

**IMPLEMENTASI DIGITAL SIGNATURE PADA LAPORAN
TUGAS AKHIR BERBASIS WEB DI JTK POLBAN**

*Web-based Implementation of Digital Signature for Final Project Report at
Computer and Informatics Engineering Department of POLBAN*

TUGAS AKHIR

Laporan ini disusun untuk memenuhi salah satu syarat menyelesaikan pendidikan
Diploma Tiga Program Studi Teknik Informatika di
Jurusan Teknik Komputer dan Informatika

Oleh :

KoTA 108

HILMY OKTOHARITSA	NIM: 181511015
ATHIYYA RAHMAWATI	NIM: 191511006
NANDHIFA AZZAHRA	NIM: 191511025



**JURUSAN TEKNIK KOMPUTER DAN INFORMATIKA
POLITEKNIK NEGERI BANDUNG**

2022

**PENGEMBANGAN SISTEM *MULTI-USER DIGITAL
SIGNATURE UNTUK LAPORAN TUGAS AKHIR
DENGAN METODE SECRET
SHARING SCHEME***

Oleh:

Andika Yudha Riyanto

NIM 191524034

Nabil Putra Hadiyani

NIM 191524052

Menyetujui

Bandung 18 Mei 2023

Pembimbing 1,



Aprianti Nanda Sari, S.T., M.Kom.

NIP 199304262019032028

Pembimbing 2,



Ghifari Munawar, S.Kom., M.T.

NIP 198604122014041001

Ketua Jurusan Teknik Komputer dan
Infomatika,

Ketua Program Studi D4 Teknik
Informatika,



POLBAN

Yadhi Aditya P., S.T., M.Kom

NIP 197912242008121001

Santi Sundari, S.Si., M.T.

NIP 197109031999032001

**PENGEMBANGAN SISTEM *MULTI-USER DIGITAL
SIGNATURE UNTUK LAPORAN TUGAS AKHIR
DENGAN METODE SECRET
SHARING SCHEME***

Oleh:

Andika Yudha Riyanto

NIM 191524034

Nabil Putra Hadiyani

NIM 191524052

Tugas Akhir ini telah disidangkan pada tanggal 25 Mei 2023
sesuai dengan ketentuan.

Tim Pengaji:

Pengaji 1: : Transmissia Semiawan, BSCS., MIT.,
Ph.D
NIP. 196111091993032001



Pengaji 1: : Transmissia Semiawan, BSCS., MIT.,
Ph.D
NIP. 196111091993032001



Pengaji 1: : Transmissia Semiawan, BSCS., MIT.,
Ph.D
NIP. 196111091993032001



PERNYATAAN PENULIS

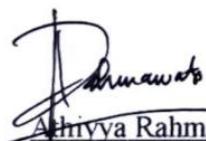
Dengan ini menyatakan bahwa laporan Tugas Akhir dengan judul Implementasi *Digital Signature* Pada Laporan Tugas Akhir Berbasis Web di JTK POLBAN adalah karya ilmiah yang bebas dari unsur komputer plagiarisme, dan sesuai dengan ketentuan tata tulis yang berlaku.

Apabila di kemudian hari ditemukan adanya unsur plagiarisme, maka hasil penilaian dari Tugas Akhir ini dicabut dan bersedia menerima sanksi sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini dibuat dengan sesungguhnya dalam keadaan sadar sepenuhnya.

Bandung, Oktober 2022

Ketua Kelompok Tugas Akhir 108



Achiyya Rahmawati

NIM. 191511006



Nandhifa Azzahra

NIM. 191511025



Hilmy Oktoharitsa

NIM. 181511015

KoTA 108

ORIGINALITY REPORT

19%	18%	4%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.scribd.com	1%
2	www.coursehero.com	1%
3	docplayer.info	1%
4	repository.unissula.ac.id	1%
5	pdfcoffee.com	1%
6	prpm.trigunadharma.ac.id	1%
7	jurnal.uisu.ac.id	1%
8	123dok.com	1%
9	repository.its.ac.id	1%

	<p>Nama : Athiyya Rahmawati NIM : 191511006</p>
<p>Tempat, Tanggal Lahir SD dan Tahun Lulus SMP dan Tahun Lulus SMA dan Tahun Lulus Prestasi yang pernah dicapai</p>	<p>: Bandung, 10 Juni 2001 : SDN 2 Kuningan, 2013 : SMPN 2 Kuningan, 2016 : SMAN 2 Kuningan, 2019 : -</p>



Nama : Hilmy Oktoharitsa

NIM : 181511015

Tempat, Tanggal Lahir	: Tangerang, 19 Oktober 2000
SD dan Tahun Lulus	: SDIT Nur Fatahillah Banten, 2012
SMP dan Tahun Lulus	: SMP Nurul Fikri Boarding School Serang, 2015
SMA dan Tahun Lulus	: SMA Al Adzkar Pamulang, 2018
Prestasi yang pernah dicapai	: Rekor Muri komputer tim HIMAKOM

	<p>Nama : Nandhifa Azzahra NIM : 191511025</p>
<p>Tempat, Tanggal Lahir SD dan Tahun Lulus SMP dan Tahun Lulus SMA dan Tahun Lulus Prestasi yang pernah dicapai</p>	<p>: Kuningan, 2 Juni 2001 : SDN 4 Kuningan, 2013 : SMPN 1 Kuningan, 2016 : SMAN 2 Kuningan, 2019 : -</p>

ABSTRAK

Salah satu aplikasi algoritma kriptografi nirsimetri yang sering digunakan adalah *digital signature*. Tujuan dari skema *digital signature* adalah untuk menggantikan tanda tangan tulisan tangan dengan mengenkripsi *message digest* dari dokumen yang ditandatangani menggunakan kunci privat pengirim. Akibatnya, integritas dari dokumen yang ditandatangani juga terjamin karena perubahan satu bit saja oleh pihak yang tidak berwenang dapat dideteksi. Untuk memastikan integritas tersebut, dokumen dapat diverifikasi menggunakan kunci publik. Tugas akhir ini berfokus pada implementasi skema *digital signature* dengan menggunakan algoritma RSA untuk laporan Tugas Akhir di JTK POLBAN. Sistem yang dibangun terdiri dari dua fitur utama yaitu penandatanganan dokumen dan verifikasi dokumen. Pada proses penandatanganan dokumen, mahasiswa mengirim dokumen laporan TA untuk diambil nilai hashnya dengan menggunakan algoritma MD5. Nilai hash tersebut kemudian diekripsi menggunakan kunci privat dari dosen pembimbing dan penguji untuk menghasilkan *digital signature*. Setelah itu, dokumen beserta *digital signature*-nya dikirim ke penerima. Untuk membuktikan integritas dokumen TA, proses verifikasi dilakukan. Pertama-tama dokumen TA yang diterima dipisahkan dengan *digital signature*-nya. Dokumen TA kemudian diambil nilai hashnya dengan algoritma yang sama seperti pada proses penandatanganan. Sementara itu, *digital signature* didekripsi menggunakan kunci publik. Jika *digital signature* yang telah terdekripsi sama dengan nilai hash dari dokumen TA, maka dapat dipastikan tidak ada modifikasi pada dokumen tersebut.

Kata kunci: Tugas Akhir, *digital signature*, Algoritma RSA, Hash.

ABSTRACT

One of the most widely used applications of asymmetric cryptography algorithms is digital signatures. The purpose of digital signature schemes is to replace the handwritten signature by encrypting the message digest with the private key of the signer. Consequently, the integrity of a signed document also provided by this scheme since a bit alteration of document by unauthorized parties are detectable. A signed document must be verifiable by using a public key. This research focused on the implementation of a digital signature scheme by using the RSA algorithm for Final Project Report documents at the Computer and Informatics Engineering Department of POLBAN. The scheme has two main features, i.e., document signing and document verification. In the document signing process, the Final Project Report document is submitted by students, and message digest extraction is done by using the MD5 hash algorithm. Then, the hash value of the document is encrypted by the private key of the signer, which consists of the supervisors and the examining committee members, to yield a digital signature. Then, this digital signature is sent along with the document to the receiver. To provide data integration, the document verification process is conducted. First, the document was separated by its digital signature. Then the message digest of the document was extracted by the same algorithm in the signing process. Meanwhile, the received digital signature was decrypted by using the public key of the signer. Finally, if the decrypted digital signature and the hash value are alike, then it can be sure that there is no modification in the documents.

Keywords: *Final project, digital signature, RSA Algorithm, Hash*

KATA PENGANTAR

Puji dan syukur atas kehadirat kepada Tuhan Yang Maha Esa yang telah menurunkan rahmat, berkah, dan ridhonya, yang telah memberikan banyak kesempatan, sehingga penulis dapat menyelesaikan penggerjaan Tugas Akhir yang berjudul “Implementasi *Digital Signature* pada Laporan Tugas Akhir Berbasis Web di JTK Polban”. Laporan Tugas Akhir ini disusun sebagai salah satu syarat untuk menyelesaikan Pendidikan Diploma Tiga Program Studi Teknik Informatika di Jurusan Teknik Komputer dan Informatika. Dalam kata pengantar ini penulis mengucapkan terima kasih kepada:

1. Tuhan Yang Maha Esa yang selalu memberikan kelancaran pada penggerjaan Tugas Akhir ini.
2. Orang tua dan keluarga dari tim penulis yang telah banyak memberikan dukungan, doa, dan motivasi.
3. Bapak Bambang Wisnuadhi, S.Si., M.T., Selaku Ketua Jurusan Teknik Komputer dan Informatika Politeknik Negeri Bandung
4. Bapak Ghifari Munawar, S.Si., M.T., Selaku Ketua Program Studi DIII Teknik Informatika Jurusan Teknik Komputer dan Informatika Politeknik Negeri Bandung.
5. Bapak Didik Suwito Pribadi, BSCS., M.Kom. Selaku dosen pembimbing I yang telah banyak memberikan bimbingan, masukan, arahan, motivasi, dan dukungan kepada penulis.
6. Ibu Aprianti Nanda Sari, S.T., M.Kom. Selaku dosen pembimbing II yang telah banyak memberikan bimbingan, masukan, arahan, motivasi, dan dukungan kepada penulis.
7. Ibu Ade Hodijah, S.T., M.T., Bapak Muhammad Rizqi Sholahuddin, S.Si., M.T., dan Bapak Djoko Cahyo Utomo Lieharyani, S.Kom., M.MT. selaku dosen penguji yang telah bersedia memberikan masukan dan pengetahuan baru kepada penulis terhadap Tugas Akhir yang telah kami kerjakan.
8. Ibu Sri Ratna Wulan selaku dosen wali penulis.

9. Seluruh tim koordinator tugas akhir DIII 2022 yang telah mengkoordinir, memberikan arahan, dan masukan kepada penulis.
10. Seluruh dosen Jurusan Teknik Komputer dan Informatika Politeknik Negeri Bandung yang telah membantu dan memberikan ilmu kepada tim penulis, sehingga tim penulis dapat menyelesaikan laporan Tugas Akhir ini.
11. Seluruh sahabat dan Rekan-rekan di Jurusan Teknik Komputer dan Informatika Politeknik Negeri Bandung khususnya angkatan 2019 yang saling memberikan dukungan dan semangat untuk menyelesaikan Tugas Akhir ini.
12. Pihak-pihak lain yang tidak dapat disebutkan satu persatu atas segala bentuk pengorbanan dan dukungan yang telah diberikan, selama tim penulis mengenyam pendidikan DIII di Politeknik Negeri Bandung ini.

Semoga Allah subhanahu wa ta'ala senantiasa membalsas semua kebaikan yang telah diberikan kepada tim penulis selama ini. Penulis mengharapkan kritik dan saran untuk penyempurnaan laporan ini, serta semoga tugas akhir ini dapat memberikan manfaat bagi semua pihak.

Bandung, Oktober 2022

KoTA 108

DAFTAR ISI

ABSTRAK	viii
ABSTRACT	ix
KATA PENGANTAR.....	x
DAFTAR ISI.....	xii
DAFTAR LAMPIRAN	xvi
DAFTAR GAMBAR.....	xvii
DAFTAR TABEL	xx
DAFTAR ISTILAH	xxii
DAFTAR SINGKATAN DAN LAMBANG	xxiii
BAB I.....	1
I.1 Latar Belakang.....	1
I.2 Rumusan Masalah	2
I.3 Tujuan.....	2
I.4 Ruang Lingkup dan Batasan	3
I.5 Sistematika Penulisan.....	3
BAB II	6
II.1 Karya Ilmiah Sejenis Sebelumnya.....	6
II.2 Dasar Teori	8
II.2.1 Tugas Akhir.....	8
II.2.2 Digital Signature	8
II.2.3 Fungsi Hash.....	8
II.2.4 Algoritma RSA.....	8
II.2.5 Aplikasi WEB	10
II.2.6 Tahapan Enkripsi Dokumen.....	10

II.2.7 Tahapan Validasi Dokumen	11
II.2.8 SDLC - Incremental	12
II.3 Teknologi yang digunakan	15
II.3.1 Bahasa Pemrograman PHP	15
II.3.2 MariaDB	15
II.3.3 Framework Codeigniter 4	15
II.3.4 Bootstrap	16
II.3.5 CSS	16
II.3.6 Library TCPDF	16
II.3.7 Library phpseclib	16
II.3.8 Library FPDI	17
II.3.9 Library PHAR	17
BAB III.....	18
III.1 Alur Pelaksanaan.....	18
BAB IV	23
IV.1 Analisis Sistem Berjalan.....	23
IV.1.1 Prosedur yang Berjalan Saat Ini	23
IV.1.2 Analisis Stakeholder yang Terlibat.....	23
IV.1.3 Analisis Alur Proses Saat Ini	25
IV.2 Analisis Aplikasi Sejenis.....	26
IV.2.1 Adobe Acrobat Reader DC.....	26
IV.2.2 DocuSign	31
IV.3 Analisis Bisnis Proses Aplikasi yang Akan Dibangun	35
IV.3.1 Identifikasi Bisnis Proses.....	35
IV.3.2 Diagram Bisnis Proses yang Diusulkan.....	35
IV.3.3 Alur Proses yang Diusulkan	42
IV.4 Analisis Aktor dan Sistem	43
IV.5 Analisis Kebutuhan Data	44

IV.6 Analisis Perangkat Lunak.....	46
IV.6.1 Arsitektur Aplikasi	46
IV.6.2 Framework.....	47
IV.6.3 Database.....	48
IV.6.4 Library phpseclib	48
IV.6.5 Perbandingan RSA dan DSA.....	48
IV.6.6 Perbandingan RSA dan Diffie-Helman	49
BAB V.....	51
V.1 Perancangan Interaksi Antar Objek	51
V.2 Perancangan Database.....	62
V.3 Perancangan User Interfaces.....	64
BAB VI.....	76
VI.1 Infrastruktur Sistem.....	76
VI.2 Matriks Implementasi	77
VI.3 Penggunaan <i>Library</i>	78
VI.4 Hasil Implementasi	78
VI.4.1 Halaman Login	78
VI.4.2 Halaman Daftar User	79
VI.4.3 Halaman Profil Dosen	80
VI.4.4 Halaman Unduh Dokumen	80
VI.4.5 Halaman Unduh Dokumen	81
VI.4.6 Halaman Verifikasi Dokumen	82
VI.4.7 Halaman Daftar Dokumen.....	83
VI.4.8 Halaman Tanda Tangan Dokumen	84
VI.4.9 Halaman Unggah Dokumen	85
VI.4.10 Halaman Detail Dokumen	86
VI.4.11 Halaman Daftar Dokumen yang Perlu Ditandatangani Oleh Dosen	87
VI.4.12 Halaman Registrasi.....	88

VI.4.13 Halaman Upload Tanda Tangan	89
VI.4.14 Halaman Upload Tanda Tangan (Generate Key)	90
BAB VII	92
VII.1 Lingkup Pengujian	92
VII.2 Rencana Pengujian.....	92
VII.2.1 Tahapan Pengujian	93
VII.2.2 Jenis Pengujian.....	94
VII.3 <i>Requirement</i> yang Telah Diujikan.....	95
BAB VIII.....	96
VIII.1 Kesimpulan.....	96
VIII.2 Saran	96
DAFTAR PUSTAKA	98

DAFTAR LAMPIRAN

DAFTAR GAMBAR

Gambar II. 1 Tahapan enkripsi dokumen.....	11
Gambar II. 2 Tahapan validasi dokumen	12
Gambar II. 3 Tahapan increment	13
Gambar III. 1 Alur pelaksanaan	18
Gambar IV. 1 Alur proses saat ini.....	25
Gambar IV. 2 Form identitas untuk menambahkan Digital ID pada Adobe Acrobat	26
Gambar IV. 3 Halaman pilih lokasi penyimpanan Digital ID dan password Digital ID	27
Gambar IV. 4 Pemilihan area penempatan Digital ID pada Adobe Acrobat	27
Gambar IV. 5 Pemilihan Digital ID yang akan digunakan pada Adobe Acrobat .	28
Gambar IV. 6 Preview bentuk Digital ID yang akan digunakan pada Adobe Acrobat.....	28
Gambar IV. 7 Halaman mengubah tampilan Digital ID pada Adobe Acrobat	29
Gambar IV. 8 Tampilan Digital ID pada file	30
Gambar IV. 9 Tampilan status validasi yang valid	30
Gambar IV. 10 Tampilan status validasi yang tidak valid	31
Gambar IV. 11 Form identitas untuk mendaftar akun di DocuSign	32
Gambar IV. 12 Halaman awal pada DocuSign	33
Gambar IV. 13 Halaman mengubah bentuk signature pada DocuSign	33
Gambar IV. 14 Dropdown fitur lain di DocuSign.....	34
Gambar IV. 15 Bisnis proses digital signature.....	37
Gambar IV. 16 Bisnis proses verifikasi dokumen laporan TA	40
Gambar IV. 17 Bisnis proses autentikasi	42
Gambar IV. 18 Alur proses digital signature	43
Gambar IV. 19 Use case diagram	44
Gambar V. 1 System sequence diagram autentikasi	54
Gambar V. 2 System sequence diagram proses digital signature	56
Gambar V. 3 System sequence diagram unduh dokumen.....	57

Gambar V. 4 System sequence diagram verifikasi dokumen	58
Gambar V. 5 System sequence diagram unggah dokumen.....	59
Gambar V. 6 System sequence diagram membubuhkan tanda tangan	61
Gambar V. 7 System sequence diagram registrasi.....	62
Gambar V. 8 Entity relationship diagram	63
Gambar V. 9 User interface login	65
Gambar V. 10 User interface Halaman dashboard.....	66
Gambar V. 11 User interface form tambah data dosen.....	67
Gambar V. 12 User interface form tambah data mahasiswa.....	68
Gambar V. 13 User interface form unggah dokumen	69
Gambar V. 14 User interface form unggah dokumen	70
Gambar V. 15 User interface verifikasi dokumen	71
Gambar V. 16 User interface hasil verifikasi dokumen (valid)	72
Gambar V. 17 User interface hasil verifikasi dokumen (tidak valid)	72
Gambar V. 18 User interface unduh dokumen (available)	74
Gambar V. 19 User interface unduh dokumen (not available)	74
Gambar V. 20 User interface registrasi.....	75
Gambar VI. 1 Infrastruktur sistem	76
Gambar VI. 2 Halaman implementasi login	79
Gambar VI. 3 Halaman implementasi daftar user.....	79
Gambar VI. 4 Halaman implementasi profil dosen	80
Gambar VI. 5 Halaman implementasi unduh dokumen.....	81
Gambar VI. 6 Halaman implementasi unduh dokumen.....	82
Gambar VI. 7 Halaman implementasi verifikasi dokumen.....	83
Gambar VI. 8 Halaman implementasi daftar dokumen	84
Gambar VI. 9 Halaman implementasi tanda tangan dokumen	85
Gambar VI. 10 Halaman implementasi unggah dokumen	86
Gambar VI. 11 Halaman implementasi detail dokumen.....	87
Gambar VI. 12 Halaman implementasi daftar dokumen	88
Gambar VI. 13 Halaman implementasi registrasi	89
Gambar VI. 14 Halaman implementasi unggah tanda tangan.....	90

Gambar VI. 15 Halaman implementasi unggah tanda tangan (generate key)..... 91

DAFTAR TABEL

Tabel II. 1 Karya ilmiah sebelumnya.....	6
Tabel III. 1 Tahap inkremen.....	20
Tabel IV. 1 Jenis stakeholder	24
Tabel IV. 2 Perbandingan fitur aplikasi	35
Tabel IV. 3 Identifikasi bisnis proses.....	35
Tabel IV. 4 Penjelasan diagram proses pembuatan digital signature.....	38
Tabel IV. 5 Penjelasan diagram proses verifikasi dokumen	41
Tabel IV. 6 Penjelasan diagram proses autentikasi.....	42
Tabel IV. 7 Data dosen.....	45
Tabel IV. 8 Data KoTA.....	45
Tabel IV. 9 Data dokumen laporan TA.....	46
Tabel IV. 10 Data koordinator TA.....	46
Tabel IV. 13 Perbandingan RSA dan Diffie-Helman	49
Tabel V. 1 Use case scenario autentikasi mahasiswa	51
Tabel V. 2 Use case scenario autentikasi dosen.....	52
Tabel V. 3 Use case scenario autentikasi koordinator TA	53
Tabel V. 4 Use case scenario proses digital signature	54
Tabel V. 5 Use case scenario unduh dokumen	56
Tabel V. 6 Use case scenario verifikasi dokumen	57
Tabel V. 7 Use case scenario unggah dokumen.....	59
Tabel V. 8 Use case scenario bubuhkan tanda tangan	60
Tabel V. 9 Use case scenario registrasi.....	61
Tabel V. 10 Penjelasan ERD.....	63
Tabel V. 11 User interface login	64
Tabel V. 12 User interface Halaman dashboard	65
Tabel V. 13 User interface form tambah data dosen.....	66
Tabel V. 14 User interface form tambah data mahasiswa	67
Tabel V. 15 User interface form unggah dokumen	68
Tabel V. 16 User interface form unggah dokumen.....	69

Tabel V. 17 User interface verifikasi dokumen	70
Tabel V. 18 User interface hasil verifikasi dokumen.....	71
Tabel V. 19 User interface unduh dokumen	73
Tabel V. 20 User interface registrasi.....	75
Tabel VI. 1 Matriks implementasi	77
Tabel VI. 2 Penjelasan library.....	78
Tabel VI. 3 Halaman implementasi login	78
Tabel VI. 4 Halaman implementasi daftar user	79
Tabel VI. 5 Halaman implementasi profil dosen	80
Tabel VI. 6 Halaman implementasi unduh dokumen.....	80
Tabel VI. 7 Halaman implementasi unduh dokumen.....	81
Tabel VI. 8 Halaman implementasi verifikasi dokumen	82
Tabel VI. 9 Halaman implementasi daftar dokumen	83
Tabel VI. 10 Halaman implementasi tanda tangan dokumen	84
Tabel VI. 11 Halaman implementasi unggah dokumen.....	85
Tabel VI. 12 Halaman implementasi detail dokumen.....	86
Tabel VI. 13 Halaman implementasi daftar dokumen	87
Tabel VI. 14 Halaman implementasi registrasi.....	88
Tabel VI. 15 Halaman implementasi unggah tanda tangan	89
Tabel VI. 16 Halaman implementasi unggah tanda tangan (generate key)	90
Tabel VII. 1 Profil tester aplikasi.....	92
Tabel VII. 2 Tahap testing aplikasi	95

DAFTAR ISTILAH

- Backend* : Bagian belakang komputer dari sebuah *website*. Bahasa pemrograman untuk *backend* diantaranya PHP, ruby, python dll.
- Bisnis Proses* : Aktivitas yang saling berkaitan di seluruh organisasi untuk mencapai pemenuhan kebutuhan pelanggan
- Database* : Suatu pengorganisasian data yang saling terhubung yang dapat memudahkan aktivitas untuk memperoleh informasi
- Framework* : Sebuah kerangka kerja yang digunakan untuk mempermudah para *developer software* dalam pembuatan aplikasi.
- Frontend* : Bagian langsung yang dilihat oleh pengguna, dan juga dapat berinteraksi langsung. Bagian komputer dibangun menggunakan HTML, CSS, dan *JavaScript*.
- Incremental* : Metode pengembangan perangkat lunak yang menggabungkan elemen proses linier dan paralel, dan menerapkan *sequences linier* secara bertahap
- Role* : Peran atau hak akses pengguna
- Server* : Sistem perangkat komputer
- Software* : Kumpulan data komputer yang disimpan dan diatur oleh komputer. Termasuk program komputer, dokumentasinya dan informasi yang dapat dibaca dan ditulis oleh komputer.
- Stakeholder* : Pemangku kepentingan yang memiliki hubungan dengan suatu aktivitas.
- Website* : Situs web (dalam Bahasa Indonesia).
Satu set halaman informasi di internet tentang subjek tertentu, diterbitkan oleh satu orang atau organisasi.

