKCS#12 PADA
ALGORITMA RSA**

SKRIPSI
**POLITEKNIK
NEGERI
JAKARTA**

Ilham Fikri Dwi Asmarayani 1807412001

**PROGRAM STUDI D4 TEKNIK INFORMATIKA
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA**

2022



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



**APLIKASI WEB UNTUK DIGITAL SIGNATURE
DENGAN PENERAPAN METODE PKCS#12 PADA
ALGORITMA RSA**

SKRIPSI

**Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh
Diploma Empat Politeknik**

**Nama: Ilham Fikri Dwi Asmarayani
NIM: 1807412001**

**PROGRAM STUDI D4 TEKNIK INFORMATIKA
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA**

2022



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN BEBAS PLAGIARISM

Saya yang bertanda tangan di bawah ini:

Nama Mahasiswa : Ilham Fikri Dwi Asmarayani
NIM : 1807412001
Jurusan/Program : T. Informatika dan Komputer / TI
Studi :
Judul Skripsi : Aplikasi Web untuk Digital Signature dengan Penerapan Metode PKCS#12 pada Algoritma RSA

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

**POLITEKNIK
NEGERI
JAKARTA**

Jakarta, 18 Mei 2022

Yang Membuat Pernyataan



Ilham Fikri Dwi Asmarayani

NIM. 1807412001

LEMBAR PENGESAHAN

Skrripsi diajukan oleh:

Nama : Ilham Fikri Dwi Asmarayani
NIM : 1807412001
Program Studi : Teknik Informatika
Judul : Aplikasi Web untuk Digital Signature dengan Penerapan Metode PKCS#12 pada Algoritma RSA

Telaah diuji oleh tim penguji dalam Sidang Skripsi pada hari Selasa, Tanggal 9, Bulan Agustus, Tahun 2022 dan dinyatakan LULUS.

Disahkan oleh

Pembimbing I : Euis Oktavianti, S.S.I., M.T.Ia
Penguji I : Mera Kartika Delimayanti, S.Si., M.T., Ph.D.
Penguji II : Iklima Ermis Ismail, S.Kom., M.Kom.
Penguji III : Syamsi Dwi Cahya, S.ST., M.Kom.

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

Mauldy Laya, S. Kom, M. Kom

NIP. 198411292020121002



© Hak Cipta : Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

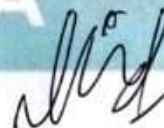
KATA PENGANTAR

Puji dan Syukur penulis panjatkan kehadirat Allah Subhanahu Wa Ta'ala atas selesainya penyusunan Proposal Tugas Akhir ini penulis susun untuk melengkapi salah satu syarat kelulusan Program Studi Teknik Informatika. Dalam penyusunan Proposal ini banyak pihak yang telah memberikan bantuan sehingga bisa terselesaikan. Oleh karena itu penulis ingin mengucapkan terima kasih sebesar-besarnya kepada:

1. Allah SWT yang telah memberikan karunia-Nya berupa kesehatan dan akal sehat kepada penulis sehingga dapat menyelesaikan laporan ini dengan baik.
2. Orang tua dan keluarga penulis yang telah memberikan dukungan secara moral maupun material.
3. Ibu Euis Oktavianti, S.S.I., M.T.I.a selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran dalam mengarahkan penyusunan Proposal Tugas Akhir.

Tiada kata yang pantas penulis ucapkan selain ucapan terima kasih kepada semua pihak yang telah membantu sehingga laporan ini bisa terselesaikan dengan baik. Semoga laporan ini dapat bermanfaat bagi semua pihak.

Depok, 02 Agustus 2022



Ilham Fikri Dwi Asmarayani

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkannya dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





© Hak Cipta milik Politeknik Negeri Jakarta

**SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK
KEPENTINGAN AKADEMIS**

Sebagai civitas akademik Politeknik Negeri Jakarta, saya bertanda tangan di bawah ini:

Nama : Ilham Fikri Dwi Asmarayani
NIM : 1807412001
Jurusan/Program Studi : T. Informatika dan Komputer / TI

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

Aplikasi Web untuk Digital Signature dengan Penerapan Metode PKCS#12 pada Algoritma RSA.