DAFTAR SINGKATAN DAN LAMBANG

Singkatan	Nama	Pemakaian pertama kali pada halaman
BPMN	<i>Business Process Model Notation</i>	25
MVC	<i>Model, View, Controller</i>	15
Polban	<i>Politeknik Negeri Bandung</i>	1
PHP	<i>Hypertext Preprocessor</i>	7
SDLC	<i>Software Development Life Cycle</i>	13
SRS	<i>Software Requirement Specification</i>	20
CSS	<i>Cascading Style Sheets</i>	16

BAB I

PENDAHULUAN

Bab ini menjelaskan terkait latar belakang, rumusan masalah, ruang lingkup, dan tujuan yang dihasilkan dari pengembangan aplikasi yang dilakukan.

I.1 Latar Belakang

Tugas Akhir merupakan suatu karya ilmiah berdasarkan kegiatan mandiri mahasiswa yang membahas suatu masalah yang sesuai dengan bidang ilmu pada program studi yang ditempuh oleh mahasiswa tersebut. Tugas Akhir merupakan salah satu syarat kelulusan di setiap perguruan tinggi termasuk di Jurusan Teknik Komputer dan Informatika Politeknik Negeri Bandung. Pada jenjang diploma tiga, Proses pelaksanaan Tugas Akhir dilakukan selama satu semester yaitu pada semester akhir.

Dalam proses pelaksanaan Tugas Akhir di Jurusan Teknik Komputer dan Informatika Polban terdapat 2-3 orang dosen pembimbing dan 2-4 orang dosen penguji. Mahasiswa akan melakukan bimbingan dengan dosen pembimbing tugas akhir selama proses pengerjaan tugas akhir. Dosen pembimbing tugas akhir memiliki peran penting karena memiliki tanggung jawab untuk memastikan bahwa mahasiswa mampu menyusun tugas akhir dengan baik sehingga tugas akhir tersebut siap diujikan dan menghasilkan karya tulis yang berkualitas.

Pada laporan Tugas Akhir tentunya terdapat lembar pengesahan yang perlu ditandatangani oleh berbagai pihak seperti pembimbing, penguji, mahasiswa dan ketua jurusan. Sejak pandemik berlangsung, berbagai proses pengesahan dokumen yang awalnya dilakukan secara manual berubah menjadi membubuhkan citra tanda tangan pada dokumen. Oleh karena itu, banyak beberapa penyesuaian yang perlu dilakukan oleh pihak-pihak terkait.

Untuk saat ini, proses tanda tangan pada lembar pengesahan laporan tugas akhir di Jurusan Teknik Komputer dan Informatika masih memakai tanda tangan yang ditempel di *pdf* tanpa ada enkripsi dan dekripsi dalam dokumen. Tentunya, teknik ini tidak aman dan rawan disalahgunakan oleh pihak yang tidak bertanggung jawab. Selain itu, saat proses pengiriman dokumen digital melalui internet sangat rentan terhadap kemungkinan modifikasi sehingga sulit membuktikan keaslian dokumen tersebut. Modifikasi tersebut diantaranya adalah mengubah isi dokumen atau mengubah tanda tangan. Oleh karena itu, dibutuhkan sebuah sistem untuk membuktikan keaslian identitas pengirim dan isi dokumen digital atau pesan yang dikirim.

Berdasarkan uraian permasalahan diatas, Jurusan Teknik Komputer dan Informatika Polban membutuhkan sistem tanda tangan digital (*digital signature*) pada lembar pengesahan laporan Tugas Akhir yang dapat menjaga keamanan tanda tangan dan mampu menjaga keaslian dokumen. Aplikasi yang dibangun memiliki fitur utama dapat mengenkripsi laporan Tugas Akhir dan memvalidasi laporan

I.2 Rumusan Masalah

Berlandaskan latar belakang diatas, dapat didefinisikan permasalahan :

1. Rentan terjadinya penyalahgunaan tanda tangan ketika teknik pengesahan dokumennya dengan menempelkan citra tanda tangan ke bagian yang harus ditandatangi tanpa ada enkripsi dan dekripsi didalamnya.
2. Saat proses pengiriman dokumen digital melalui internet sangat rentan terhadap kemungkinan modifikasi sehingga sulit membuktikan keaslian dokumen tersebut.

I.3 Tujuan

Berdasarkan rumusan masalah yang telah dirumuskan maka tujuan dibuatnya aplikasi ini yaitu:

1. Menyediakan fitur untuk proses pembubuhan tanda tangan pada lembar pengesahan Laporan TA.

2. Mengaplikasikan kriptografi *digital signature* pada laporan Tugas Akhir di JTK Polban.

I.4 Ruang Lingkup dan Batasan

Berikut ini merupakan ruang lingkup dari aplikasi yang dibuat :

1. Mengkaji pengelolaan dokumen Tugas Akhir di JTK Polban. Aplikasi ini hanya menangani dokumen laporan Tugas Akhir pada program studi D3 Teknik Informatika dan D4 Teknik Informatika.
2. Membuat aplikasi *Digital Signature* untuk mahasiswa tingkat akhir program studi D3 Teknik Informatika dan D4 Teknik Informatika JTK Polban. Aplikasi ini memiliki fitur utama menyisipkan tanda tangan digital (*digital signature*) dan verifikasi terhadap tanda tangan digital. Dokumen yang diperuntukkan hanya dokumen dengan ekstensi *.pdf.
3. Algoritma *digital signature* yang digunakan adalah RSA (*Rivest-Shamir-Adleman*).
4. Pembubuhan citra tanda tangan dilakukan pada lembar pengesahan laporan Tugas Akhir.

Terdapat juga batasan pada sistem yaitu sebagai berikut:

1. Aplikasi ini hanya tersedia dalam platform website.
2. Satu akun diperuntukkan untuk satu Kelompok TA dan Mahasiswa yang dimaksud ialah ketua kelompok TA.
3. Aplikasi ini hanya menangani digital signature oleh pembimbing dan penguji.
4. Tidak ada urutan penandatanganan dalam alur menandatangani dokumen Laporan Tugas Akhir.
5. Key pada tanda tangan dosen bersifat statis.

I.5 Sistematika Penulisan

Sistematika laporan tugas akhir ini terdiri dari beberapa bab dan sub bab yang tersusun sebagai berikut berikut:

BAB 1 PENDAHULUAN

Pada bab ini berisi tentang gambaran umum dari Tugas Akhir yang akan dikerjakan. Terdiri beberapa sub bab diantaranya, latar belakang, rumusan masalah, tujuan, ruang lingkup dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi karya ilmiah sejenis yang sudah ada dan dasar-dasar teori yang akan digunakan untuk penunjang dalam membangun Aplikasi Tanda Tangan Digital.

BAB III METODOLOGI PENYELESAIAN

Pada bab ini berisi tahapan-tahapan yang digunakan dalam menyelesaikan Tugas Akhir ini.

BAB IV ANALISIS

Pada bab ini berisi hasil analisis yang telah dilakukan untuk mengetahui kebutuhan aplikasi web yang akan dikembangkan pada Tugas Akhir ini. Terdiri dari beberapa sub bab, diantaranya analisis *stakeholder*, analisis *business process*, analisis kebutuhan data, analisis kebutuhan, analisis aplikasi sejenis, analisis teknologi, dan evaluasi analisis aplikasi sejenis.

BAB V PERANCANGAN

Pada bab ini berisi perancangan dalam mengembangkan aplikasi berdasarkan dari hasil analisis. Terdiri dari beberapa sub bab diantaranya perancangan *database*, perancangan interaksi antar objek, dan perancangan *user interface*.

BAB VI IMPLEMENTASI

Pada bab ini berisi hasil dari implementasi berdasarkan perancangan yang telah dibuat. Terdiri hasil implementasi fitur-fitur aplikasi yang dibuat.

BAB VII PENGUJIAN

Pada bab ini berisi kesimpulan hasil pengujian aplikasi berdasarkan fitur-fitur yang telah didefinisikan. Terdiri dari penjelasan lingkup pengujian dan hasil pengujian.

BAB VIII PENUTUP

Pada bab ini berisi kesimpulan dan saran mengenai aplikasi yang telah dibuat. Kesimpulan yang dimaksud yaitu mengenai penyebutan tercapai atau tidaknya fitur sesuai dengan tujuan yang sudah ditetapkan. Saran yang dimaksud saran mengenai fitur yang akan dikembangkan pada aplikasi.

BAB II

TINJAUAN PUSTAKA

Bab ini menjelaskan tinjauan pustaka yang digunakan selama proses pengembangan aplikasi dilakukan. Bab ini terdiri atas tinjauan karya ilmiah sejenis sebelumnya dan dasar teori.

II.1 Karya Ilmiah Sejenis Sebelumnya

Terdapat karya ilmiah sejenis dan aplikasi sejenis yang digunakan penulis sebagai sumber referensi dalam pengembangan aplikasi yang dijelaskan pada tabel II.1

Tabel II. 1 Karya ilmiah sebelumnya

No.	Tahun	Judul Karya Tulis Ilmiah	Penulis
1.	2019	Digital Signature untuk Menjaga Keaslian Data dengan Algoritma MD5 dan Algoritma RSA	Budi K. Hutasuhut, Syahril Efendi, dan Zakarias Situmorang
2.	2017	Implementasi <i>Digital Signature</i> dalam Validasi Online <i>Local E-Government</i> Menggunakan Algoritma RSA dan MD5	Prasta Muhtadin

Di bawah ini akan dijelaskan hasil analisa pengetahuan karya tulis ilmiah yang dipakai sebagai referensi, yaitu:

1. Karya ilmiah yang berjudul “*Digital Signature untuk Menjaga Keaslian Data dengan Algoritma MD5 dan Algoritma RSA*” menjelaskan bagaimana *digital signature* dapat menjaga keaslian untuk meyakinkan penerima data bahwa data tersebut tidak diubah oleh pihak lain, dan jika telah diubah, maka penerima akan mengetahui bahwa data tersebut sudah dimodifikasi. Dalam penelitian ini, digunakan Algoritma RSA untuk membuat kunci *private* dan publik dan Fungsi Hash MD5 untuk menghasilkan *message digest*. Sistem yang dibuat dalam penelitian dibangun menggunakan bahasa pemrograman PHP. Pengujian yang

dilakukan dalam penelitian ini adalah dengan menguji *digital signature* dari file berformat .jpg sebelum ditambahkan coretan dengan *digital signature* dari file berformat .jpg sesudah ditambahkan coretan. Hasilnya file berformat .jpg yang diberi coretan, *digital signature*-nya berubah sehingga saat diverifikasi file tersebut tidak valid. Selain itu dilakukan pengujian lamanya waktu proses *digital signature* dari berbagai format file. Format file yang diuji adalah format file .txt, .jpg, .pdf, .docx, .xlsx, .rar, .mp3, dan .mp4. Hasil pengujinya adalah file berformat .mp3 berukuran 4,15 mb waktu prosesnya paling lama jika dibandingkan dengan format file lain.

Hal yang menjadi pembelajaran pada karya ilmiah ini adalah kombinasi algoritma RSA dan MD5 dapat meningkatkan keamanan pada keaslian data. Maka pada penggeraan tugas akhir ini akan diterapkan algoritma RSA dan MD5 untuk mengimplementasikan Tanda Tangan Digital (Digital Signature) ini. Selain itu juga bahasa pemrograman PHP dipilih untuk membangun sistem *digital signature* ini dikarenakan bersifat *open source* dan mudah dilakukanya pengembangan karena sudah banyak terdapat dokumentasi dan referensinya di internet.

2. Karya ilmiah yang berjudul "***Implementasi Digital Signature dalam Validasi Online Local E-Government Menggunakan Algoritma RSA dan MD5***" menjelaskan bagaimana mengimplementasikan Digital Signature dalam validasi sebuah dokumen. Tujuan penelitian ini adalah mengimplementasikan digital signature pada validasi online sistem *local e-government* menggunakan algoritma RSA dan MD5. Penelitian ini menghasilkan sistem yang dapat melakukan fungsi dasar pengajuan permohonan dan penerimaan permohonan, serta mampu memberikan layanan standar digital signature seperti pembangkitan kunci, pembangkitan tanda tangan digital, dan verifikasi permohonan. Karya ilmiah ini memiliki kesamaan dengan topik yang akan diangkat yaitu digital signature memakai algoritma RSA dan MD5.

Hal yang menjadi pembelajaran pada karya ilmiah ini adalah terdapat beberapa hal yang serupa akan diimplementasikan pada aplikasi yang akan dibangun yaitu dari sisi algoritmanya. Pada pengerjaan tugas akhir ini akan diterapkan algoritma RSA dan MD5 yang terinspirasi dari karya ilmiah kedua ini.

II.2 Dasar Teori

Dalam pengerjaan Tugas Akhir, dibutuhkan beberapa pemahaman teori dalam pelaksanaan tugas akhir. Berikut adalah beberapa dasar teori yang digunakan.

II.2.1 Tugas Akhir

Tugas Akhir (TA) merupakan aktivitas berbentuk proyek yang berlangsung pada semester akhir program Diploma Tiga dan memiliki beban 4 SKS. Tugas akhir dikerjakan oleh 1 – 3 mahasiswa dan dibimbing oleh dosen yang berkompетensi dan berkualifikasi yang sesuai.[6]

II.2.2 Digital Signature

Digital signature adalah suatu mekanisme kriptografi yang dapat digunakan untuk menjaga keaslian suatu data, sehingga penerima mengetahui dengan pasti apakah data yang diterima itu asli atau data palsu. Teknik ini mencegah penggunaan data palsu oleh penerima data. Semua data yang diterima memiliki tanda tangan yang selalu berbeda dengan data lainnya, sehingga perubahan kecil saja akan mengubah tanda tangan secara signifikan.[12]

II.2.3 Fungsi Hash

Fungsi *Hash* sering disebut dengan fungsi *Hash* satu arah (*one-way function*). *Message digest*, fungsi kompresi dan *fingerprint* adalah suatu fungsi matematika yang mengambil input dengan panjang variabel dan mengubahnya menjadi urutan biner dengan panjang tetap. Fungsi *Hash* biasanya dibutuhkan bila ingin membuat kode unik dari suatu pesan. Kode unik pada pesan menunjukkan bahwa pesan tersebut benar-benar dikirim dari pengirim yang sebenarnya.[1]

II.2.4 Algoritma RSA

RSA adalah algoritma kriptografi untuk enkripsi kunci publik (*public-key encryption*). Pada algoritma ini terdapat tiga proses yaitu, pembangkitan kunci, proses enkripsi, dan dekripsi. Letak kesulitan algoritma ini adalah bagaimana menentukan dua faktor bilangan prima yang besar yang akan digunakan sebagai kunci publik dan kunci privat.[2]

Dalam Tugas Akhir ini, algoritma ini digunakan untuk membuat kunci privat dan kunci publik, enkripsi, dan dekripsi laporan Tugas Akhir.

Proses yang terdapat pada algoritma RSA ini diantaranya :

1. Pembuatan kunci publik dan privat

Langkah-langkah pembuatan kunci pada algoritma RSA :

1. Pilih bilang prima p dan q (p dan q rahasia).
2. Hitunglah nilai n dengan rumus :

$$n = p \times q \quad (p \neq q)$$

Nilai n ini tidak perlu dirahasiakan.

3. Hitunglah nilai m dengan rumus :

$$m = (p - 1)(q - 1)$$

Nilai m ini harus dirahasiakan.

4. Pilihlah sebuah bilangan bulat sebagai kunci publik (e), yaitu relatif prima terhadap m. e relatif prima terhadap m artinya faktor pembagi terbesar keduanya adalah 1, secara matematis disebut GCD (m,e) =1. Untuk mencarinya dapat digunakan algoritma Euclid. Nilai e bersifat tidak rahasia. Kunci publik ini tidak dirahasiakan. [10]

Syarat kunci publik :

$$e = e > 1 \text{ and } \text{GCD } (m,e) = 1$$

5. Dipilih sebuah bilangan bulat sebagai kunci privat (d). Syaratnya :

$$d = (d * e) \bmod m = 1$$

Kunci privat ini harus dirahasiakan.