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 18 Mei 2022

Yang Menyatakan




Ilham Fikri Dwi Asmarayani

NIM. 1807412001

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkannya dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

ABSTRAK

Tanda tangan digital adalah bentuk tanda tangan elektronis yang menggunakan metode kriptografi untuk menandai keabsahan suatu dokumen digital. Tanda tangan digital bukan berarti tanda tangan fisik yang di-scan atau digambar di komputer kemudian ditempelkan di dokumen, melainkan perhitungan matematis menggunakan konsep kriptografi kunci publik atas data digital yang ditandatangani. Terdapat dua kegiatan dalam konsep tanda tangan digital: Sign, yaitu kegiatan membubuhkan tanda tangan digital pada dokumen dan Verify, yaitu kegiatan menentukan apakah tanda tangan digital pada dokumen valid. Metode yang digunakan untuk pembuatan aplikasi yaitu menggunakan PKCS#12 karena keamanan dan fleksibilitasnya sesuai untuk penerapan digital signature. Sistem dikembangkan dengan aplikasi web menggunakan Node.JS sebagai dan MongoDB sebagai database.

Kata kunci: *aplikasi web, digital signature, PKCS#12, RSA, sign, verify, algoritma kriptografi.*

POLITEKNIK
NEGERI
JAKARTA



DAFTAR ISI

DAFTAR ISI.....	vii
DAFTAR GAMBAR	xi
DAFTAR TABEL.....	xiv
Bab I.....	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah.....	2
1.3 Batasan Masalah.....	3
1.4 Tujuan dan Manfaat.....	3
1.5 Sistematika Penulisan.....	4
BAB II.....	7
2.1 Algoritma RSA (Rivest Shamir Adleman).....	7
2.2 Sertifikat Digital.....	7
2.3 PKCS#12 (Public Key Cryptography Standards).....	8
2.4 Enkripsi dan Dekripsi.....	9
2.5 Metode Waterfall.....	10
2.5.1 Requirement gathering.....	10
2.5.2 Analysis.....	10
2.5.3 Design	12
2.5.4 Implementasi	14
2.5.5 Integration & Testing	15
2.5.6 Verification.....	15
2.5.7 Operation & Maintenance	15
2.6 Tanda Tangan Digital.....	16

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



© Hak Cipta milik Politeknik Negeri Jakarta

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.7	Perbandingan Penelitian Terdahulu.....	16
BAB III	18
1.1	Rancangan Penelitian	18
3.1.1	Deskripsi Program Aplikasi	18
3.1.2	Analisa Algoritma RSA	18
3.1.3	Analisa PKCS#12.....	22
1.2	Tahapan Penelitian.....	22
1.3	Objek Penelitian.....	23
BAB IV	24
4.1	Analisis Kebutuhan	24
4.2	Perancangan Sistem.....	25
4.2.1	Flowchart Aplikasi	25
4.2.2	Use Case Diagram.....	31
4.2.3	Activity Diagram.....	32
4.2.4	Class Diagram	41
4.3	Implementasi Sistem	43
4.3.1	Tujuan Implementasi Sistem.....	43
4.3.2	Pembahasan Aplikasi	43
4.4	Pengujian.....	73
4.4.1	Deskripsi Pengujian.....	73
4.4.2	Prosedur Pengujian.....	73
4.4.3	Data Hasil Pengujian.....	75
4.4.4	Evaluasi Hasil Pengujian.....	93
BAB V	94
5.1	Kesimpulan	94
5.2	Saran.....	94
DAFTAR PUSTAKA	97



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DATA RIWAYAT HIDUP PENULIS	99
DATA HASIL KUESIONER USER ACCEPTANCE TESTING	100





DAFTAR GAMBAR

Gambar 2.1 Sertifikat Digital.....	8
Gambar 2.2 Enkripsi dan dekripsi.....	9
Gambar 2.2 Waterfall.....	10
Gambar 2.3 QR Code.....	15
Gambar 3.1 Proses signing dan verification.....	21
Gambar 4.1 Flowchart sistem tanda tangan digital.....	26
Gambar 4.2 Flowchart login.....	27
Gambar 4.3 Flowchart registrasi.....	28
Gambar 4.4 Flowchart pembuatan tanda tangan.....	29
Gambar 4.5 Flowchart pembuatan sertifikat digital.....	30
Gambar 4.6 Flowchart otentikasi.....	30
Gambar 4.7 Use Case Diagram.....	31
Gambar 4.8 Activity diagram login.....	32
Gambar 4.9 Activity diagram registrasi.....	33
Gambar 4.10 Activity diagram pembuatan sertifikat digital.....	34
Gambar 4.11 Activity diagram pembuatan tanda tangan.....	35
Gambar 4.12 Activity diagram otentikasi.....	36
Gambar 4.13 Activity diagram download dokumen.....	37
Gambar 4.14 Activity diagram permintaan tanda tangan.....	38
Gambar 4.15 Activity diagram upload dokumen.....	39
Gambar 4.16 Activity diagram upload&sign.....	40
Gambar 4.17 Class Diagram.....	42
Gambar 4.18 Halaman index.....	44
Gambar 4.19 Halaman about.....	44
Gambar 4.20 Halaman login.....	45
Gambar 4.21 <i>Source code</i> login.....	46
Gambar 4.22 Halaman dashboard.....	46
Gambar 4.23 Halaman digital certificate yang masih kosong.....	47
Gambar 4.24 Halaman digital certificate.....	48
Gambar 4.25 Halaman hapus digital certificate.....	48

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.26 <i>Source code</i> hapus digital certificate.....	49
Gambar 4.27 Halaman pembuatan digital certificate.....	49
Gambar 4.28 <i>Source code</i> pembuatan digital certificate.....	50
Gambar 4.29 Halaman signature.....	51
Gambar 4.30 Halaman hapus tanda tangan.....	51
Gambar 4.31 <i>Source code</i> hapus tanda tangan.....	52
Gambar 4.32 Halaman upload tanda tangan.....	52
Gambar 4.33 <i>Source code</i> upload tanda tangan.....	53
Gambar 4.34 Halaman menggambar tanda tangan.....	54
Gambar 4.35 <i>Source code</i> menggambar tanda tangan.....	54
Gambar 4.36 Halaman uploaded dokumen yang masih kosong.....	55
Gambar 4.37 Halaman uploaded dokumen.....	55
Gambar 4.38 <i>Source code</i> download dokumen.....	56
Gambar 4.39 <i>Source code</i> hapus dokumen.....	56
Gambar 4.40 Halaman detail dokumen.....	57
Gambar 4.41 Halaman detail dokumen di menu signer.....	57
Gambar 4.42 Halaman detail dokumen di menu signed by.....	58
Gambar 4.43 Halaman detail dokumen di menu rejected by.....	58
Gambar 4.44 Halaman signature request.....	59
Gambar 4.45 <i>Source code approve</i> dokumen.....	59
Gambar 4.46 <i>Source code</i> tolak dokumen.....	60
Gambar 4.47 Halaman detail dokumen.....	60
Gambar 4.48 <i>Source code</i> dokumen lihat dokumen.....	61
Gambar 4.49 Halaman signature request pada saat input password sertifikat digital.....	61
Gambar 4.50 <i>Source code</i> input password sertifikat digital.....	62
Gambar 4.51 Halaman tandatangani dokumen yang masih kosong.....	62
Gambar 4.52 Halaman tandatangani dokumen.....	63
Gambar 4.53 <i>Source code</i> tanda tangani dokumen.....	64
Gambar 4.54 Halaman upload dokumen yang masih kosong.....	65
Gambar 4.55 Halaman upload dokumen.....	65
Gambar 4.56 <i>Source code</i> upload dokumen.....	66
Gambar 4.57 Halaman upload&sign.....	67
Gambar 4.58 <i>Source code</i> upload dokumen.....	67
Gambar 4.59 Halaman tandatangani dokumen yang masih kosong.....	68



© Hak Cipta Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.60 Halaman tandatangani dokumen	68
Gambar 4.61 <i>Source code</i> tandatangani dokumen	69
Gambar 4.62 Halaman otentikasi dokumen	70
Gambar 4.63 Halaman otentikasi setelah di upload	70
Gambar 4.64 <i>Source code</i> otentikasi dokumen	71
Gambar 4.65 Halaman hasil otentikasi	72
Gambar 4.66 Halaman hasil otentikasi dari qrcode	72