2. Enkripsi

Enkripsi adalah data yang dikunci dengan kunci publik (n,e) agar data (informasi) yang akan dikirimkan (P) tidak diketahui orang lain. Lalu, hitung *ciphertext* (c) dengan rumus : [11]

$$c = p^e \bmod n$$

3. Dekripsi

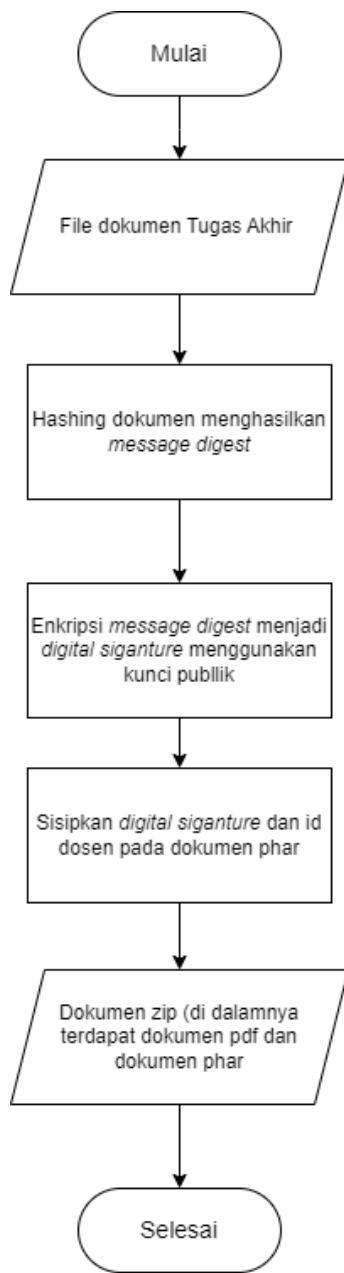
Dekripsi adalah metode untuk mendapatkan data (informasi) yang telah dienkripsi (n,e) dari pengirim untuk membaca data asli menggunakan kunci privatnya, dapat didekripsi dengan rumus : [11]

$$P = c^d \bmod n$$

II.2.5 Aplikasi WEB

Aplikasi web adalah suatu aplikasi yang diakses menggunakan penjelajah web melalui suatu jaringan seperti internet atau intranet. Ia juga suatu aplikasi perangkat lunak komputer yang dikodekan dalam bahasa yang didukung penjelajah web (seperti ASP, Perl, Java, JavaScript, PHP, Python, Ruby, dll.) dan bergantung pada penjelajah tersebut untuk menampilkan aplikasi (Kontributor Wikipedia, 2020).[3]

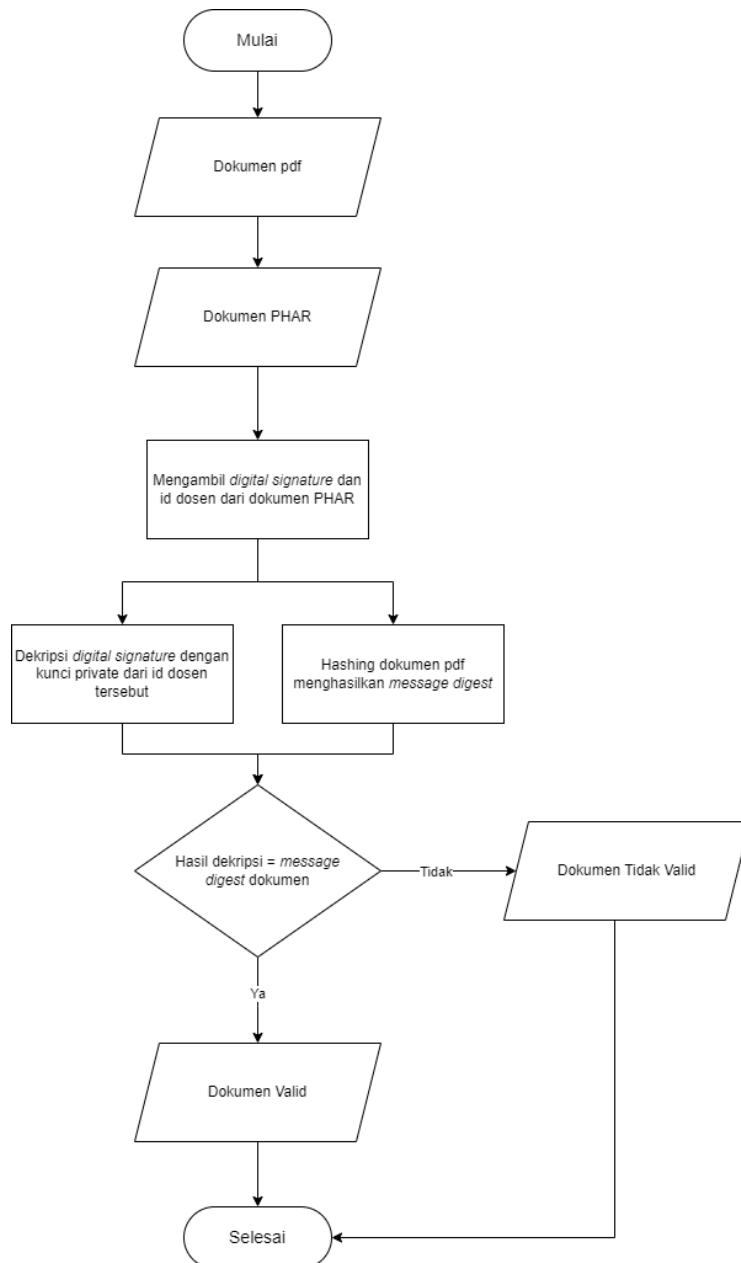
II.2.6 Tahapan Enkripsi Dokumen



Gambar II. 1 Tahapan enkripsi dokumen

Tahapan dari enkripsi dokumen adalah file dokumen diubah terlebih dahulu menjadi *message digest* dengan menggunakan fungsi *hash*. Setelah itu enkripsi *message digest* dengan menggunakan algoritma RSA dan kunci publik. Hasilnya adalah *digital signature*. Dalam aplikasi ini, *digital signature* ini disisipkan beserta id dosen di file berekstensi phar.[13]

II.2.7 Tahapan Validasi Dokumen



Gambar II. 2 Tahapan validasi dokumen

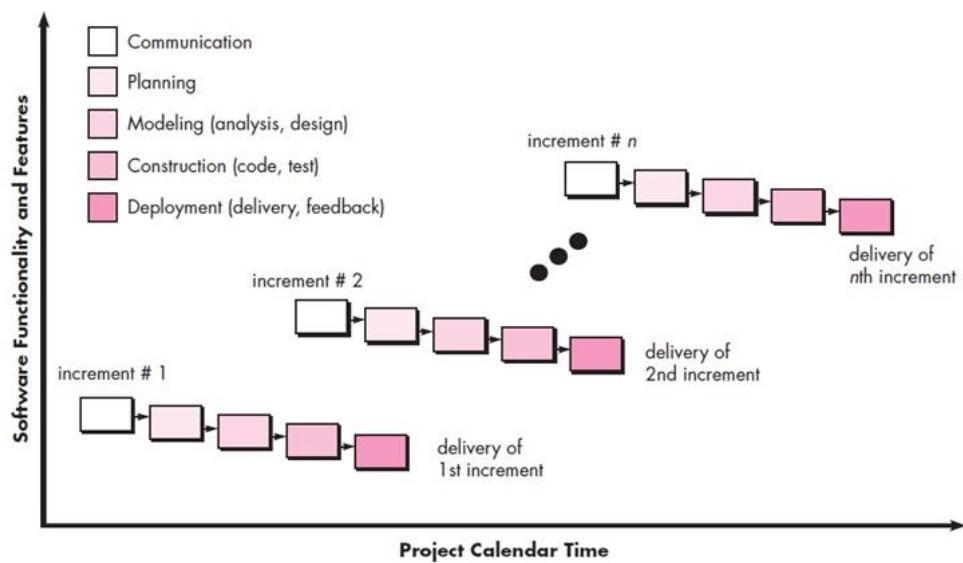
Tahapan dari deskripsi dokumen adalah dengan mengunggah dokumen pdf dan juga PHAR. Lalu memisahkan *digital signature* dan id dosen yang ada pada dokumen phar. Lalu deskripsi *digital signature* tersebut dengan menggunakan kunci private algoritma RSA. Lalu lakukan hashing pada dokumen pdf untuk mengambil *message digest*. Jika hasil deskripsi *digital signature* ini sama dengan

message digest dari dokumen maka dokumen tersebut valid atau asli dari si pengirim dokumen. Jika hasil dekripsi *digital signature* ini tidak sama dengan *message digest* dari dokumen maka dokumen tersebut tidak valid atau bukan dari pengirim aslinya.[13]

II.2.8 SDLC - Incremental

Incremental model merupakan model pengembangan sistem pada *software development* dengan memecah suatu proses besar menjadi proses-proses kecil sehingga model pengembangannya dilakukan secara bertahap. *Incremental model* menggambarkan suatu proses dimana mengutamakan perhatian pada sistem *requirement* dan mengimplementasikan dalam *team development*. Dengan menggunakan SDLC *Incremental*, *requirement* dan ruang lingkup perlu didefinisikan dengan baik, agar ketika masuk ke proses increment tidak terjadi perluasan ruang lingkup.

Berdasarkan Pressman edisi-7, tahapan *incremental model* adalah sebagai berikut:[16]



Gambar II. 3 Tahapan *increment*

1. *Communication*

Communication merupakan tahap komunikasi dengan tim pengembang untuk memperjelas tujuan dari *increment* yang akan dikerjakan, serta output dari *increment* tersebut. Hasil dari tahap ini yaitu *functional requirements* dan *non-functional requirements*.

2. *Planning*

Tahap *planning* merupakan tahap untuk melakukan perencanaan pada *increment* tersebut, dalam hal ini dapat mendiskusikan kembali *timeline increment* yang akan dikerjakan, pembagian tugas kepada tiap anggota.

Kegiatan yang dilakukan pada tahap ini yaitu memperkirakan waktu pengerjaan tugas yang akan dilakukan, penyusunan jadwal pengerjaan tugas, serta menganalisa risiko-risiko yang mungkin terjadi pada setiap tahap pengembangan perangkat lunak. Hasil dari tahap ini yaitu jadwal pelaksanaan.

3. *Modelling (Analysis, design)*

Tahap ini melakukan desain terhadap aplikasi yang akan dibuat, dapat berupa desain tampilan, desain sistem dan mendesain database.

Kegiatan yang akan dilakukan pada tahap ini yaitu analisis desain, mulai dari desain arsitektur sistem, proses bisnis, database, hingga user interface. Hasil dari tahap ini yaitu *use case diagram, user stories, wireframe, dan mockup*.

4. *Construction (Code, test)*

Tahap *construction* terdiri dari 2 pekerjaan yaitu :

- a. *Code* merupakan mengimplementasikan desain yang telah dirancang pada tahap *modeling*.
- b. *Testing*, tahap untuk melakukan pengecekan terhadap hasil code.

Hasil dari tahap ini yaitu *prototype, test plan, dan test case*.

5. Deployment (*delivery, feedback*)

Tahap deployment merupakan tahap penyampaian hasil dari *increment* kepada *user*. Pada tahap ini, akan didapatkan *feedback* yang akan dijadikan evaluasi untuk melaksanakan *increment* selanjutnya dengan cara fitur aplikasi akan didemokan kepada pengguna. Tujuan dari mendemokan fitur aplikasi ini untuk mendapatkan *feedback* dari pengguna.

II.3 Teknologi yang digunakan

Terdapat beberapa teknologi yang digunakan dalam pengerjaan Tugas Akhir ini. Berikut adalah teknologi yang digunakan dalam pengerjaan Tugas Akhir ini.

II.3.1 Bahasa Pemrograman PHP

PHP (Hypertext Preprocessor) menurut Anhar (2010 : 3) adalah sebuah bahasa pemrograman yang digunakan untuk membuat *web* dan bersifat *open source*. Dengan menggunakan PHP, *website* akan lebih dinamis. Selain itu, kelebihan dari PHP ini adalah dapat terintegrasi dengan database seperti MySQL.

Dalam aplikasi yang akan dibangun pada Tugas Akhir ini, PHP digunakan sebagai bahasa pemrograman untuk pengembangan aplikasi berbasis web. Selain lebih memiliki banyak fungsi dan *library* yang dapat digunakan, PHP merupakan salah satu bahasa pemrograman yang lebih mudah dan nyaman digunakan.

II.3.2 MariaDB

MariaDB adalah sistem database tipe MySQL yang open source. MariaDB juga merupakan pengganti MySQL yang ditingkatkan. MariaDB ini dikembangkan pada tahun 2009 oleh MySQL. MariaDB sudah mendukung API dan dukungan klien. MariaDB ini digunakan sebagai database dalam aplikasi ini.[16]

II.3.3 Framework Codeigniter 4

Supono dan Putratama (2016:109) mendefinisikan CodeIgniter sebagai “Aplikasi open source berupa framework dengan model MVC (Model, View, Controller) untuk membangun website dinamis dengan menggunakan PHP.[7]

Codeigniter ini digunakan sebagai *framework* utama dari pengembangan aplikasi ini. Selain bersifat *open-source* codeigniter juga salah satu *framework* yang dapat dipahami dengan mudah dan tidak memerlukan waktu banyak untuk dipelajari lagi.

II.3.4 Bootstrap

Bootstrap menurut Josi (2016) adalah framework ataupun tools untuk membuat aplikasi web ataupun website yang bersifat responsive secara cepat, mudah dan gratis. Kata responsive disini berarti bahwa tampilan web (lebar dan susunan isinya) dapat berubah secara otomatis sesuai dengan lebar layar yang menampilkannya.[8]

Bootstrap akan digunakan sebagai *framework* CSS dari aplikasi yang akan dibangun. Bootstrap cukup dikenal dan banyak digunakan oleh para pengembang baik baru maupun lama, dan juga bootstrap ini mendukung bahasa PHP sehingga dapat digunakan untuk pengembangan aplikasi ini.

II.3.5 CSS

Menurut Hidayat, Hartono, dan Sukiman (2017), CSS merupakan salah satu bahasa pemrograman yang bertujuan membangun tampilan web lebih terstruktur sehingga tampilan web tersebut lebih menarik, selain itu CSS memiliki arti menata sebuah halaman bertingkat, yang artinya CSS memiliki format elemen induk dan format elemen anak dimana format elemen anak tersebut akan secara otomatis mengikuti format elemen induknya ketika elemen format induknya berubah.[9]

II.3.6 Library TCPDF

TCPDF adalah kelas PHP perangkat lunak sumber terbuka dan gratis untuk menghasilkan dokumen PDF. TCPDF adalah satu-satunya perpustakaan berbasis PHP yang menyertakan dukungan lengkap untuk UTF-8 Unicode dan bahasa kanan-ke-kiri, termasuk algoritma dua arah.[17]

II.3.7 Library phpseclib

Library phpseclib merupakan library yang menyediakan implementasi PHP murni dari SSH2, SFTP, RSA, DSA, Elliptic Curves, AES, ChaCha20, X.509, CSR, CRL, SPKAC, dll. Ekstensi yang terdapat dalam library ini seperti bcmath, gmp, libsodium, dan openssl.[18]

II.3.8 Library FPDI

FPDI adalah kumpulan kelas PHP yang memfasilitasi pengembang untuk membaca halaman dari dokumen PDF yang ada dan menggunakannya sebagai template di FPDF, yang dikembangkan oleh Olivier Plathey. Selain salinan FPDF, FPDI tidak memerlukan ekstensi PHP khusus.[19]

II.3.9 Library PHAR

Phar adalah ekstensi php yang menyediakan sarana untuk mendistribusikan kode sebagai arsip tunggal, yang tidak harus diekstrak ke folder sebelum digunakan. Konsepnya mirip dengan JVM Jars: setiap arsip menjadi direktori virtual tempat file dapat diakses. Namun, folder virtual tidak terbatas pada pemuatan kelas, tetapi Anda dapat membuka dan membaca file internal seolah-olah didekompresi ke dalam direktori. Phar tersedia untuk PHP 5.3 dan yang lebih baru.[20]

II.3.10 Apache

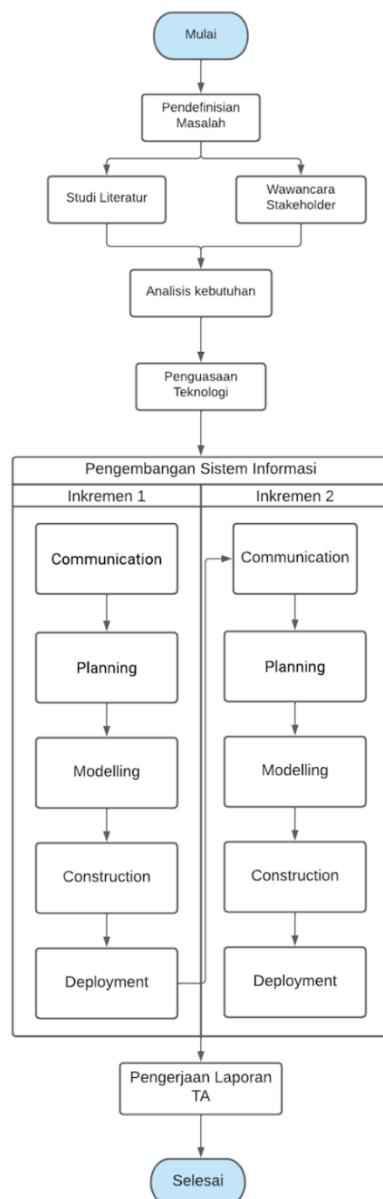
Apache adalah salah satu jenis web server populer yang memungkinkan pengguna mengunggah website di internet. Apache ini dirilis pada tahun 1995 dan sampai masih populer. Apache juga bersifat open source. Jenis web server yang digunakan di aplikasi ini adalah apache.[21]

BAB III

METODOLOGI PELAKSANAAN

Pada bab ini berisi tahapan-tahapan yang digunakan dalam menyelesaikan Tugas Akhir ini.

III.1 Alur Pelaksanaan



Gambar III. 1 Alur pelaksanaan

Tahapan yang akan dilakukan dalam menyelesaikan Tugas Akhir ini adalah:

1. Pendefinisian masalah

Tahap awal yang akan dilakukan adalah mendefinisikan masalah. Selama fase ini melibatkan menentukan latar belakang, rumusan masalah, tujuan, ruang lingkup serta batasan pengembangan aplikasi dengan berdiskusi bersama anggota tim dan dosen pembimbing untuk menentukan kelayakan topik permasalahan yang diangkat dan mengidentifikasi stakeholder. Penulis mencari informasi terhadap isu dari dokumen laporan Tugas Akhir di JTK Polban dengan cara wawancara stakeholder dan mengumpulkan dokumen yang terlibat.

2. Studi Literatur

Setelah mendefinisikan masalah, penulis melakukan kegiatan eksplorasi untuk mengumpulkan informasi dan pengetahuan terkait landasan atau referensi untuk memenuhi kebutuhan dan menyelesaikan pengembangan aplikasi. Studi literatur bersumber dari buku, jurnal, dan karya ilmiah serupa. Berdasarkan aplikasi yang akan dibangun, terdapat beberapa teknologi yang perlu dipelajari, yaitu Digital Signature, Algoritma RSA, Fungsi Hash, Aplikasi Web, Enkripsi dan Dekripsi.

3. Wawancara Stakeholder

Setelah memahami permasalahan yang terjadi secara umum dan mempelajari mengenai hal yang dibutuhkan, setelahnya dilakukan wawancara stakeholder untuk lebih memusatkan kebutuhan dan masalah apa yang krisis dan perlu diperhatikan menjadi fokus utama dari topik yang telah ditentukan. Dilakukan wawancara terhadap salah satu stakeholder yaitu dosen yang pernah menjadi pembimbing, penguji dan koordinator pada tugas akhir.

4. Penguasaan teknologi

Pada tahap ini dilakukan penguasaan teknologi yang dibutuhkan dalam pengembangan perangkat lunak. Pada pelaksanaan tugas akhir ini menggunakan teknologi PHP dengan framework Codeigniter 4. Penulis mempelajari teknologi yang akan digunakan melalui dokumentasi teknologi tersebut, *ebook* teknologi terkait, video di *Youtube* dan mencari *project* yang telah dibangun oleh orang lain untuk dipelajari.

5. Pengembangan Aplikasi

Pengembangan aplikasi ini akan dilakukan dengan menggunakan model SDLC *Incremental*. Berikut rincian kegiatan pengembangan aplikasi.

Tabel III. 1 Tahap inkremen

Tanggal Mulai	Tanggal Selesai	Target		Artefak
<i>Increment 1</i>				
28 Februari 2021	27 Maret 2021	<i>Communication</i>	Wawancara dengan <i>stakeholder</i>	Lampiran Hasil Wawancara
		<i>Planning</i>	Membuat <i>planning documentation</i>	Dokumentasi <i>planning</i>
			Membuat SRS v.1	Dokumen SRS
			Merancang skema database	<i>Entity Relationship Diagram</i>
		<i>Modelling</i>	Merancang desain fitur autentikasi	Mockup aplikasi
			Merancang desain fitur registrasi	
		<i>Construction</i>	Implementasi fitur autentikasi	Produk Inkremen 1
			Implementasi fitur registrasi	

		<i>Deployment</i>	Melakukan diskusi dengan <i>user</i> terkait fitur yang telah diimplementasikan	
<i>Increment 2</i>				
28 Maret 2021	24 April 2021	<i>Communication</i>	Berdiskusi dengan anggota kelompok dan pembimbing	Lampiran Hasil Diskusi
		<i>Planning</i>	Membuat planning documentation	Planning Dokumentasi
		<i>Modelling</i>	Membuat SRS v.2	Dokumen SRS
			Merancang desain fitur verifikasi dokumen	Mockup aplikasi
			Merancang desain fitur enkripsi dan digital signature	
			Merancang desain fitur unggah dokumen	
			Merancang desain fitur unduh dokumen	
			Merancang desain fitur membubuhkan tanda tangan dosen	
		<i>Construction</i>	Implementasi fitur verifikasi dokumen	Produk Inkremen 2
			Implementasi fitur enkripsi dan digital signature	
			Implementasi fitur unggah dokumen	
			Implementasi fitur unduh dokumen	
			Implementasi fitur membubuhkan tanda tangan dosen	
		<i>Deployment</i>	Melakukan UAT oleh <i>user</i> terkait yaitu mahasiswa, dosen pembimbing dan penguji, koordinator TA	Dokumen UAT

Keterangan warna pada *construction*:



: Mengambil modul dari *library*

: Membuat modul sendiri

6. Pengerjaan Laporan TA

Untuk pengerjaan laporan TA akan dikerjakan secara bertahap, bagian ini diisi untuk melengkapi penjelasan pada proposal.

BAB IV

ANALISIS

Analisis merupakan tahapan yang dilakukan dalam pengembangan aplikasi pada tugas akhir. Bab ini berisi berisi hasil analisis mengenai sistem yang berjalan di JTK Polban, analisis aplikasi sejenis, dan analisis aplikasi yang akan dibangun. Analisis dilakukan untuk mendapatkan gambaran detail mengenai sistem yang sedang berjalan dan mempelajari masalah yang sedang terjadi, serta mendefinisikan requirement untuk perancangan pada pengembangan Aplikasi Tanda Tangan Digital.

IV.1 Analisis Sistem Berjalan

Analisis sistem berjalan menjelaskan secara detail terkait prosedur, stakeholder, dan data yang terlibat selama ini di JTK. Analisis sistem berjalan bertujuan untuk mengetahui proses dan karakteristik yang terjadi pada saat ini di lapangan. Tujuan akhir analisis adalah dapat mengetahui proses apa saja yang dapat terkomputerisasi untuk diimplementasikan ke dalam pengembangan aplikasi.

IV.1.1 Prosedur yang Berjalan Saat Ini

Analisis dilakukan terhadap lingkungan yang terlibat di dalam prosedur yang berlaku saat ini di JTK. Analisis *stakeholder* dan prosedur yang berlaku didapat dari hasil wawancara kepada dosen JTK yang berperan sebagai Koordinator TA dan membaca buku panduan Tugas Akhir program diploma tiga Polban.

Berdasarkan hasil wawancara dengan salah satu koordinator TA, terdapat beberapa aturan dalam proses tanda tangan Laporan Tugas Akhir. Aturan tersebut ialah Ketua Jurusan boleh menandatangani Laporan Tugas Akhir ketika pembimbing dan penguji sudah menandatangani Laporan Tugas Akhir.

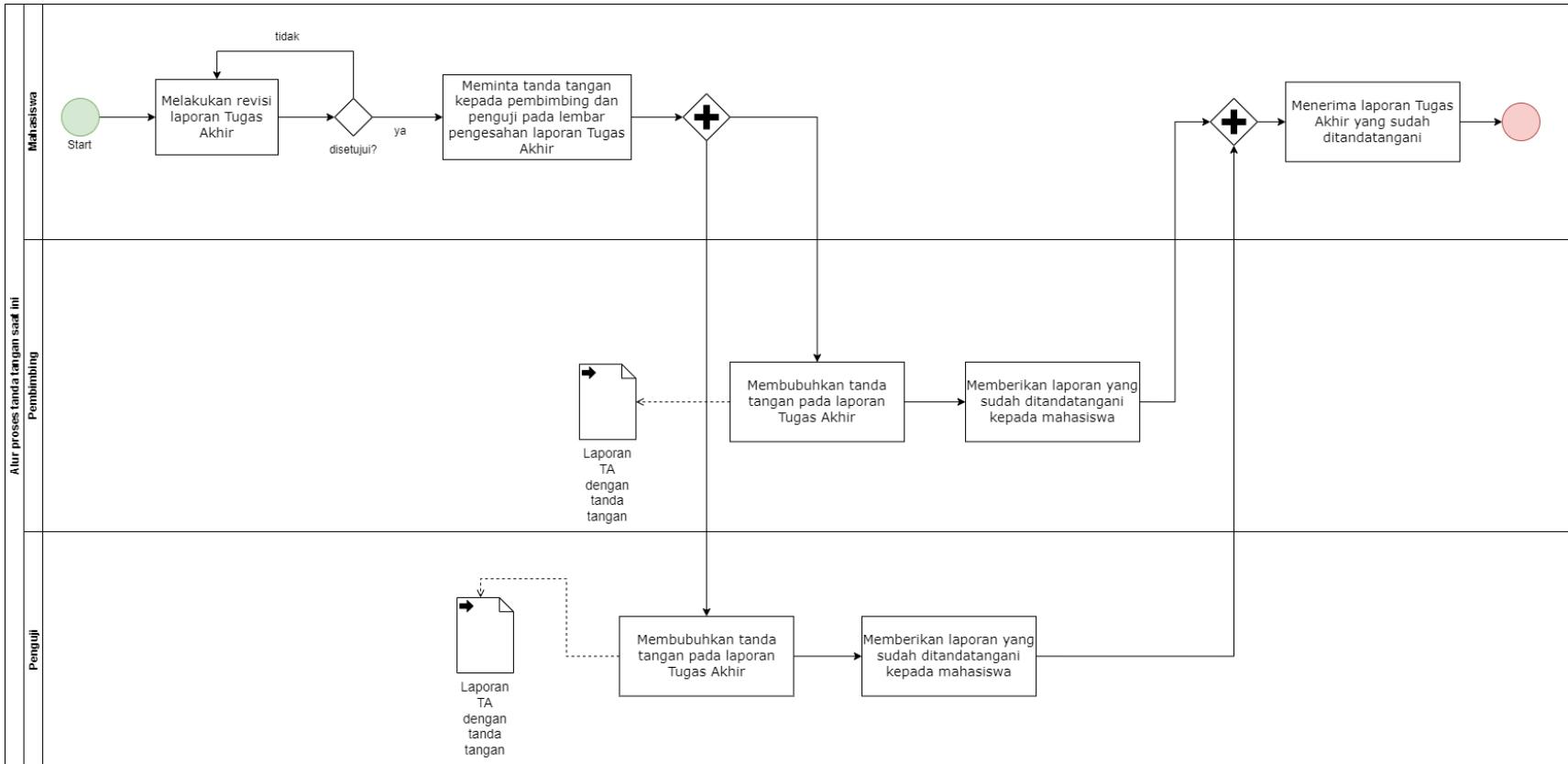
IV.1.2 Analisis Stakeholder yang Terlibat

Untuk menganalisis proses-proses yang terdapat pada sistem yang berjalan, perlu mengetahui beberapa stakeholders dan interest yang ada di JTK POLBAN. Terdapat 5 stakeholders yang terlibat pada penandatanganan Laporan Tugas Akhir. Pada Tabel berikut merupakan tabel yang menjelaskan stakeholders dan interest pada prosedur yang saat ini berjalan.

Tabel IV. 1 Jenis stakeholder

No.	Stakeholders	Deskripsi	Interest
1.	KoTA	KoTA (Kelompok Tugas Akhir) adalah mahasiswa aktif Polban yang sedang menempuh semester akhir di jurusan Teknik Komputer dan Informatika.	KoTA mengajukan dokumen Laporan Tugas Akhir kepada pembimbing, pengujian ketua jurusan untuk ditandatangani
2.	Pembimbing	Pembimbing adalah dosen Polban yang telah memenuhi kualifikasi untuk membimbing kegiatan Tugas Akhir berdasarkan kepakaran, golongan, dan jabatan fungsionalnya.	Pembimbing bertugas melaksanakan bimbingan dan evaluasi pelaksanaan Tugas Akhir mahasiswa bimbingannya.
			Pembimbing menandatangani laporan Tugas Akhir
3.	Pengujian	Pengujian adalah dosen di bidang ilmu yang ditunjuk oleh Jurusan untuk melakukan evaluasi terhadap mahasiswa atas Penyelesaian Laporan Tugas Akhir	Pengujian bertanggung jawab untuk mengevaluasi mahasiswa atas penyelesaian Laporan Tugas Akhir
			Pengujian menandatangani laporan tugas akhir
4.	Ketua Jurusan	Ketua jurusan adalah dosen yang mempunyai hak atas segala hal mengenai jurusan.	Ketua jurusan bertanggung jawab menandatangani laporan Tugas Akhir final.
5.	Koordinator TA	Koordinator TA adalah dosen pada jurusan di POLBAN yang ditunjuk oleh jurusannya sebagai panitia Tugas Akhir pada kurun waktu tertentu.	Koordinator TA bertanggung jawab untuk mengkoordinasikan mata kuliah TA yang meliputi tahap persiapan, penyusunan proposal, pelaksanaan, evaluasi hingga penyelesaian Tugas Akhir.

IV.1.3 Analisis Alur Proses Saat Ini



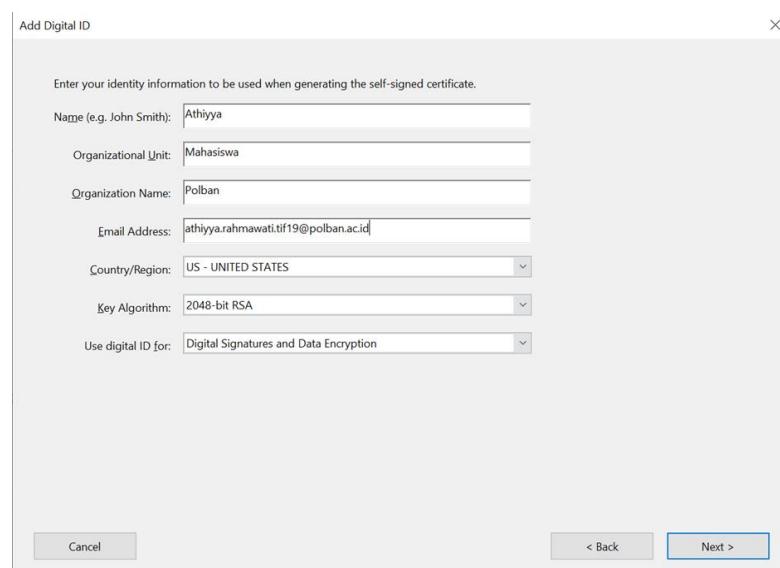
Gambar IV. 1 Alur proses saat ini

IV.2 Analisis Aplikasi Sejenis

IV.2.1 Adobe Acrobat Reader DC

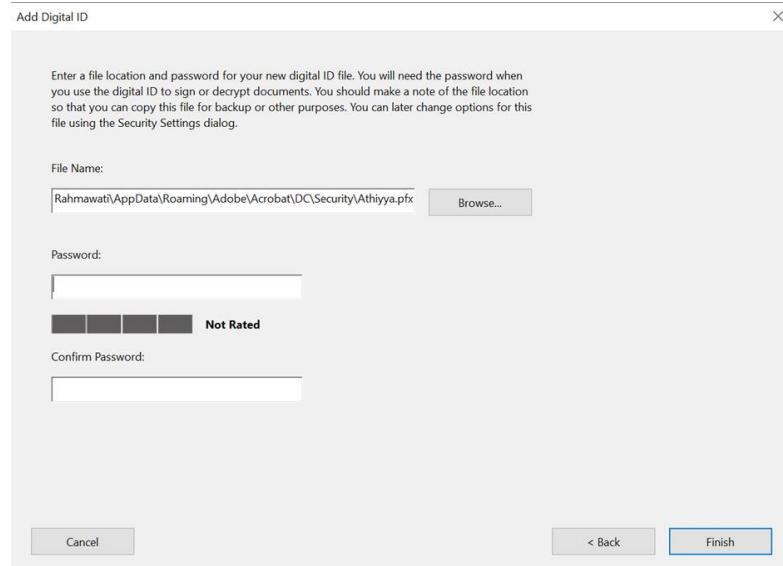
Acrobat Reader adalah salah satu perangkat lunak dari keluarga Adobe Acrobat yang dikembangkan oleh Adobe Systems. Pengguna Acrobat Reader dapat membaca, memberi notasi, mencari, verifikasi, *certificates*, menandai secara digital dan mencetak data dengan format Portable Document Format atau PDF.

Fitur pada Adobe Acrobat yang akan dibandingkan adalah fitur *certificates*. Fitur ini digunakan untuk mengenkripsi dokumen dan memverifikasi digital signature. Hal pertama untuk mengenkripsi dokumen adalah membuat digital ID. User akan diminta untuk mengisi form identitas.



Gambar IV. 2 Form identitas untuk menambahkan Digital ID pada Adobe Acrobat

Setelah itu, user akan diminta untuk membuat password untuk digital ID karena password ini akan digunakan ketika user menggunakan digital ID ini.



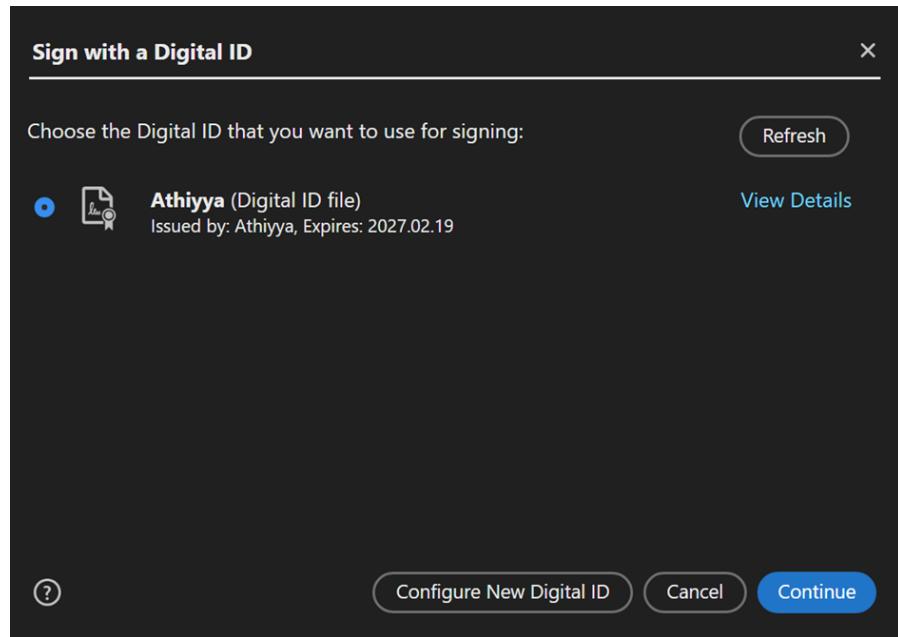
Gambar IV. 3 Halaman pilih lokasi penyimpanan Digital ID dan password Digital ID

Setelah digital ID dibuat, user baru bisa menggunakan digital ID untuk dibubuhkan ke dokumen. Untuk menggunakan digital ID ini, user cukup memilih area yang akan diberi digital ID/tanda tangan.



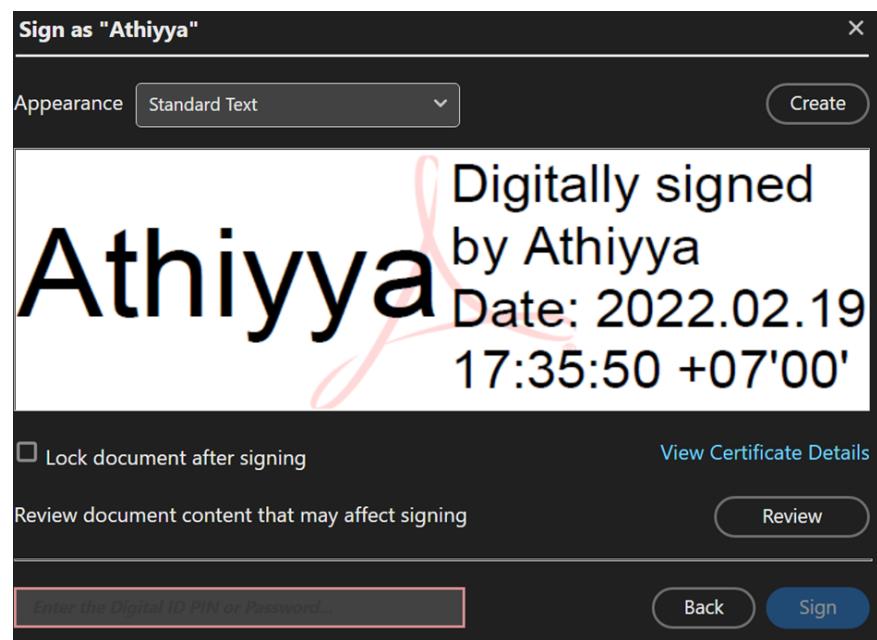
Gambar IV. 4 Pemilihan area penempatan Digital ID pada Adobe Acrobat

Setelah itu pilih digital ID yang akan digunakan.



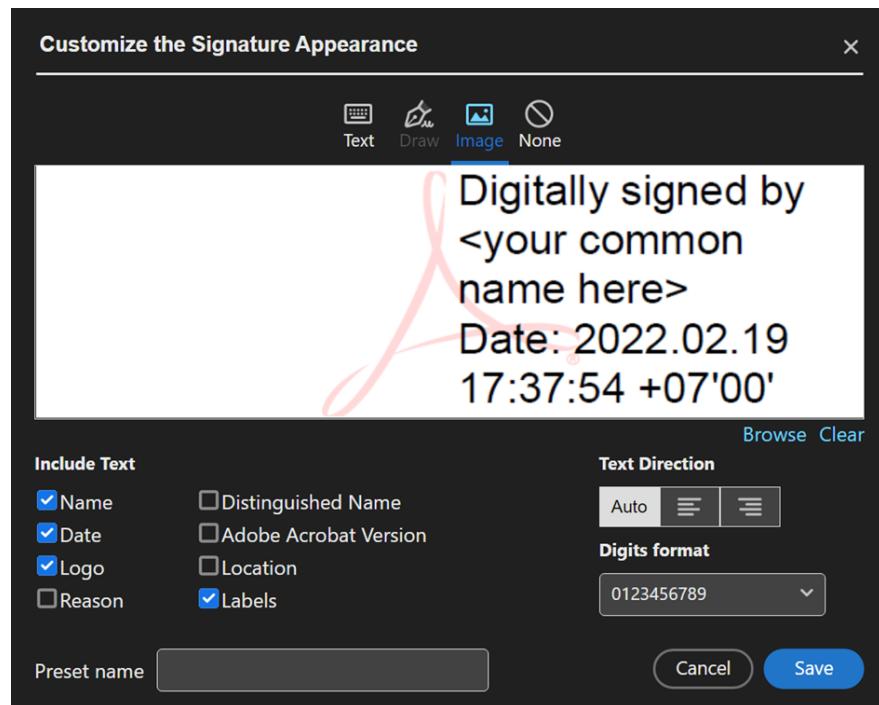
Gambar IV. 5 Pemilihan Digital ID yang akan digunakan pada Adobe Acrobat

Lalu masukan password dari digital ID yang digunakan.



Gambar IV. 6 Preview bentuk Digital ID yang akan digunakan pada Adobe Acrobat

Jika user ingin menambahkan tulisan atau citra tanda tangan, user bisa memilih menu '*View Certificate Details*'.



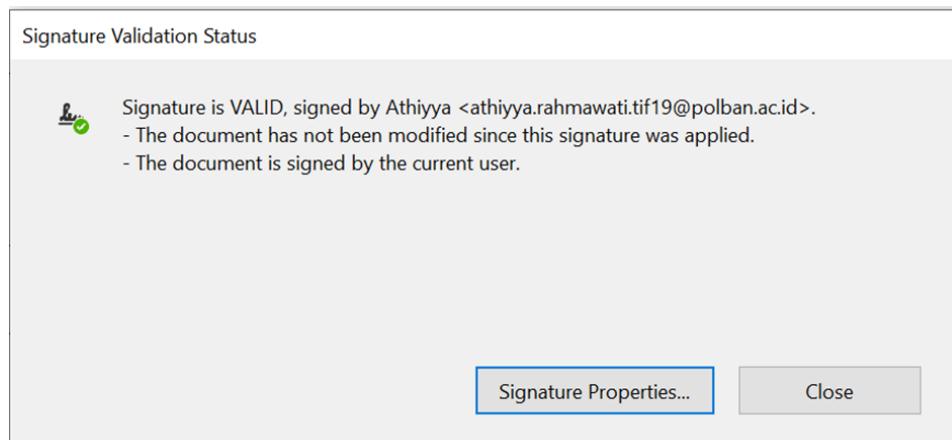
Gambar IV. 7 Halaman mengubah tampilan Digital ID pada Adobe Acrobat

Berikut tampilan file setelah diberi digital ID.



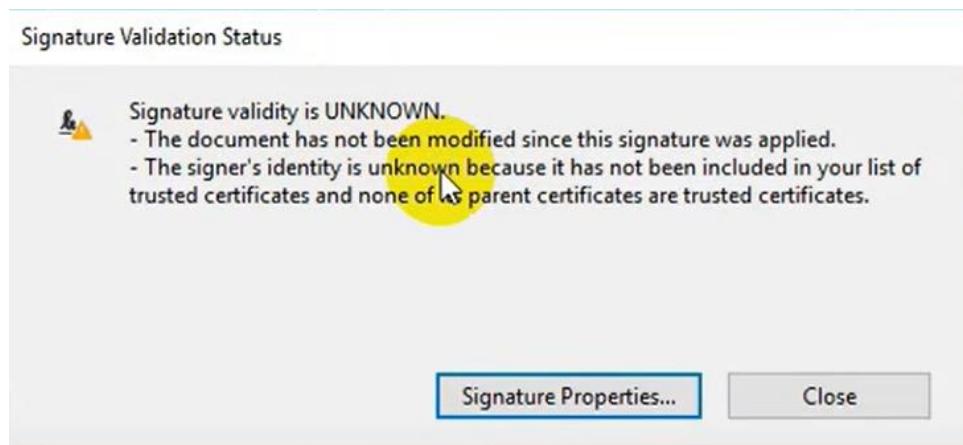
Gambar IV. 8 Tampilan Digital ID pada file

Selain itu user dapat melakukan verifikasi digital signature dari sebuah dokumen. Caranya masukan file sertifikat digital ID dari pengirim dokumen. Hal ini bertujuan agar aplikasi adobe acrobat ini mengenali bahwa digital ID si pengirim. Setelah itu buka dokumen yang akan diverifikasi. Pilih area yang terdapat digital ID atau tanda tangan. Lalu nantikan akan keluar popup berisikan validnya sebuah signature.



Gambar IV. 9 Tampilan status validasi yang valid

Berikut salah satu tampilan jika sebuah signature tidak memiliki sertifikat.



Gambar IV. 10 Tampilan status validasi yang tidak valid

Jadi agar dokumen dapat diverifikasi, pengirim harus mengirimkan juga sertifikat signaturenya kepada penerima dokumen.

IV.2.2 DocuSign

DocuSign merupakan sebuah aplikasi berbasis website yang menyediakan fitur tanda tangan elektronik, analisis kontrak dokumen, dan beberapa fitur lainnya. DocuSign akan menawarkan masa percobaan penggunaan aplikasi kepada pengguna yang baru mendaftar selama 30 hari.

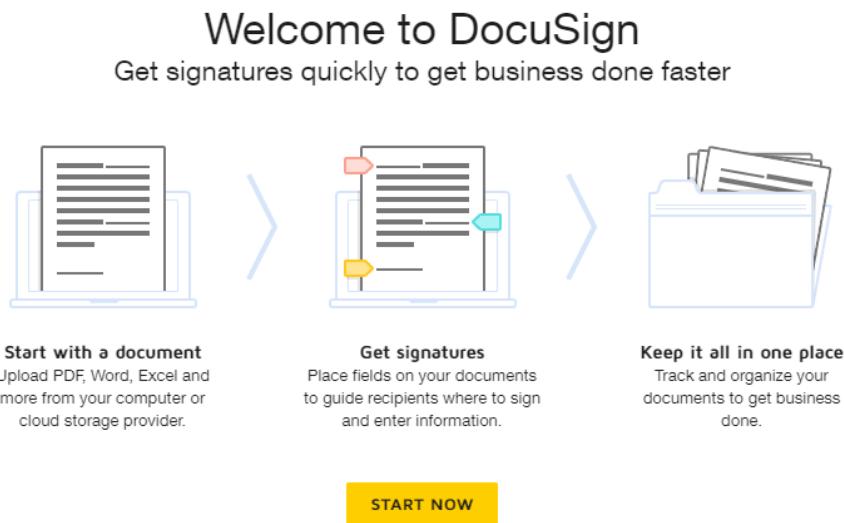
The screenshot shows a sign-up form for DocuSign. At the top, it says 'Try DocuSign free for 30 days' and 'No credit card required'. The form fields include 'First Name*' (Hilmy), 'Last Name*' (Oktoharitsa), 'Email*' (hilmy.oktoharitsa.tif1@polban.ac.id), 'Phone*' (redacted), 'Job Title*' (Student), 'Valid phone # required', 'Industry*' (Technology), and a 'GET STARTED' button. Below the button, a small note states: 'By clicking the 'Get Started' button above, you agree to the Terms & Conditions and Privacy Policy.'