DAFTAR TABEL

Tabel 2.1	Simbol Use Case Diagram	13
Tabel 2.2	Perbandingan penelitian terdahulu	16
Tabel 4.1	Rencana Pengujian	73
Tabel 4.2	Hasil Pengujian Autentikasi	75
Tabel 4.3	Hasil Pengujian Registrasi	76
Tabel 4.4	Hasil Pengujian Sertifikat Digital	78
Tabel 4.5	Hasil Pengujian Tanda Tangan	80
Tabel 4.6	Hasil Pengujian Dokumen yang telah di Upload	82
Tabel 4.7	Hasil Pengujian Permintaan Tanda Tangan pada Dokumen	83
Tabel 4.8	Hasil Pengujian Upload Dokumen	85
Tabel 4.9	Hasil Pengujian Upload dan Tanda Tangan Sendiri	87
Tabel 4.10	Hasil Pengujian Detail Dokumen	89
Tabel 4.11	Hasil Pengujian Tanda Tangan & QR Code pada Dokumen	90
Tabel 4.12	Hasil Pengujian Otentikasi pada Dokumen	91
Tabel 4.13	Hasil Pengujian UAT	92

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB V PENUTUP

5. Kesimpulan

Aplikasi Web untuk Digital Signature telah berhasil mengimplementasikan Metode PKCS#12 pada Algoritma RSA, karena sebagai berikut:

1. Aplikasi Web untuk Digital Signature dengan Penerapan Metode PKCS#12 pada Algoritma RSA berhasil memberikan fasilitas kepada SMAN 90 Jakarta dalam membantu proses tanda tangan pada dokumen.
2. Fitur sign dan otentikasi dapat dilakukan oleh semua user.
3. Hasil otentikasi dapat memastikan bahwa dokumen memang ditandatangani oleh penanda tangan yang sah dan dapat memastikan bahwa dokumen tidak diubah setelah ditandatangani.
4. Pengujian alpha testing dengan 52 skenario dan 52 pengujian berhasil sehingga didapat persentase pengujian sebesar 100%.

5.2 Saran

Dalam proses pembuatan aplikasi Digital Signature ini, penyusun masih banyak memiliki kekurangan dan jauh dari kata sempurna. Sehingga penyusun berharap untuk peneliti selanjutnya dapat mengembangkan lagi aplikasi ini, diantaranya:

1. Dapat menerapkan algoritma pembangkit bilangan selain PKCS#12 pada RSA.
2. Pembuatan aplikasi digital signature data diharapkan dapat dibuat berbasis mobile.



DAFTAR PUSTAKA

- Arifa Amanda (2018) *PERANCANGAN SISTEM APLIKASI PEMBELAJARAN UNTUK ANAK USIA DINI BERBASIS ANDROID*.
- Arifa, K., Susanto, E.R. and Wahyudi, A.D. (2020) *APLIKASI LOWONGAN PEKERJAAN BERBASIS WEB PADA SMK CAHAYA KARTIKA*, *Jurnal Teknologi dan Sistem Informasi (JTSI)*. Available at: <http://jim.teknokrat.ac.id/index.php/sisteminformasi>.
- Aspri, F. (2017) *PERENCANAAN IMPLEMENTASI SERTIFIKAT ELEKTRONIK PADA LABORATORIUM PENGUJIAN DAN KALIBRASI ALAT KESEHATAN*.
- Ba'ri, N. (2016) "Fakultas Sains Dan Teknologi Universitas Islam Negeri (Uin) Alauddin," *Biologi*, 2(112), pp. 2–4.
- Cahyo Prabowo, E. and Afrianto, I. (2017) "Ilmiah Komputer dan PENERAPAN DIGITAL SIGNATURE DAN KRIPTOGRAFI PADA Teknik Informatika – Universitas Komputer Indonesia Ilmiah Komputer dan," *Jurnal Ilmiah Komputer dan Informatika (KOMPUTA)*, 6(2), pp. 83–90.
- Cobb, M. (no date) *RSA algorithm (Rivest-Shamir-Adleman)*. Available at: <https://www.techtarget.com/searchsecurity/definition/RSA> (Accessed: February 17, 2022).
- Dirjen, S.K. *et al.* (2017) "Terakreditasi SINTA Peringkat 2 Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital sebagai Alternatif Pengesahan Dokumen di Masa Pandemi," *Masa Berlaku Mulai*, 1(3), pp. 1058–1069.
- Himawan, C. *et al.* (2016) "Studi Perbandingan Algoritma RSA dan Algoritma El-Gamal," *Seminar Nasional APTIKOM (SEMNASTIKOM)*, 6(1), pp. 28–29.
- Ilham Akhsanu Ridlo (2017) *PEMBUATAN FLOWCHART*.
- James A, O, B. and George M. Marakas (2017) *MANAGEMENT INFORMATIN SYSTEMS*. Makassar.
- Jati, A.B. *et al.* (2021) *Pembangunan Sistem Tanda Tangan Digital pada Sistem Informasi Universitas Atma Jaya Yogyakarta* 133.
- Jennings, C.P. *et al.* (2015) "Pengertian Script Library," 3(7), pp. 59–78.
- Kamsyakawuni, A., Fanani, A.H. and Riski, A. (2018) "Pengamanan Citra Dengan Algoritma Diffie-Hellman Dan Algoritma Simplified Data Encryption Standard (S-Des)," *Jurnal Ilmiah Matematika dan Pendidikan Matematika*, 10(2), p. 63. Available at: <https://doi.org/10.20884/1.jmp.2018.10.2.2846>.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Nur El Deen M. Khalifa and Hesham N. Elmahdy (2019) *The impact of frame rate on securing real time transmission of video over IP Networks.*