Gambar IV. 11 Form identitas untuk mendaftar akun di DocuSign

DocuSign juga memberikan pilihan apakah pemilik akun akan melakukan integrasi atau tidak, jenis integrasi yang diberikan DocuSign antara lain adalah,

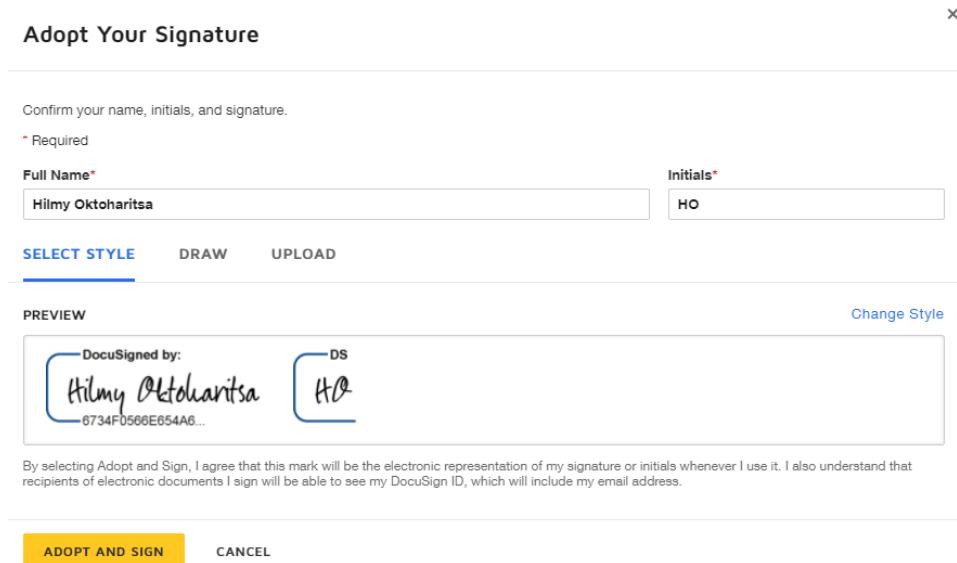
- a. CRM (*Customer Relationship Management*), dimana pengguna dapat melakukan integrasi dokumen dengan perusahaan lain yang sekiranya sedang melakukan kerja sama.
- b. ERP (*Enterprise Resource Planning*), integrasi ini diberikan agar pusat pengelolaan dalam bisnis bisa langsung diatur secara *real time* atau langsung.

3 fungsi utama dalam DocuSign adalah mengupload dokumen, tanda tangan digital, kemudian menyimpan file tersebut dalam cloud pada akun Docusign yang telah dibuat sebelumnya.



Gambar IV. 12 Halaman awal pada DocuSign

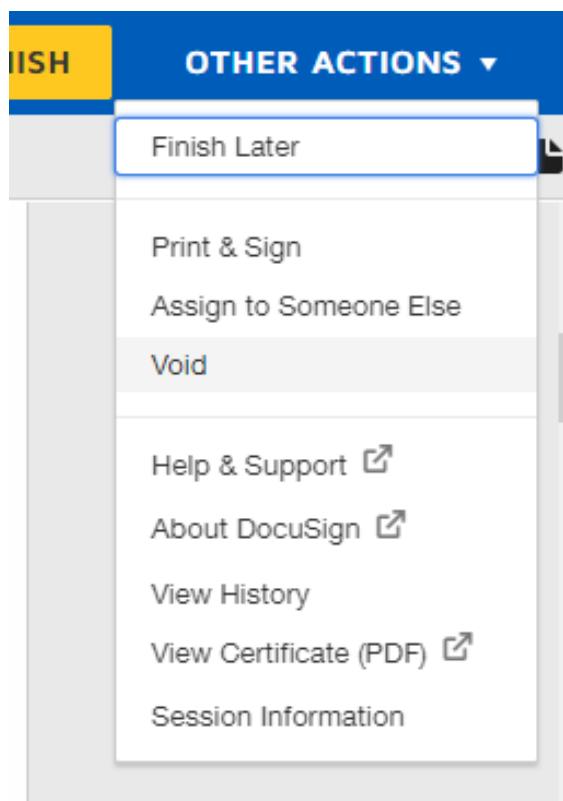
Setelah melakukan upload, maka DocuSign akan membuat sebuah desain tanda tangan berdasarkan info yang telah diberikan secara otomatis, atau pengguna dapat menggambar atau upload citra tanda tangan mereka sendiri, seperti yang terdapat pada gambar dibawah.



Gambar IV. 13 Halaman mengubah bentuk signature pada DocuSign

Terdapat beberapa fitur tambahan lain yang diberikan DocuSign seperti,

- a. *Print and Sign*, dimana dokumen yang sebelumnya di tanda tangan akan bisa langsung diunduh oleh pengguna, yang kemudian dapat dibagikan dengan orang lain menggunakan email.
- b. *Assign to Someone Else*, dokumen yang sebelumnya sudah ditandatangani oleh 1 pengguna dapat mengundang beberapa pengguna lain yang bisa menandatangani dokumen tersebut secara bersamaan.
- c. *Void*, fungsi fitur ini mengirimkan bahwa dokumen ditolak dan tidak ditandatangani yang kemudian pengguna juga dapat mengirimkan pesan kenapa dokumen tersebut dibatalkan/ditolak.



Gambar IV. 14 Dropdown fitur lain di DocuSign

Pada DocuSign ini tidak ditemukan untuk melakukan verifikasi dokumen, namun terdapat *ID Document* yang belum diketahui kegunaannya. Terdapat juga beberapa fitur yang masih dikunci untuk akun percobaan sehingga tidak dapat digunakan.

Tabel IV. 2 Perbandingan fitur aplikasi

Fitur-fitur	Adobe Acrobat	DocuSign	Aplikasi yang akan dibangun
Membuat digital ID	Ya	Ya	Ya
Enkripsi Dokumen	Ya	Tidak	Ya
Verifikasi Dokumen	Ya	Tidak	Ya
Ketentuan alur tanda tangan	Tidak	Tidak	Ya
Jenis Aplikasi	Offline	Online	Online

IV.3 Analisis Bisnis Proses Aplikasi yang Akan Dibangun

Pada sub bab ini akan dijelaskan mengenai analisis bisnis proses yang akan dibangun yaitu identifikasi bisnis proses, diagram bisnis proses dan alur proses.

IV.3.1 Identifikasi Bisnis Proses

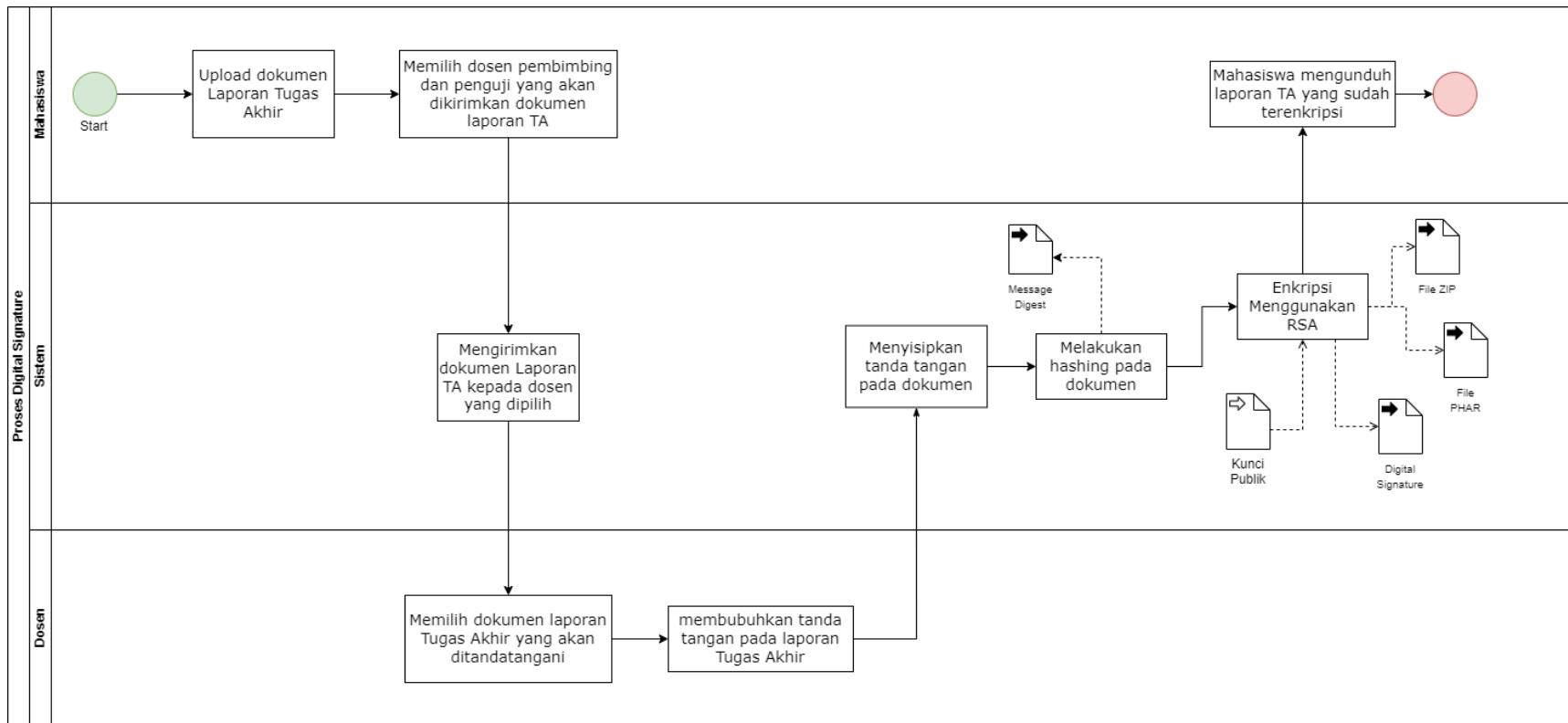
Tabel IV. 3 Identifikasi bisnis proses

No	ID Business Process	Nama Business Process	Deskripsi Business Process
1.	BP-001	Pembuatan <i>Digital Signature</i>	Proses ini digunakan oleh dosen pengirim untuk mengunggah laporan TA yang sudah ditandatangani olehnya
2.	BP-002	Verifikasi Dokumen Tugas Akhir	Proses ini digunakan oleh dosen penerima untuk mengunggah laporan TA yang telah ditandatangani dosen pengirim
3.	BP-003	Autentikasi	Proses ini digunakan oleh user untuk mengakses website.

IV.3.2 Diagram Bisnis Proses yang Diusulkan

IV.3.2.1 Proses Pembuatan Digital Signature

Pada proses bisnis ini mahasiswa mengunggah laporan TA ke sistem dan memilih dosen pembimbing dan penguji terkait. Setelah itu sistem akan mengenkripsi laporan TA. Hasilnya adalah laporan TA yang telah terenkripsi. Laporan TA yang telah terenkripsi ini dapat diunduh oleh Mahasiswa.



Gambar IV. 15 Bisnis proses digital signature

Berikut tabel penjelasan diagram BPMN proses pembuatan digital signature :

Tabel IV. 4 Penjelasan diagram proses pembuatan digital signature

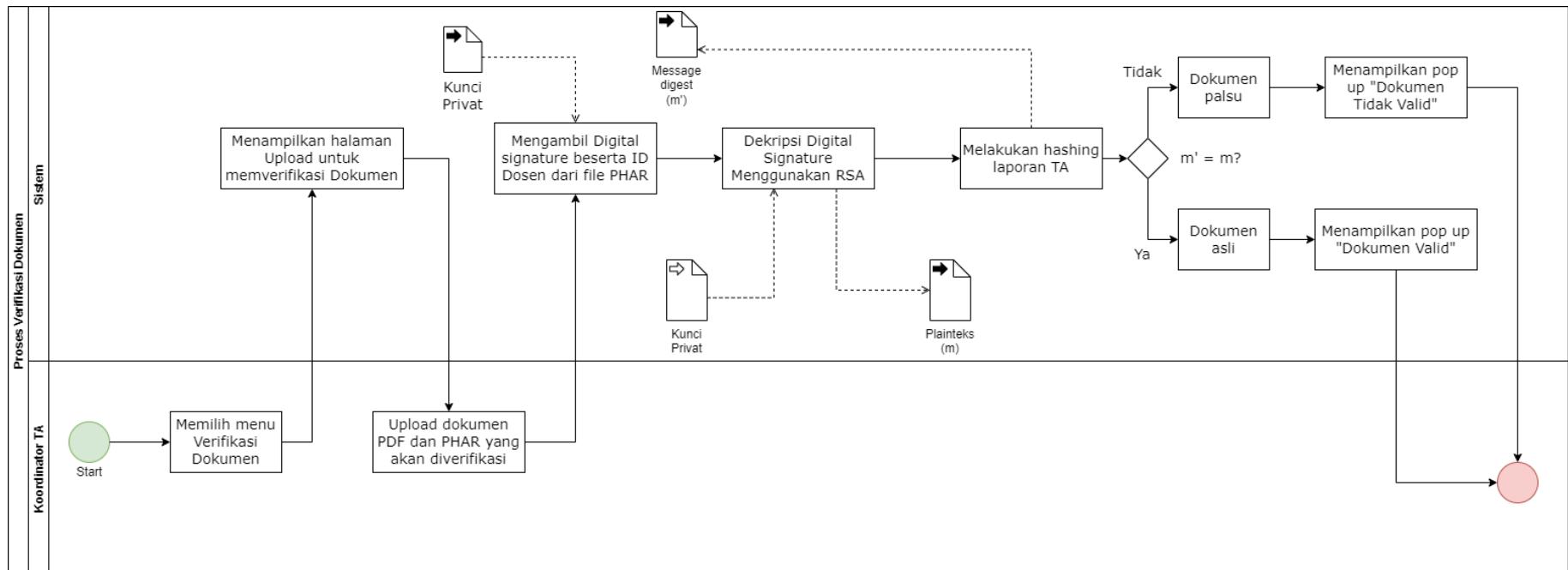
Nama Proses	Pembuatan Digital Signature
No Proses	BP-001
Business Process	<ol style="list-style-type: none">1. Mahasiswa mengunggah laporan TA dan memilih dosen terkait yang akan dikirimkan dokumen.2. Sistem menyimpan file laporan TA ke database3. Dosen membubuhkan tanda tangan pada dokumen laporan TA4. Dosen melakukan generate key5. Sistem melakukan proses pembangkitan kunci yang menghasilkan kunci privat dan kunci publik6. Sistem melakukan hashing pada laporan TA7. Sistem melakukan dekripsi laporan TA menggunakan algoritma RSA dan kunci publik8. Mahasiswa mengunduh laporan TA yang sudah terenkripsi
Input	Data Dokumen Laporan Tugas Akhir
Output	<ul style="list-style-type: none">• Dokumen Laporan Tugas Akhir yang sudah terdapat digital signature• Kunci Publik• Kunci Privat

Ketentuan Proses :

1. Dokumen yang ditangani dalam sistem ini adalah laporan tugas akhir.
2. Satu laporan tugas akhir ini dibuat oleh 1 kelompok Tugas Akhir
3. Kelompok Tugas Akhir sudah menyelesaikan semua revisi yang didapat saat sidang
4. Mahasiswa yang dimaksud ialah ketua kelompok tugas akhir.
5. Jumlah pembimbing dan penguji tergantung dari situasi dan kondisi.
6. Satu kelompok Tugas Akhir memiliki 1 akun.

IV.3.2.2 Proses Verifikasi Dokumen Laporan Tugas Akhir

Pada proses ini Admin mengunggah laporan TA yang akan diverifikasi. Setelah laporan TA terverifikasi, mahasiswa dapat mengunduh sertifikat digital signature.



Gambar IV. 16 Bisnis proses verifikasi dokumen laporan TA

Berikut tabel penjelasan diagram BPMN proses verifikasi dokumen tugas akhir :

Tabel IV. 5 Penjelasan diagram proses verifikasi dokumen

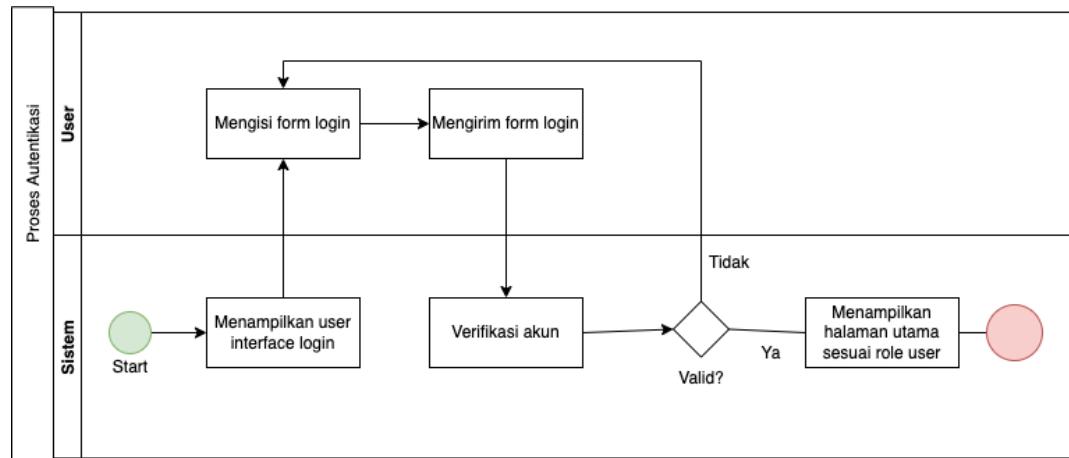
Nama Proses	Verifikasi Dokumen Laporan Tugas Akhir
No Proses	BP-002
Business Process	<ol style="list-style-type: none">1. Admin memilih menu Verifikasi Dokumen2. Sistem menampilkan halaman verifikasi dokumen3. Admin mengunggah laporan TA4. Sistem melakukan dekripsi dokumen laporan TA menggunakan kunci privat yang dihasilkan saat enkripsi<ul style="list-style-type: none">• Jika dokumen laporan TA valid maka sistem menampilkan pop up “Dokumen Valid”• Jika dokumen laporan TA tidak valid maka sistem menampilkan pop up “Dokumen Tidak Valid”
Input	Data Dokumen Laporan Tugas Akhir
Output	Dokumen sertifikat laporan Tugas Akhir

Ketentuan Proses :

1. Dokumen yang akan diverifikasi sudah :
 - o terlebih dahulu dienkripsi oleh sistem
 - o ditanda tangani oleh semua pembimbing, penguji, dan ketua jurusan
2. Mahasiswa dapat mengunduh laporan ketika laporan sudah selesai diverifikasi

IV.3.2.3 Proses Autentikasi

Pada proses ini, KoTA, Dosen maupun Koordinator TA melakukan autentikasi untuk mengidentifikasi akun masing-masing role.



Gambar IV. 17 Bisnis proses autentikasi

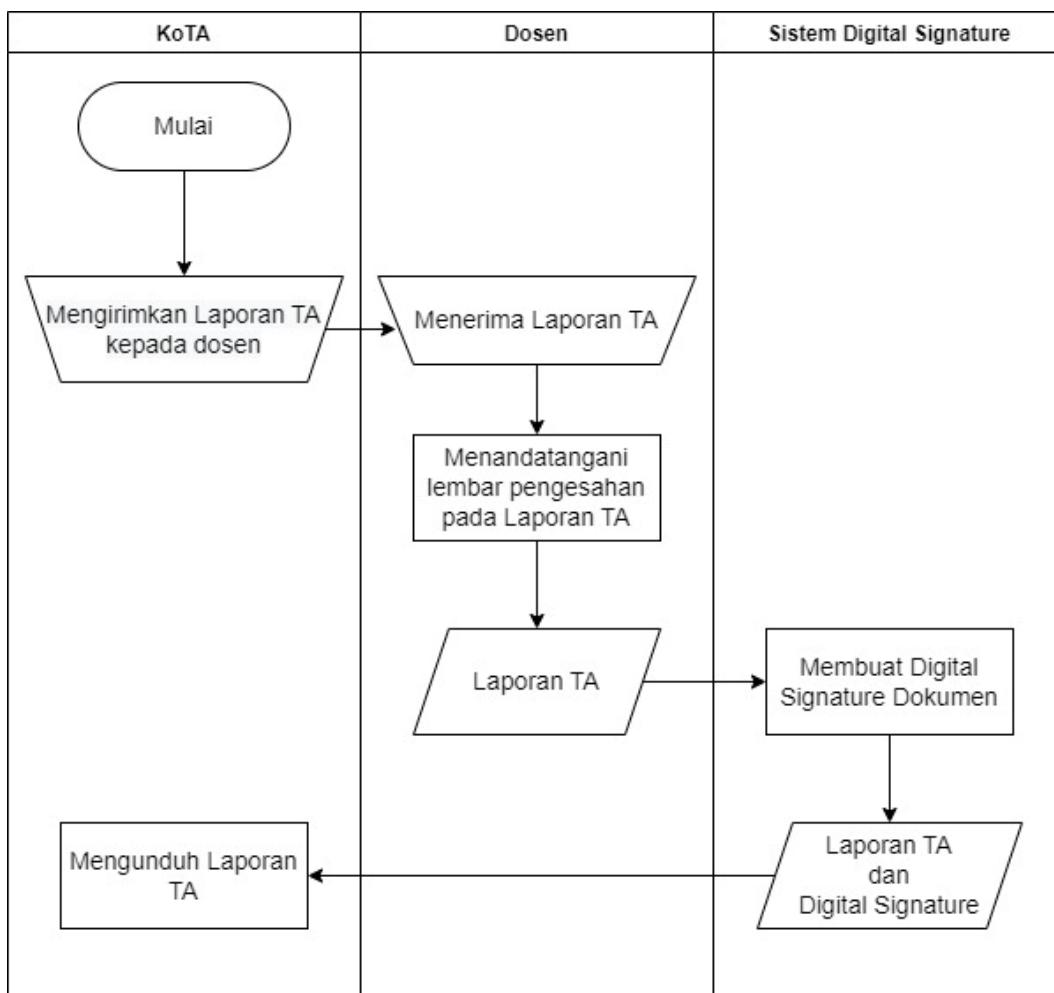
Berikut tabel penjelasan diagram BPMN proses autentikasi:

Tabel IV. 6 Penjelasan diagram proses autentikasi

Nama Proses	Proses Autentikasi
No Proses	BP-003
Business Process	<ol style="list-style-type: none"> 1. Sistem menampilkan user interface 2. User mengisi form login 3. User mengirim form login 4. Sistem memverifikasi akun <ol style="list-style-type: none"> a. Jika akun tidak valid maka sistem akan menampilkan halaman formular login Kembali b. Jika akun valid maka sistem akan menampilkan halaman utama aplikasi
Input	Data User
Output	Halaman dashboard

IV.3.3 Alur Proses yang Diusulkan

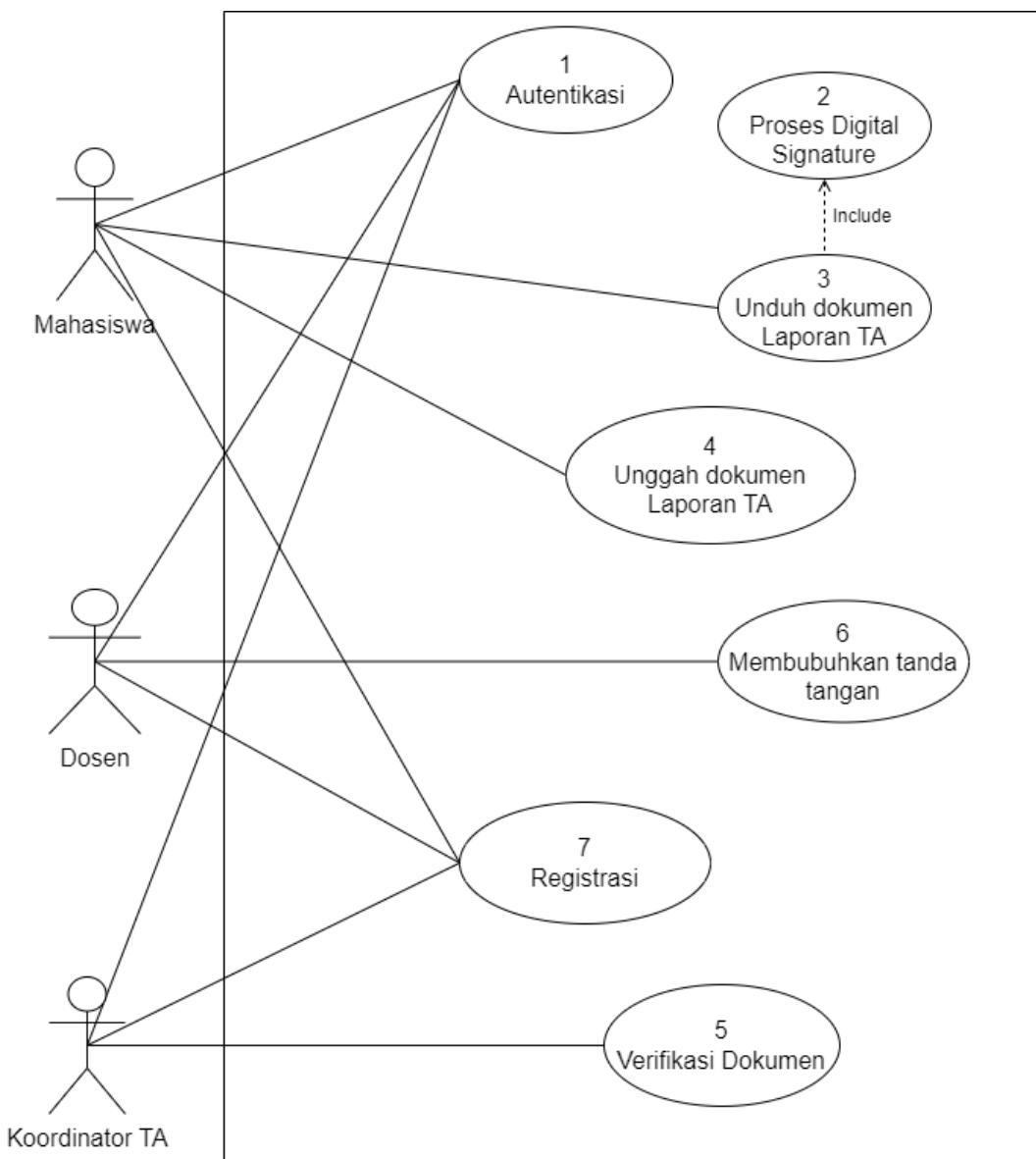
Berikut merupakan alur proses dari pembuatan *digital signature*.



Gambar IV. 18 Alur proses digital signature

IV.4 Analisis Aktor dan Sistem

Berdasarkan evaluasi dan usulan solusi dari analisis sebelumnya, setiap fitur yang telah disebutkan pada sub bab tersebut secara umum akan digambarkan dengan menggunakan use case diagram pada gambar dibawah ini.



Gambar IV. 19 *Use case diagram*

Detail mengenai persyaratan kebutuhan aplikasi yang telah di direpresentasikan ke dalam use case diagram, use case scenario dijelaskan lebih detail pada dokumen SRS.

IV.5 Analisis Kebutuhan Data

Untuk mengembangkan aplikasi, dibutuhkan data-data yang akan disimpan diolah, yaitu:

1. Data Dosen

Data dosen berisi kumpulan data dosen di JTK POLBAN yang diuraikan dalam tabel berikut:

Tabel IV. 7 Data dosen

No	Nama Data
1.	Nama Dosen
2.	NIP
3.	Status pembimbing
4.	Status pengaji

2. Data KoTA

Data KoTA berisi kumpulan data KoTA mahasiswa tingkat akhir di JTK POLBAN yang diuraikan dalam tabel berikut:

Tabel IV. 8 Data KoTA

No	Nama Data
1.	Nama KoTA
2.	Kelas
3.	Nama pembimbing
4.	Nama pengaji
5.	Laporan Tugas Akhir

3. Data Dokumen Laporan Tugas Akhir

Data Dokumen Laporan Tugas Akhir berisi kumpulan data Dokumen Laporan Tugas Akhir yang diuraikan dalam tabel berikut:

Tabel IV. 9 Data dokumen laporan TA

No	Nama Data
1.	Nama Dokumen
2.	Status
3.	Kunci Publik
4.	Kunci Privat

4. Data Koordinator TA

Data koordinator TA berisi kumpulan data koordinator TA yang diuraikan dalam tabel berikut:

Tabel IV. 10 Data koordinator TA

No	Nama Data
1.	Nama Koordinator TA
2.	NIP

IV.6 Analisis Perangkat Lunak

Sebelum dilakukan pengembangan aplikasi, dilakukan eksplorasi untuk menentukan teknologi-teknologi yang tepat dalam pembangunan aplikasi untuk tugas akhir ini. Terdapat eksplorasi mengenai arsitektur aplikasi, framework dan database, yang akan digunakan pada pembangunan aplikasi.

IV.6.1 Arsitektur Aplikasi

Dalam pengembangan aplikasi tanda tangan digital menggunakan konsep *Model, View, Controller* (MVC). Pada konsep ini, arsitektur aplikasi dibuat menjadi tiga lapisan yaitu: (1) *model* menangani data; (2) *view* yang menangani antarmuka pengguna; dan (3) *controller* yang menangani proses dan operasi pada data. Ada beberapa pertimbangan dalam memilih arsitektur aplikasi yang akan digunakan sebagai berikut:

1. Konsep MVC dapat memproses efektivitas pengembangan *website* lebih cepat. Dikarenakan, MVC membagi *website* menjadi tiga bagian yaitu Bagian *model* dan *controller* dapat dikerjakan oleh *backend developer* dan *view* dapat dilakukan oleh *frontend developer* dan UI/UX tim.
2. Proses testing dapat dilakukan setiap bagian yang telah selesai dengan menggunakan kerangka MVC dan menunggu keseluruhan *website* jadi.
3. Kerangka MVC mendukung penggunaan *script* yang lebih terstruktur dan rapi. Hal ini dapat memudahkan tim pengembang dalam proses pengembangan dan perbaikan *website*.

Berdasarkan hasil eksplorasi, maka dalam mengembangkan aplikasi tanda tangan digital ini memutuskan dengan mengimplementasikan arsitektur *model view controller* menggunakan *framework* Codeigniter.

IV.6.2 Framework

IV.6.2.1 Framework Codeigniter

Codeigniter sebagai framework yang akan digunakan dalam implementasi pembuatan aplikasi tanda tangan digital. Ada beberapa pertimbangan dalam memilih Codeigniter diantaranya:

1. Codeigniter mempunyai banyak *library object-oriented* yang tersedia serta dokumentasinya yang lengkap.
2. Komponen CodeIgniter dapat bekerja secara mandiri tanpa bergantung dengan komponen lainnya. Tentunya hal ini sangat memudahkan maintenance atau pemeliharaan *website* nantinya.
3. CodeIgniter mampu berjalan dengan baik pada hampir semua *platform hosting*. CodeIgniter juga mendukung database-database paling umum, termasuk MySQL.

Maka dari itu, untuk mengembangkan aplikasi tanda tangan digital ini akan menggunakan framework Codeigniter sebagai penggeraan bagian *backend* atau sisi server.

IV.6.2.2 Framework Bootstrap

Bootstrap sebagai framework yang akan digunakan dalam implementasi pembuatan aplikasi tanda tangan digital. Ada beberapa pertimbangan dalam memilih Bootstrap diantaranya:

1. Bootstrap memiliki dokumentasi yang cukup lengkap sehingga sangat membantu pengembang dalam mengembangkan bagian *frontend* aplikasi.
2. Desain yang responsif merupakan salah satu keunggulan dari penggunaan Bootstrap. Dimana, saat ini kebutuhan akan aplikasi berbasis web yang dapat diakses di berbagai perangkat menjadi prioritas utama untuk kemudahan dari sisi *user experience* (pengalaman pengguna).

IV.6.3 Database

MariaDB sebagai *database* yang akan digunakan dalam implementasi pembuatan aplikasi tanda tangan digital. Ada beberapa pertimbangan dalam memilih *database* MariaDB diantaranya:

1. MariaDB memiliki kinerja lebih cepat karena menggunakan penyimpanan kolom
2. MariaDB memiliki open source yang disediakan secara gratis dan memiliki lingkungan pengembangan yang besar.
3. Untuk migrasi data, MariaDB ini sudah mendukung berbagai macam koneksi seperti Kafka, Python, Java, dan C. Oleh karena itu untuk impor data langsung jadi lebih efisien

Maka dari itu, untuk mengembangkan aplikasi tanda tangan digital ini akan menggunakan MariaDB sebagai penyimpanan data-data pada sistem.

IV.6.4 Library phpseclib

Dalam implementasi pembuatan aplikasi tanda tangan digital ini digunakan *library* phpseclib untuk menerapkan algoritma RSA dalam pembuatan *digital signature* nya. *Library* phpseclib ini dipilih dikarenakan jika dibandingkan dengan OpenSSL, phpseclib lebih mendukung untuk algoritma RSA itu sendiri.

IV.6.5 Perbandingan RSA dan DSA

RSA dan DSA adalah algoritma yang biasanya terdapat pada proses *digital signature*. Kedua tipe algoritma ini memiliki fungsi utama yang sama yaitu adalah membuat enkripsi pada *digital signature*, tentu keduanya memiliki kekurangan dan kelebihan masing - masing. Diantara kelebihan dan kekurangan antara RSA dan DSA terdapat pada tabel berikut.

Tabel IV. 11 Kelebihan dan Kekurangan RSA & DSA

	RSA	DSA
Kelebihan	Lebih cepat dalam mengenkripsi <i>Digital Signature</i>	Proses penghasilan kunci lebih cepat
	Proses verifikasi <i>Digital Signature</i> lebih cepat	Proses cepat pada pembuatan <i>Digital Signature</i>
Kekurangan	Lambat dalam penghasilan kunci pada proses enkripsi	Lambat saat melakukan proses enkripsi
	Lambat dalam pembuatan <i>Digital Signature</i>	Verifikasi dokumen akan lebih lambat

Kedua perbandingan diatas memiliki faktor tertentu dimana, pada pembuatan *digital signature* pada DSA lebih cepat namun proses enkripsi RSA dibilang lebih unggul. Pada faktor ini DSA merupakan algoritma yang menggunakan fungsi tunggal sehingga lebih berfokus pada pembuatan *digital signature* dan kunci. Kesimpulannya adalah apabila berfokus hanya pada pembuatan *digital signature* atau kunci DSA lebih baik. Namun apabila fokus utama pada enkripsi dokumen dan validasi lebih baik menggunakan algoritma RSA.

IV.6.6 Perbandingan RSA dan Diffie-Helman

RSA dan Diffie-Helman adalah algoritma yang biasanya terdapat pada proses *digital signature*. Kedua tipe algoritma ini memiliki fungsi utama yang sama yaitu adalah membuat enkripsi pada *digital signature*, tentu keduanya memiliki kekurangan dan kelebihan masing - masing. Diantara kelebihan dan kekurangan antara RSA dan Diffie-Helman terdapat pada tabel berikut.

Tabel IV. 12 Perbandingan RSA dan Diffie-Helman

Aspek	RSA	Diffie-Helman
-------	-----	---------------

Pertukaran Kunci	Hanya penerima pesan yang memiliki kunci privat si pengirim pesan	Pengirim dan penerima saling bertukar kunci privatnya masing-masing
Kompleksitas	Rendah	Tinggi
Keamanan	Bilangan prima yang besar sehingga sulit untuk difaktorkan	Menjaga kunci privat dari pihak masing-masing

BAB V

PERANCANGAN

Pada bab ini akan dijelaskan mengenai perancangan dari aplikasi tanda tangan digital yang akan dibangun. Perancangan yang dijelaskan mencakup perancangan interaksi antar objek, user interface, dan perancangan database.

V.1 Perancangan Interaksi Antar Objek

Perancangan interaksi antar objek menggambarkan proses interaksi antar objek pada aplikasi yang akan dibangun. Perancangan ini mengacu kepada spesifikasi kebutuhan, *use case*, *user scenario*, dan *system sequence diagram* yang telah dijelaskan lebih detail pada dokumen SRS. Tujuan dari perancangan ini untuk menggambarkan komunikasi yang terjadi antar objek pada aplikasi digital signature.

1. Use Case UC1: Autentikasi

Autentikasi Mahasiswa

Tabel V. 1 Use case scenario autentikasi mahasiswa

Scope	Aplikasi Tanda Tangan Digital
Level	User Goal
Primary Actor	Mahasiswa
Stakeholder and Interests	Dapat terautentikasi sesuai akun
Preconditions	<ul style="list-style-type: none">- Aplikasi dapat mengakses database- Mahasiswa sudah memiliki akun yang tersimpan di database
Success Guarantee (Postconditions)	<ul style="list-style-type: none">- Mahasiswa berhasil terautentikasi sesuai akun yang tersimpan di database dan aplikasi menampilkan halaman awal aplikasi sesuai role.
Main Success Scenario	
Actor Action (Intention)	System Responsibility
1. Mahasiswa melakukan autentikasi	
	2. Aplikasi menampilkan form login
3. Mahasiswa mengisi NIM dan password	

	4. Aplikasi membaca data user berdasarkan NIM dari database
	5. Aplikasi memeriksa kesamaan password data user dan password yang diisi mahasiswa
	6. Aplikasi menyimpan data user pada session
	7. Aplikasi menampilkan halaman awal aplikasi role mahasiswa
Extensions (Alternative Flows)	
4. a. Data user tidak ditemukan.	
1. Aplikasi menampilkan notifikasi akun tidak terdaftar.	
5. a. Password data user dan password yang diisi mahasiswa tidak sama.	
1. Aplikasi menampilkan notifikasi password tidak sesuai.	
Special Requirements	
Technology and data Variations List	
Frequency of Occurrence	
Miscellaneous	

Autentikasi Dosen

Tabel V. 2 Use case scenario autentikasi dosen

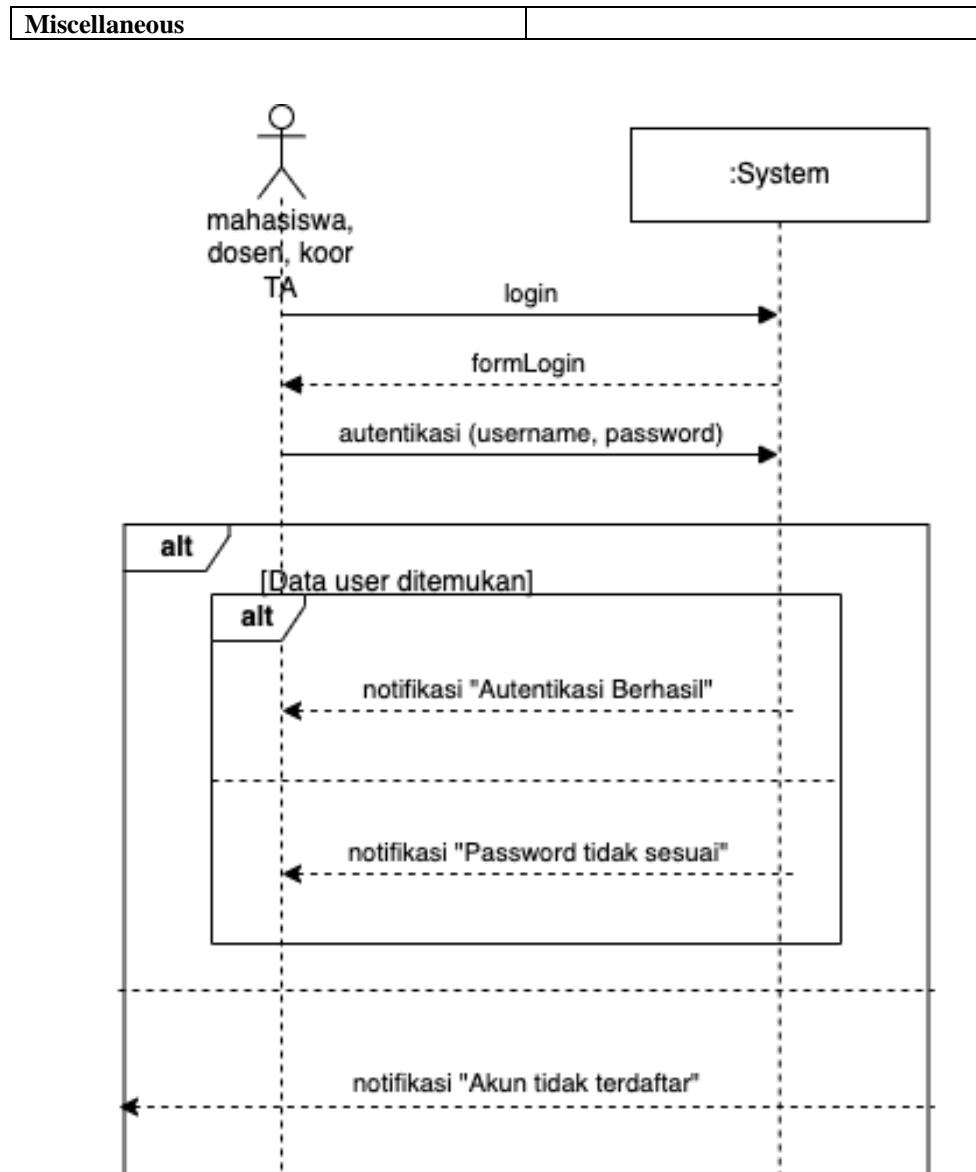
Scope	Aplikasi Tanda Tangan Digital
Level	User Goal
Primary Actor	Dosen
Stakeholder and Interests	Dapat terautentikasi sesuai akun
Preconditions	<ul style="list-style-type: none"> - Aplikasi dapat mengakses database - Dosen sudah memiliki akun yang tersimpan di database
Success Guarantee (Postconditions)	<ul style="list-style-type: none"> - Dosen berhasil terautentikasi sesuai akun yang tersimpan di database dan aplikasi menampilkan halaman awal aplikasi sesuai role.
Main Success Scenario	
Actor Action (Intention)	System Responsibility
1. Dosen melakukan autentikasi	
	<ul style="list-style-type: none"> 2. Aplikasi menampilkan form login
3. Dosen mengisi NIP dan password	
	<ul style="list-style-type: none"> 4. Aplikasi membaca data user berdasarkan NIP dari database
	<ul style="list-style-type: none"> 5. Aplikasi memeriksa kesamaan password data user dan password yang diisi dosen
	<ul style="list-style-type: none"> 6. Aplikasi menyimpan data user pada session
	<ul style="list-style-type: none"> 7. Aplikasi menampilkan halaman awal aplikasi role dosen
Extensions (Alternative Flows)	
4. a. Data user tidak ditemukan.	