Pratiwi (2018) "Big Data Analytics with R and Hadoop."

Radarjo and Budi (2018) "Keamanan Sistem Informasi Berbasis Internet."

Saputra, A. and Negara, T.P. (2021) "Implementasi Algoritma Tanda Tangan Digital Berbasis Kriptografi Kurva Eliptik Diffie-Hellman," *Jurnal Ilmiah Ilmu Komputer dan Matematika*, 18(1), pp. 22–28.

Sugary, Y. and Widia, H. (2020) "Implementasi Digital Signature Menggunakan Algoritma Kriptografi RSA Untuk Pengamanan Data Di Smk Wirakarya 1 Ciparay," *Jurnal Informatika (Computing)*, 07(01), pp. 20–29.

Suho, M. and Kurniati, R. (2018) *RANCANG BANGUN WEBSITE TOKO ONLINE MENGGUNAKAN METODE WATERFALL.*

Umar, A. (2018) "Bab iii perancangan alat 3.1.," pp. 22–43.

Yanti, S.N. and Rihyanti, E. (2021) "Penerapan Rest API untuk Sistem Informasi Film Secara Daring," *Jurnal Informatika Universitas Pamulang*, 6(1), p. 195. Available at: <https://doi.org/10.32493/informatika.v6i1.10033>.



POLITEKNIK
NEGERI
JAKARTA



DAFTAR RIWAYAT HIDUP PENULIS



Iham Fikri Dwi Asmarayani

Lahir di Jakarta, 31 juli 2001. Lulus dari SDN 05 Petukangan Selatan tahun 2012, SMPN 110 Jakarta Selatan tahun 2015, dan SMAN 63 Jakarta Selatan tahun 2018. Kemudian melanjutkan untuk kuliah di CCIT Fakultas Teknik Universitas Indonesia dengan program kerjasama Politeknik Negeri Jakarta untuk program studi Teknik Informatika. Untuk sistem kerjasama, menyelesaikan perkuliahan di CCIT di dua tahun pertama untuk mendapat sertifikasi professional IT dan dilanjutkan dengan menyelesaikan jenjang sarjana di Politeknik Negeri Jakarta sampai saat ini.