1. Aplikasi menampilkan notifikasi akun tidak terdaftar. 5. a. Password data user dan password yang diisi mahasiswa tidak sama. 1. Aplikasi menampilkan notifikasi password tidak sesuai.
Special Requirements
Technology and data Variations List
Frequency of Occurrence
Miscellaneous

Autentikasi Koordinator TA

Tabel V. 3 Use case scenario autentikasi koordinator TA

Scope	Aplikasi Tanda Tangan Digital
Level	User Goal
Primary Actor	Koordinator TA
Stakeholder and Interests	Dapat terautentikasi sesuai akun
Preconditions	<ul style="list-style-type: none"> - Aplikasi dapat mengakses database - Koordinator TA sudah memiliki akun yang tersimpan di database
Success Guarantee (Postconditions)	<ul style="list-style-type: none"> - Koordinator TA berhasil terautentikasi sesuai akun yang tersimpan di database dan aplikasi menampilkan halaman awal aplikasi sesuai role.
Main Success Scenario	
Actor Action (Intention)	System Responsibility
1. Koordinator TA melakukan autentikasi	
	2. Aplikasi menampilkan form login
3. Koordinator TA mengisi username dan password	
	4. Aplikasi membaca data user berdasarkan username dari database
	5. Aplikasi memeriksa kesamaan password data user dan password yang diisi koordinator TA
	6. Aplikasi menyimpan data user pada session
	7. Aplikasi menampilkan halaman awal aplikasi role koordinator TA
Extensions (Alternative Flows)	
4. a. Data user tidak ditemukan.	
1. Aplikasi menampilkan notifikasi akun tidak terdaftar.	
5. a. Password data user dan password yang diisi koordinator TA tidak sama.	
1. Aplikasi menampilkan notifikasi password tidak sesuai.	
Special Requirements	
Technology and data Variations List	
Frequency of Occurrence	



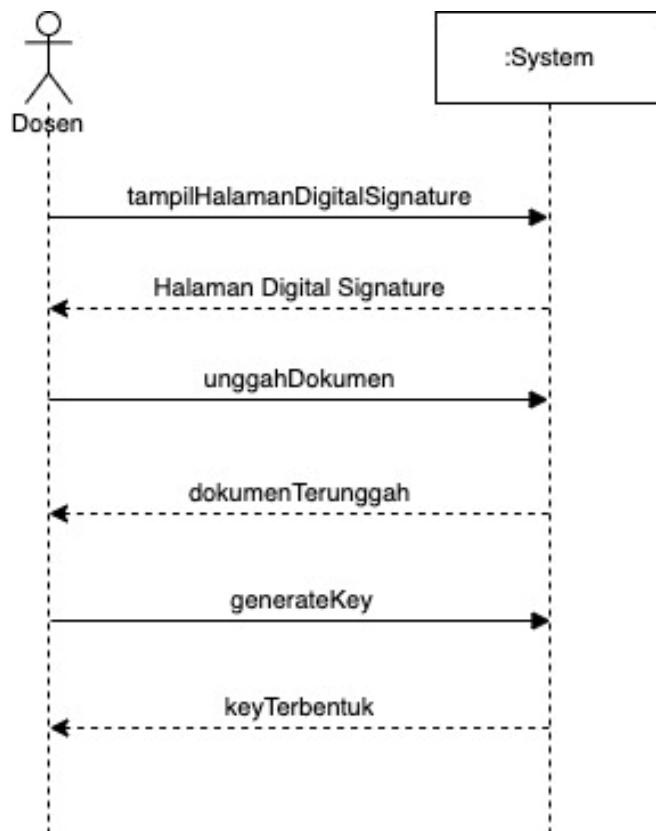
Gambar V. 1 System sequence diagram autentikasi

2. Use Case UC2: Proses Digital Signature

Tabel V. 4 Use case scenario proses digital signature

Scope	Aplikasi Tanda Tangan Digital
Level	User Goal
Primary Actor	Dosen
Stakeholder and Interests	Dapat menyisipkan digital signature pada dokumen Laporan TA
Preconditions	- Aplikasi dapat mengakses database

	- Dokumen laporan TA sudah dibubuhkan tanda tangan coretan
Success Guarantee (Postconditions)	- Berhasil menyisipkan digital signature pada dokumen laporan TA
Main Success Scenario	
Actor Action (Intention)	System Responsibility
1. Dosen memuat halaman digital signature	
	2. Aplikasi menampilkan halaman digital signature
3. Dosen mengunggah dokumen Laporan TA	
	4. Aplikasi menyimpan dokumen ke database yang diunggah dosen
5. Dosen melakukan <i>generate key</i> pada dokumen yang sudah diunggah	
	6. Aplikasi membentuk key
Extensions (Alternative Flows)	
Special Requirements	
Technology and data Variations List	
Frequency of Occurrence	
Miscellaneous	



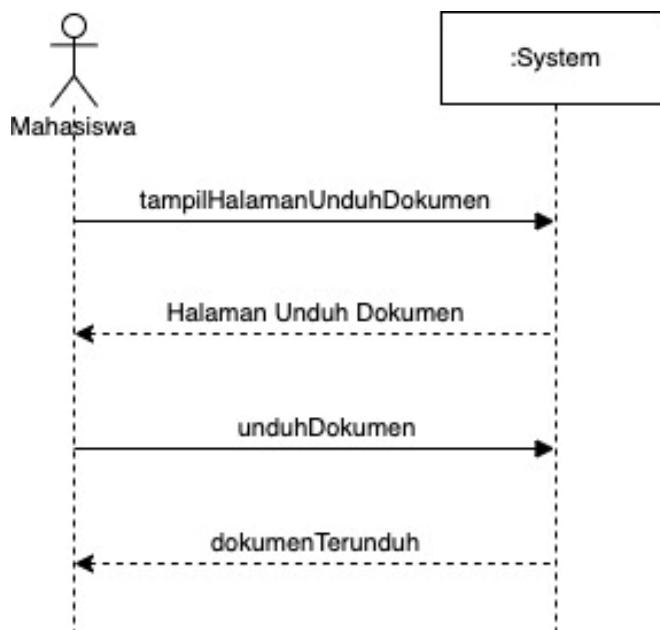
Gambar V. 2 System sequence diagram proses digital signature

3. Use Case UC3: Unduh Dokumen Laporan TA

Tabel V. 5 Use case scenario unduh dokumen

Scope	Aplikasi Tanda Tangan Digital
Level	User Goal
Primary Actor	Mahasiswa
Stakeholder and Interests	Dapat mengunduh dokumen Laporan TA yang sudah ditandatangani.
Preconditions	<ul style="list-style-type: none"> - Aplikasi dapat mengakses database - Dokumen yang akan diunduh sudah dienkripsi
Success Guarantee (Postconditions)	<ul style="list-style-type: none"> - Berhasil mengunduh dokumen Laporan TA yang sudah disisipkan digital signature
Main Success Scenario	
Actor Action (Intention) System Responsibility	
1. Mahasiswa memuat halaman unduh dokumen Laporan TA	
	2. Aplikasi menampilkan halaman unduh dokumen Laporan TA

3. Mahasiswa mengunduh dokumen laporan TA yang tersedia.	
	4. Aplikasi mengunduh dokumen dari database
Extensions (Alternative Flows)	
Special Requirements	
Technology and data Variations List	
Frequency of Occurrence	
Miscellaneous	



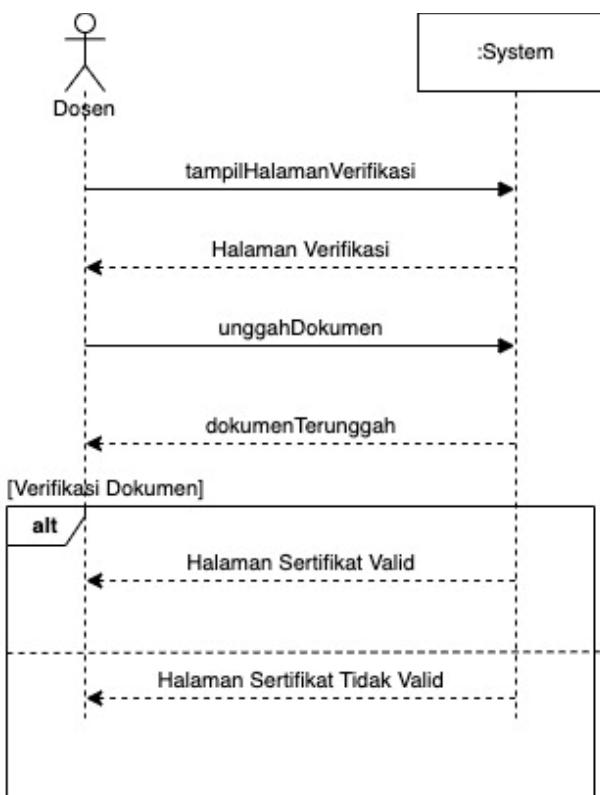
Gambar V. 3 System sequence diagram unduh dokumen

4. Use Case UC4: Verifikasi Dokumen

Tabel V. 6 Use case scenario verifikasi dokumen

Scope	Aplikasi Tanda Tangan Digital
Level	User Goal
Primary Actor	Dosen
Stakeholder and Interests	Dapat melakukan verifikasi dokumen Laporan TA yang sudah ditandatangan.
Preconditions	- Aplikasi dapat mengakses database
Success Guarantee (Postconditions)	- Berhasil melakukan verifikasi dokumen Laporan TA yang sudah ditandatangan
Main Success Scenario	
Actor Action (Intention)	System Responsibility

1. Dosen memuat halaman verifikasi dokumen Laporan TA.	
	2. Aplikasi menampilkan halaman verifikasi dokumen Laporan TA
3. Dosen mengunggah dokumen Laporan TA yang sudah disisipkan digital signature	
	4. Aplikasi menyimpan dokumen ke database yang diunggah dosen
	5. Aplikasi menampilkan halaman sertifikat valid
Extensions (Alternative Flows)	
5. a. Aplikasi tidak menampilkan halaman sertifikat valid	
1. Dokumen tidak valid	
Special Requirements	
Technology and data Variations List	
Frequency of Occurrence	
Miscellaneous	

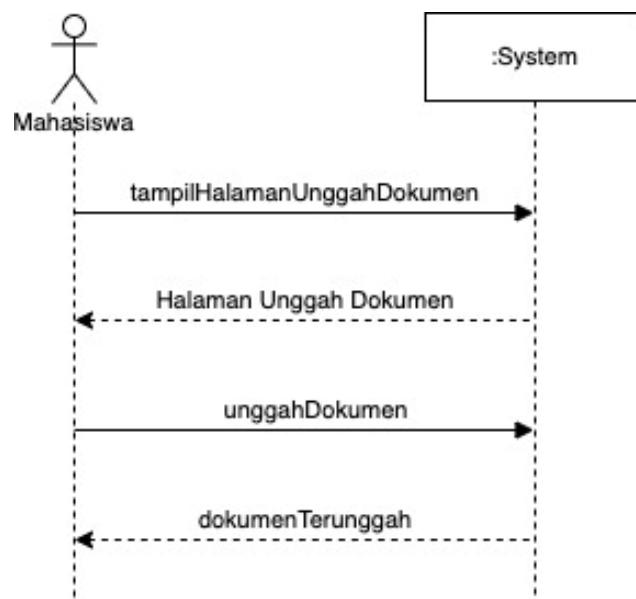


Gambar V. 4 System sequence diagram verifikasi dokumen

5. Use Case UC5: Unggah dokumen Laporan TA

Tabel V. 7 Use case scenario unggah dokumen

Scope	Aplikasi Tanda Tangan Digital
Level	User Goal
Primary Actor	Dosen
Stakeholder and Interests	Dapat mengunggah dokumen Laporan TA yang sudah ditandatangan.
Preconditions	<ul style="list-style-type: none"> - Aplikasi dapat mengakses database - Dokumen laporan TA sudah disisipkan digital signature
Success Guarantee (Postconditions)	<ul style="list-style-type: none"> - Berhasil mengunggah dokumen Laporan TA
Main Success Scenario	
Actor Action (Intention)	System Responsibility
1. Dosen memuat halaman unduh dokumen Laporan TA	
	2. Aplikasi menampilkan halaman unggah dokumen Laporan TA
3. Dosen mengunggah dokumen Laporan TA yang sudah disisipkan digital signature	
	4. Aplikasi menyimpan dokumen ke database yang diunggah dosen
Extensions (Alternative Flows)	
Special Requirements	
Technology and data Variations List	
Frequency of Occurrence	
Miscellaneous	

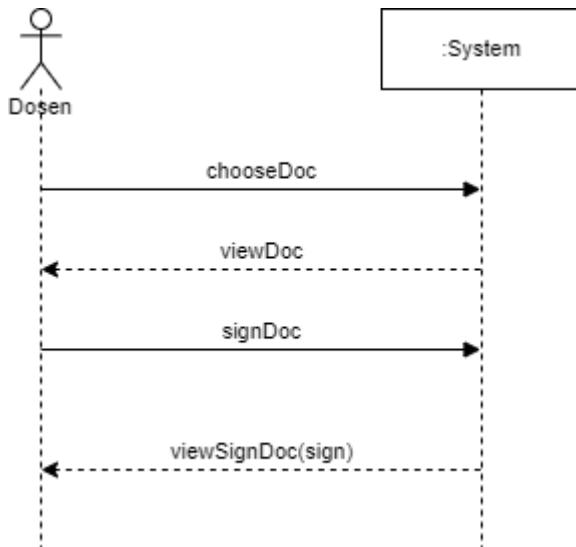


Gambar V. 5 System sequence diagram unggah dokumen

6. Use Case UC6: Membubuhkan Tanda Tangan

Tabel V. 8 Use case scenario bubuhkan tanda tangan

Scope	Aplikasi Tanda Tangan Digital
Level	User Goal
Primary Actor	Dosen
Stakeholder and Interests	Dapat membubuhkan tanda tangan pada dokumen
Preconditions	<ul style="list-style-type: none"> - User berada di halaman tampilan dokumen yang akan ditandatangani
Success Guarantee (Postconditions)	<ul style="list-style-type: none"> - Citra tanda tangan tertempel pada dokumen
Main Success Scenario	
Actor Action (Intention)	System Responsibility
1. Dosen menekan tombol tanda tangan	<ol style="list-style-type: none"> 2. Aplikasi membubuhkan tanda tangan pada dokumen 3. Aplikasi menyimpan dokumen yang sudah ditanda tangan ke database
Extensions (Alternative Flows)	
3. a. Gagal menyimpan ke database	
1. Aplikasi menampilkan pesan error	
Special Requirements	
Technology and data Variations List	
Frequency of Occurrence	
Miscellaneous	

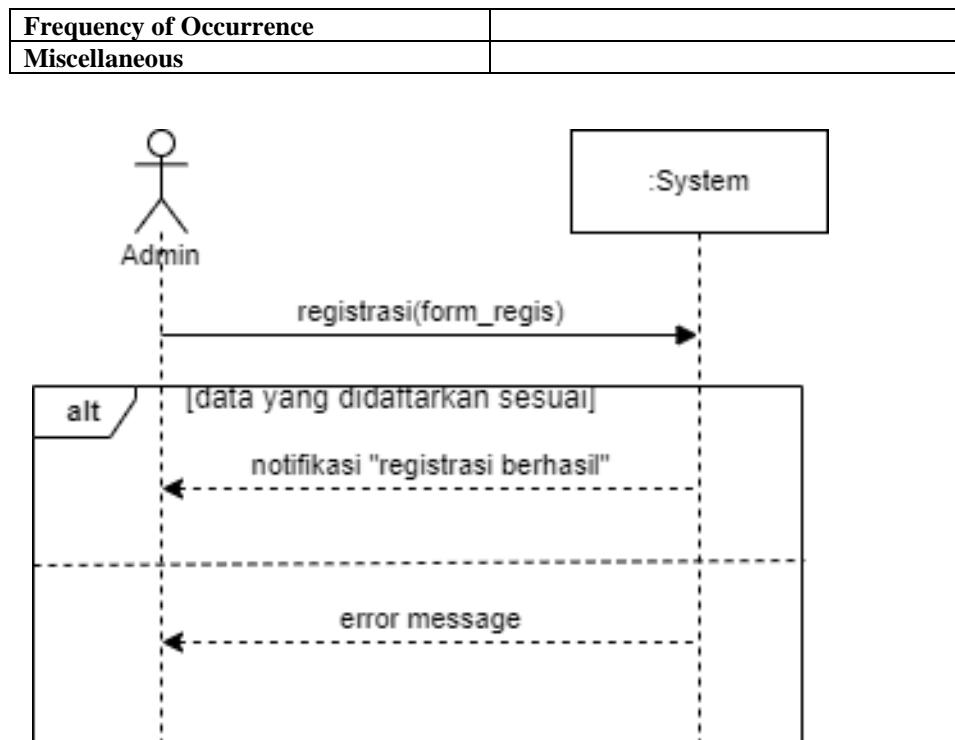


Gambar V. 6 System sequence diagram membubuhkan tanda tangan

7. Use Case UC7: Registrasi

Tabel V. 9 Use case scenario registrasi

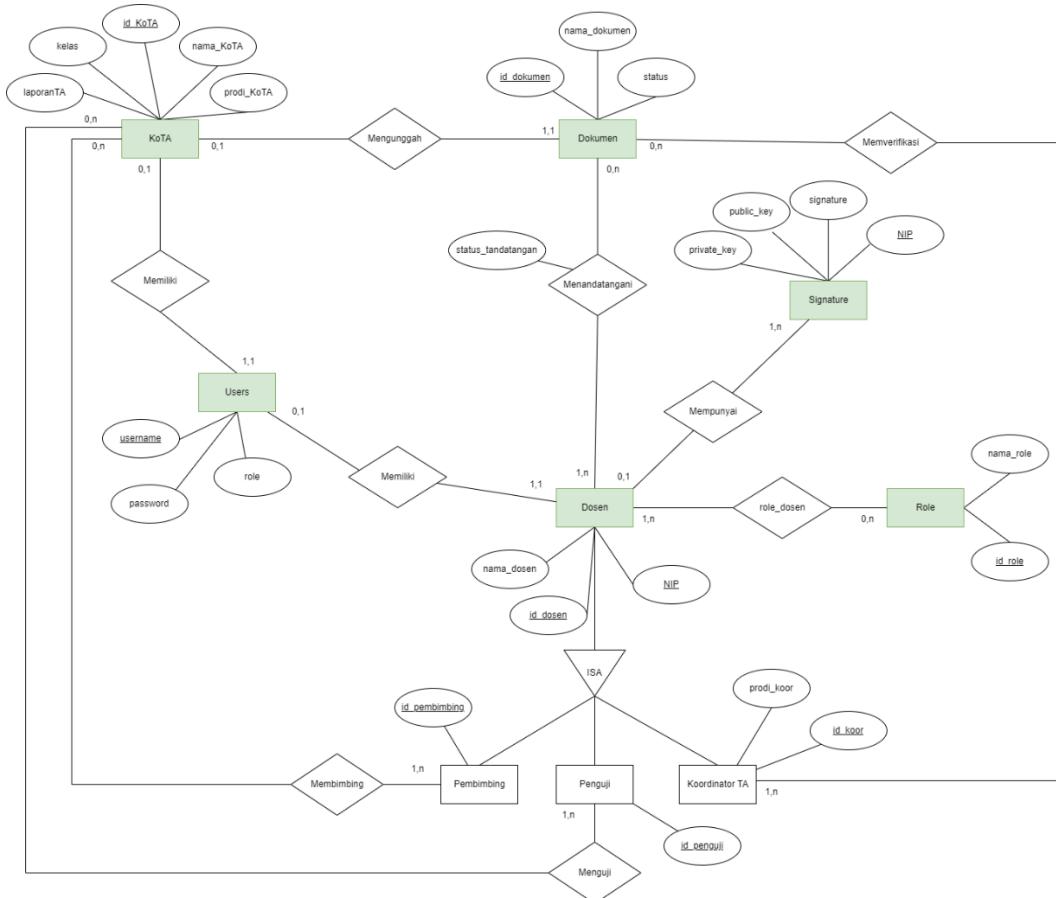
Scope	Aplikasi Tanda Tangan Digital
Level	User Goal
Primary Actor	Koordinator TA
Stakeholder and Interests	Dapat melakukan registrasi akun
Preconditions	<ul style="list-style-type: none"> - Admin belum terdaftar di dalam aplikasi, data belum terdaftar di database
Success Guarantee (Postconditions)	<ul style="list-style-type: none"> - Akun admin telah ditambahkan dalam database.
Main Success Scenario	
Actor Action (Intention)	System Responsibility
1. Admin mengakses halaman registrasi	
	2. Aplikasi menampilkan halaman registrasi
3. Admin mengisi formulir yang ditampilkan	
	4. Sistem melakukan pengecekan kesesuaian data input admin.
	5. Jika sudah sesuai, aplikasi akan menyimpan data admin ke database
Extensions (Alternative Flows)	
4. a. Tidak sesuai dengan ketentuan	
1. Aplikasi menampilkan pesan gagal registrasi.	
Special Requirements	
Technology and data Variations List	



Gambar V. 7 System sequence diagram registrasi

V.2 Perancangan Database

Perancangan database dilakukan untuk mengilustrasikan database yang ada pada aplikasi tanda tangan digital agar sesuai dengan kebutuhan pengguna. Gambar berikut merupakan perancangan database untuk aplikasi tanda tangan digital yang berupa Entity Relationship Diagram.



Gambar V. 8 Entity relationship diagram

Tabel berikut adalah penjelasan detail mengenai gambar ERD diatas.