POLITEKNIK
NEGERI
JAKARTA

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

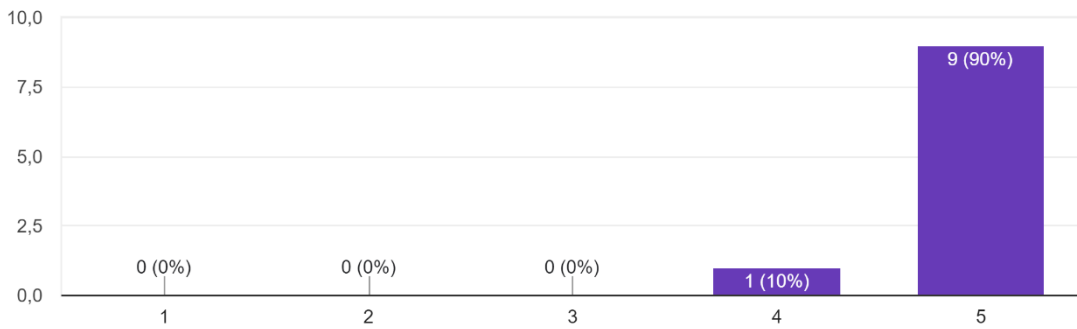


© Hak Cipta milik

DATA HASIL KUESIONER USER ACCEPTANCE TESTING

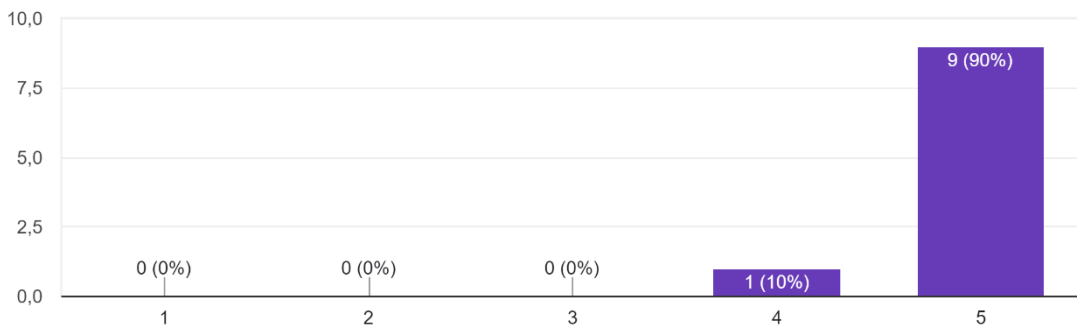
Apakah tampilan pada web ini menarik?

10 jawaban



Apakah Aplikasi digital signature mudah digunakan?

10 jawaban



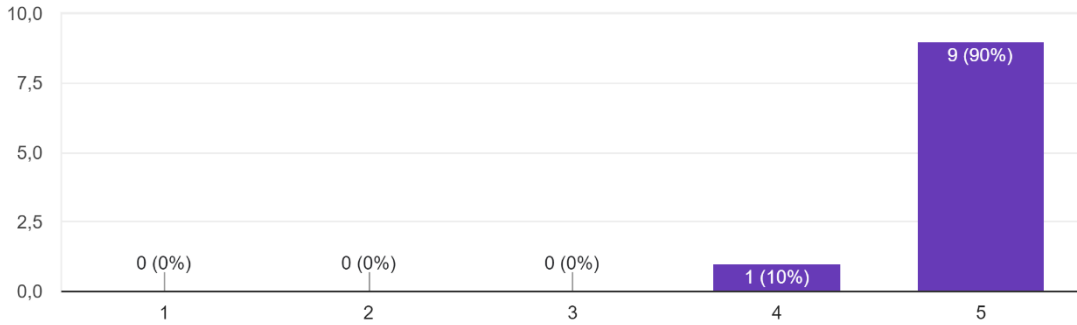
- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritikan atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumumkannya dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

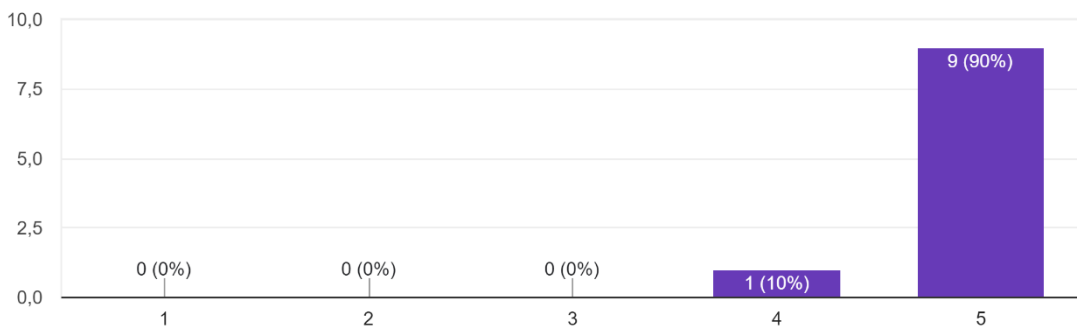
Apakah Penyusunan menu serta isi tiap – tiap menu pada website sudah rapih?

10 jawaban



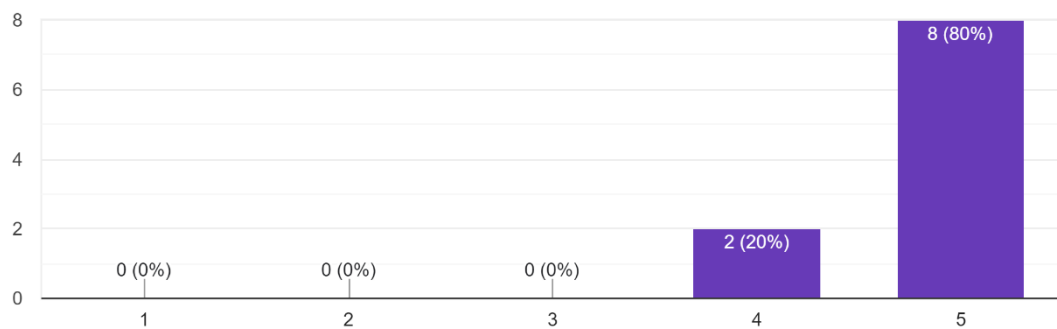
Apakah menu-menu pada Aplikasi digital signature sudah berjalan sebagaimana mestinya?

10 jawaban



Apakah prosedur penggunaan aplikasi sederhana, jelas, dan mudah dimengerti oleh pengguna biasa?

10 jawaban

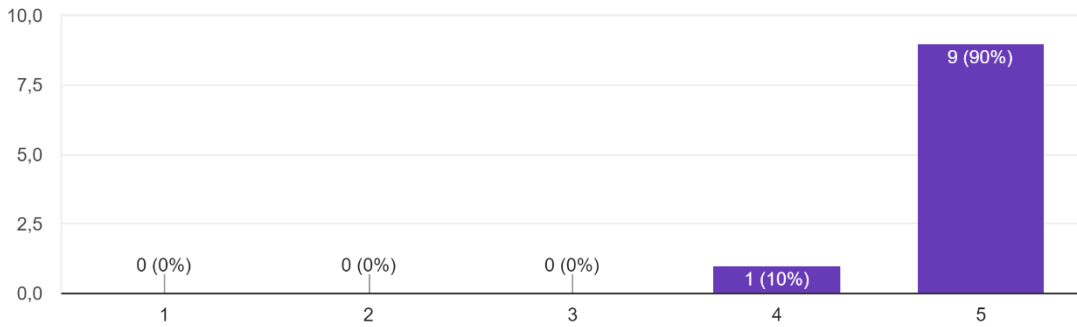




- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

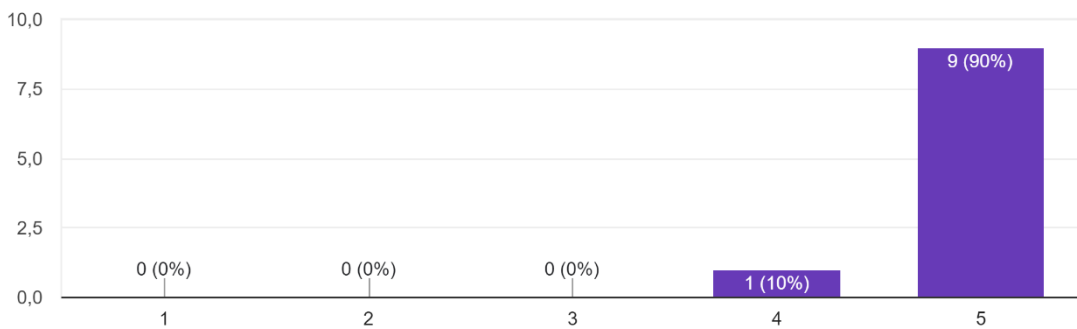
Apakah Pemilihan warna pada website sudah terlihat nyaman oleh pengguna?

10 jawaban



Apakah mudah untuk menggunakan fitur fitur didalam web ini?

10 jawaban



Apakah aplikasi digital signature sudah sesuai dengan yang diharapkan

10 jawaban