Tabel V. 10 Penjelasan ERD

	Attribute	Type	Access	Frequency
Entity-set: KoTA	laporanTA	String	Public	Ketika pengelolaan data KoTA
	kelas	String	Public	
	id_KoTA	Integer	Public	
	nama_KoTA	String	Public	
	prodi_KoTA	String	Public	
Entity-set: Dokumen	id_dokumen	Integer	Public	Ketika pengelolaan data Dokumen
	nama_dokumen	String	Public	
	status	Boolean	Public	
Relationship: mengunggah				Ketika mengalokasikan data KoTA dengan data Dokumen
Entity-set: Koordinator TA	role_koor	Integer	Public	Ketika pengelolaan data Koordinator TA

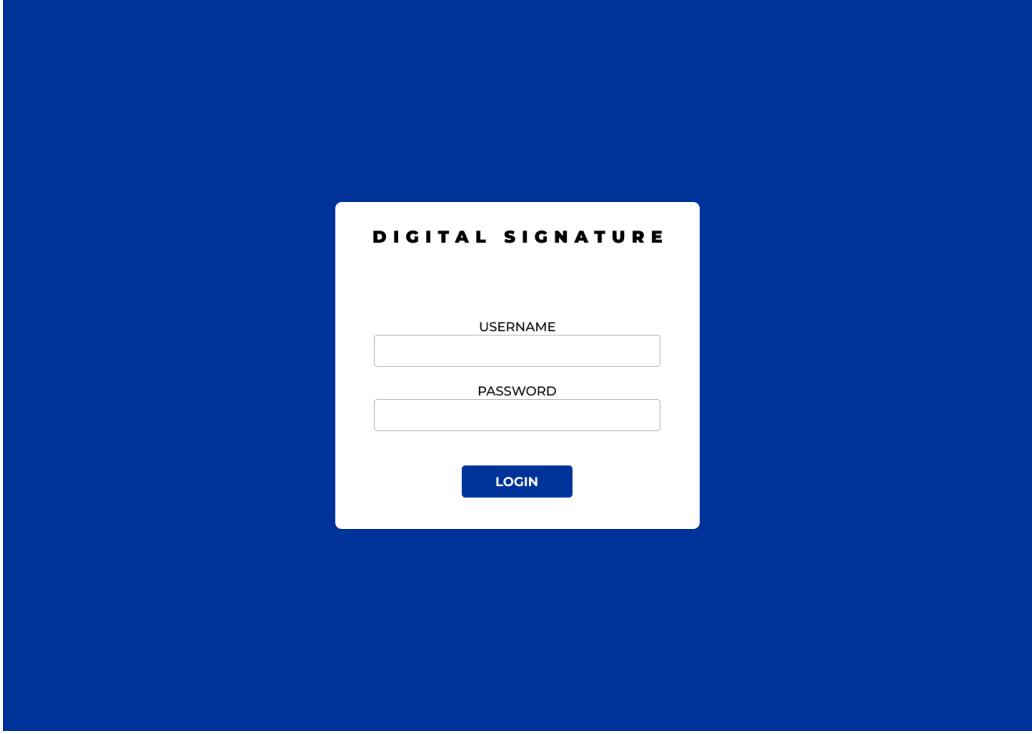
Relationship: memvalidasi				Ketika mengalokasikan data Dokumen dengan data Koordinator TA
Entity-set: Prodi	kode_prodi	Integer	Public	Ketika pengelolaan data Prodi
	nama_prodi	String	Public	
Relationship: memiliki				Ketika mengalokasikan data Prodi dengan data KoTA
Entity-set: Dosen	nama_dosen	String	Public	Ketika pengelolaan data Dosen
	kode_dosen	Integer	Public	
	NIP	String	Public	
	password_dosen	String	Public	
Relationship: menandatangani				Ketika mengalokasikan data Dokumen dengan data Dosen
Entity-set: Pembimbing	role_pembimbing	Integer	Public	
Entity-set: Penguji	role_penguji	Integer	Public	
Relationship: Menjadi				Ketika mengalokasikan data Dosen dengan data Pembimbing, Penguji dan Koordinator TA
Relationship: Menguji				Ketika mengalokasikan data KoTA dengan data Penguji
Relationship: Membimbing				Ketika mengalokasikan data KoTA dengan data Pembimbing

V.3 Perancangan User Interfaces

Pada bab ini dijelaskan tampilan tampilan antarmuka yang akan dibangun pada pengembangan aplikasi. Gambar berikut merupakan gambar tampilan antarmuka untuk aplikasi digital signature.

Tabel V. 11 User interface login

Kode UI/ Nama UI	UI-001/Halaman Login
Aktor	Dosen, Mahasiswa dan Koordinator TA

Gambar	
	
<p>Gambar V. 9 User interface login</p>	

Deskripsi	Halaman login ini digunakan oleh dosen, mahasiswa dan koordinator TA. Pada halaman ini terdapat <i>button login</i> yang digunakan ketika pengguna selesai menginputkan <i>username</i> dan <i>password</i>
------------------	---

Tabel V. 12 User interface Halaman dashboard

Kode UI/ Nama UI	UI-003/Halaman Dashboard Admin
Aktor	Admin
Gambar	

The screenshot shows a user interface for a digital signature application. On the left, there is a vertical sidebar with a dark blue background and white text. The text "DIGITAL SIGNATURE" is at the top, followed by a horizontal line, then "Tambah Pengguna" in the middle, and another horizontal line at the bottom. To the right of this sidebar, the main area has a white background. At the top center, the word "DASHBOARD" is written in a small, bold, black font. Below it is a simple line-art icon of a person's head and shoulders. Underneath the icon, the text "ADMIN 1" is displayed in a bold, black, sans-serif font.

Gambar V. 10 User interface Halaman dashboard

Deskripsi	Halaman dashboard ini menampilkan profil admin dan juga menu untuk menambahkan pengguna
-----------	---

Tabel V. 13 User interface form tambah data dosen

Kode UI/ Nama UI	UI-004/Halaman Tambah Pengguna Dosen
Aktor	Admin
Gambar	

The image shows a user interface for adding a teacher (Dosen) user. On the left, there is a vertical sidebar with a dark blue background labeled "DIGITAL SIGNATURE" at the top. Below it, the text "Tambah Pengguna" is visible. The main content area has a white background and is titled "Tambah Pengguna Dosen". It contains a form with the following fields:

- Sebagai :** A dropdown menu set to "Pembimbing 1".
- Username**: An input field.
- Password**: An input field.
- Email**: An input field.
- Add**: A green rectangular button at the bottom right.

Gambar V. 11 User interface form tambah data dosen

Deskripsi	Halaman ini menampilkan form tambah data dosen. Terdapat <i>button add</i> yang digunakan untuk menyimpan data dosen yang telah diinputkan.
------------------	---

Tabel V. 14 User interface form tambah data mahasiswa

Kode UI/ Nama UI	UI-005/Halaman Tambah Pengguna Mahasiswa
Aktor	Admin
Gambar	

Gambar V. 12 User interface form tambah data mahasiswa

Deskripsi	Halaman ini menampilkan form tambah data mahasiswa. Terdapat <i>button add</i> yang digunakan untuk menyimpan data mahasiswa yang telah diinputkan.
------------------	---

Tabel V. 15 User interface form unggah dokumen

Kode UI/ Nama UI	UI-006/Halaman Unggah Dokumen
Aktor	Mahasiswa
Gambar	

DIGITAL SIGNATURE

Upload Dokumen

Verifikasi Digital Signatuare

1 Upload Laporan → 2 Detail Laporan

Upload File

Browse
No file selected

Upload

Gambar V. 13 User interface form unggah dokumen

Deskripsi	Halaman ini menampilkan form untuk mengunggah dokumen yang akan diberi signature. Halaman ini hanya dapat digunakan oleh mahasiswa.
------------------	---

Tabel V. 16 User interface form unggah dokumen

Kode UI/ Nama UI	UI-006/Halaman Detail Dokumen
Aktor	Mahasiswa
Gambar	

DIGITAL SIGNATURE

Digital Signature

Verifikasi Digital Signatuare

1 Upload Laporan —→ 2 Pihak Penerima

Penerima

- * Pembimbing 1
- * Pembimbing 2
- Pembimbing 3
- * Pengaji 1
- * Pengaji 2
- * Pengaji 3
- Pengaji 4

Gambar V. 14 User interface form unggah dokumen

Deskripsi	Halaman ini menampilkan form untuk mengunggah dokumen yang akan diberi signature. Halaman ini hanya dapat digunakan oleh mahasiswa.
------------------	---

Tabel V. 17 User interface verifikasi dokumen

Kode UI/ Nama UI	UI-007/Halaman Verifikasi Dokumen
Aktor	Dosen
Gambar	



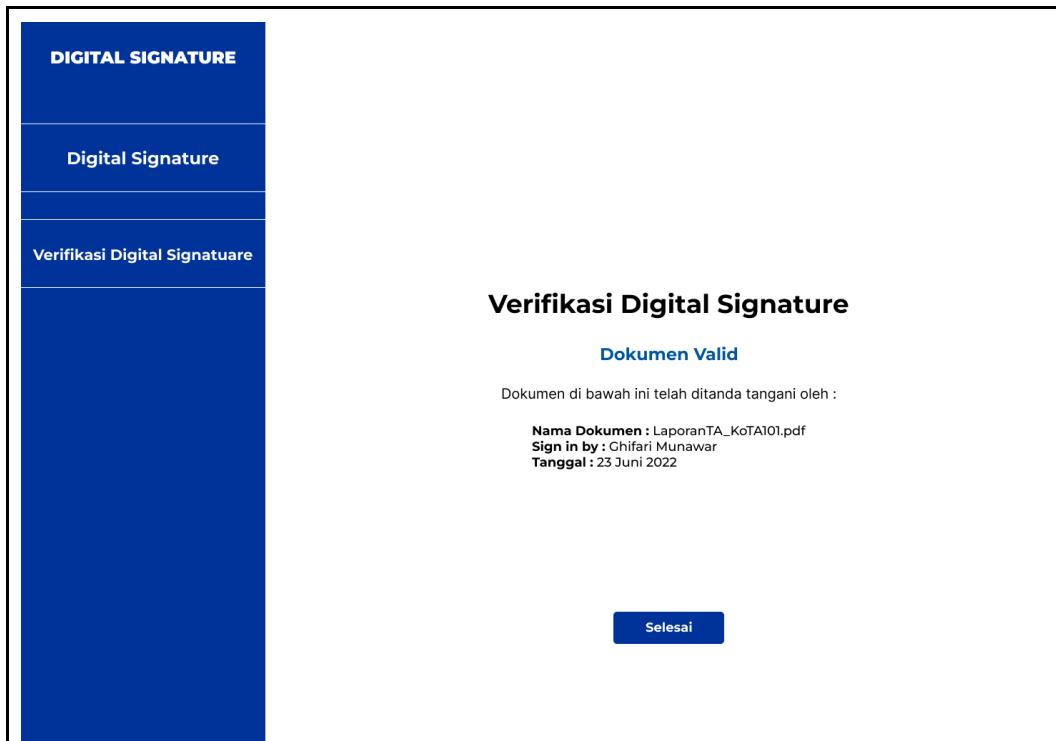
The image shows a user interface for digital signature verification. On the left, there is a vertical sidebar with a dark blue background and white text. It contains the title "DIGITAL SIGNATURE" at the top, followed by "Digital Signature" and "Verifikasi Digital Signatuare". The main area has a light blue background and features a central title "Upload File Digital Signature". Below this title is a "Browse" button with the placeholder text "No file selected". At the bottom right of the main area is a blue "Upload" button.

Gambar V. 15 User interface verifikasi dokumen

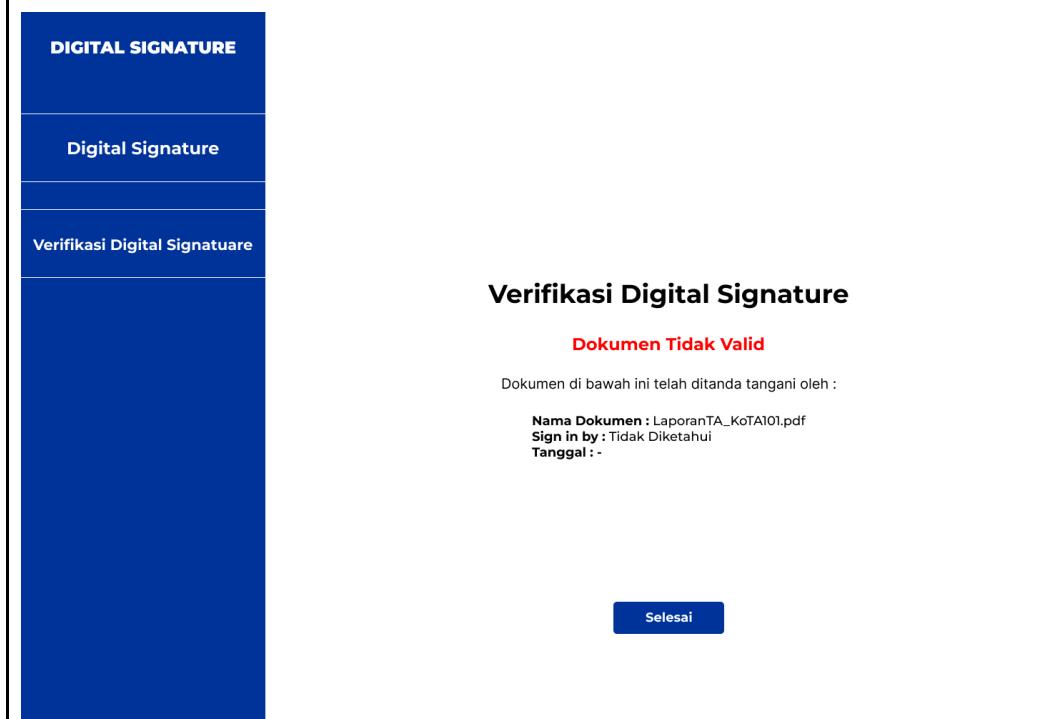
Deskripsi	Halaman ini menampilkan form untuk mengunggah dokumen digital signature yang akan diverifikasi. Halaman ini hanya dapat digunakan oleh dosen.
------------------	---

Tabel V. 18 User interface hasil verifikasi dokumen

Kode UI/ Nama UI	UI-008/Halaman Hasil Verifikasi Dokumen
Aktor	Dosen
Gambar	



Gambar V. 16 User interface hasil verifikasi dokumen (valid)

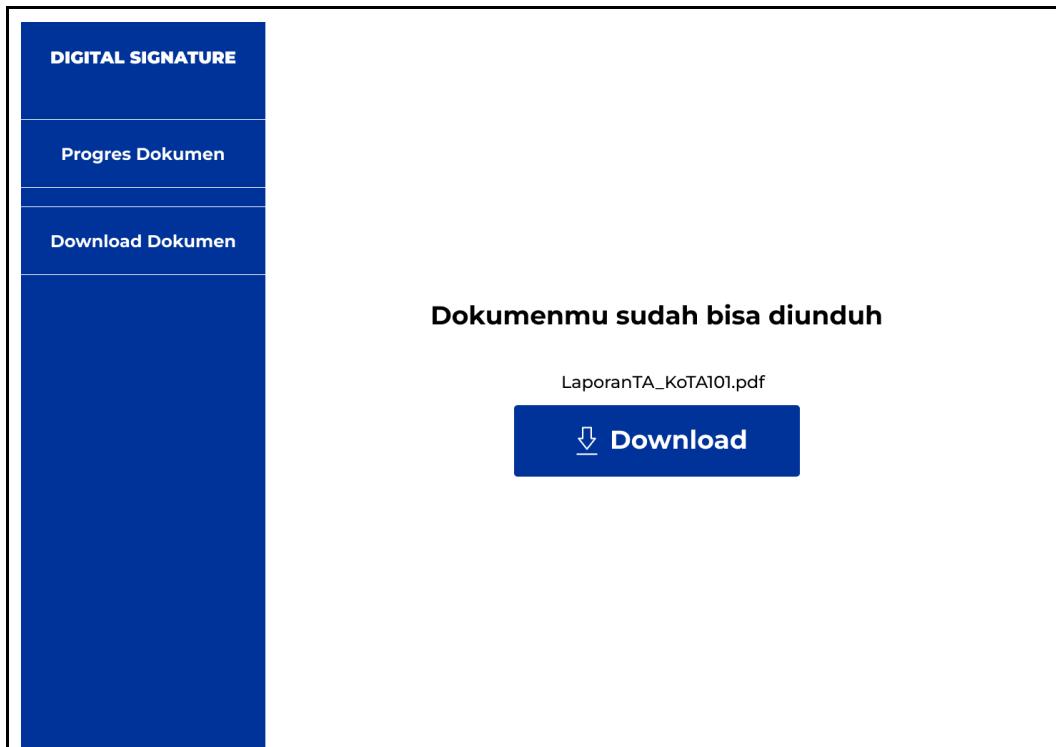


Gambar V. 17 User interface hasil verifikasi dokumen (tidak valid)

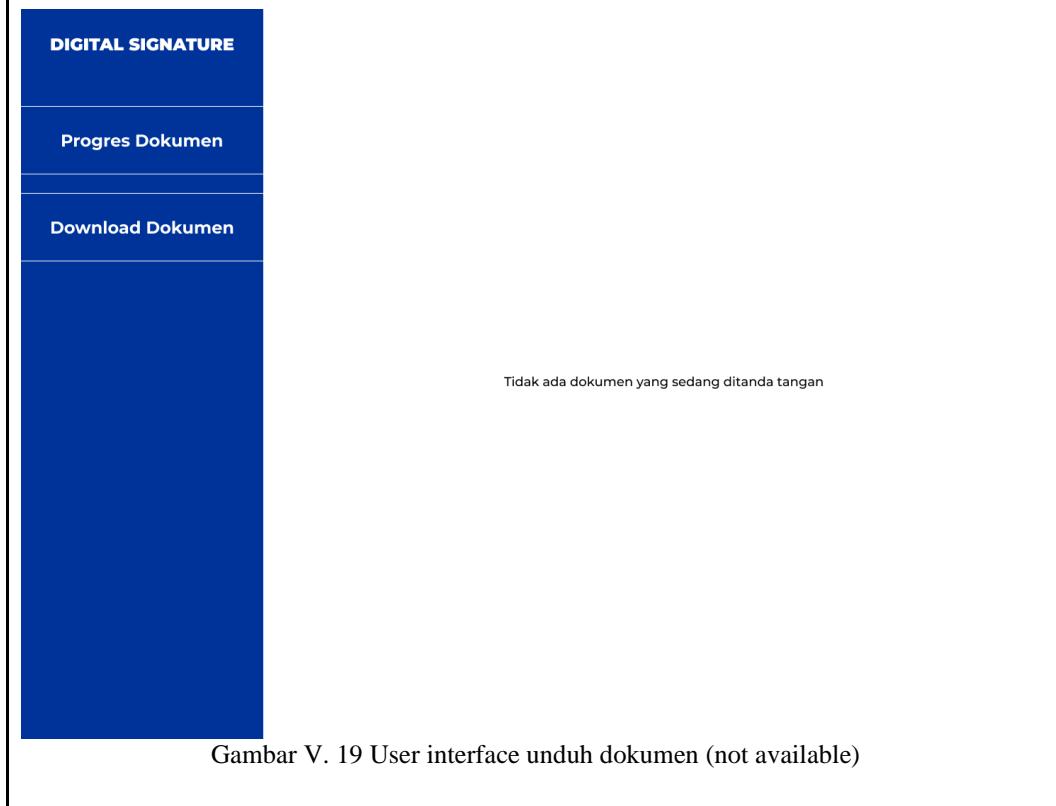
Deskripsi	Halaman ini menampilkan hasil verifikasi keaslian dokumen
------------------	---

Tabel V. 19 User interface unduh dokumen

Kode UI/ Nama UI	UI-009/Halaman Unduh Dokumen
Aktor	Mahasiswa
Gambar	



Gambar V. 18 User interface unduh dokumen (available)



Gambar V. 19 User interface unduh dokumen (not available)

Deskripsi	Halaman ini menampilkan form untuk mengunduh dokumen yang sudah terdapat <i>digital signature</i>
------------------	---

Tabel V. 20 User interface registrasi

Kode UI/ Nama UI	UI-010/Halaman Registrasi Admin
Aktor	Admin
Gambar	
Deskripsi	Halaman ini menampilkan form untuk mendaftarkan data admin baru. Field username diisi oleh NIP dari admin baru.

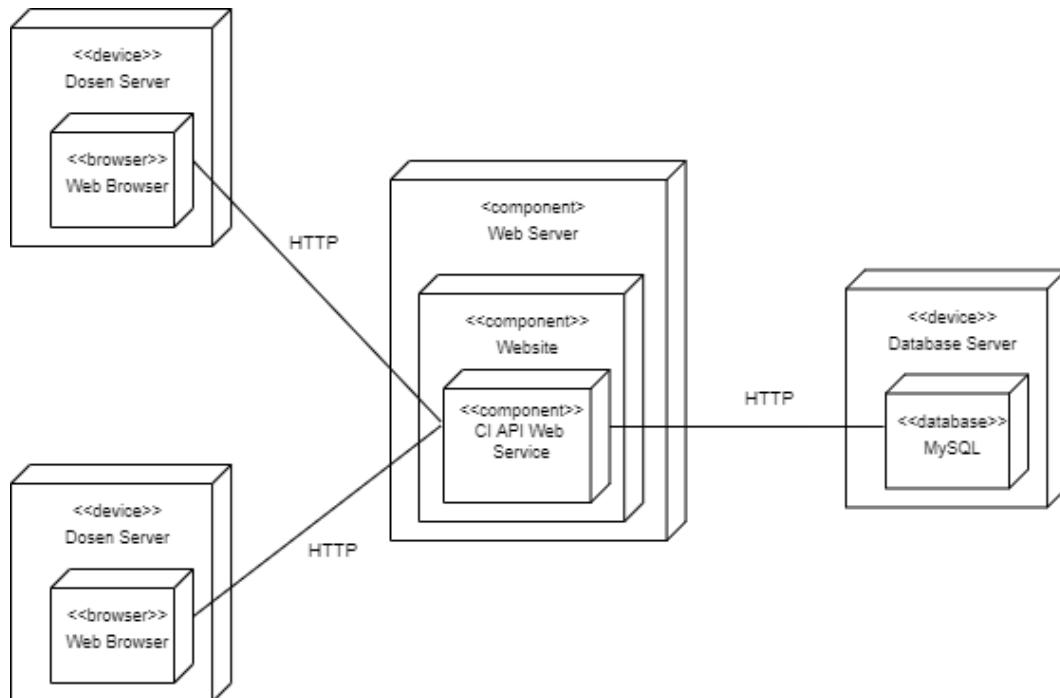
BAB VI

IMPLEMENTASI

Pada bab ini dijelaskan hasil implementasi dari perancangan yang telah dilakukan pada BAB V dokumen ini.

VI.1 Infrastruktur Sistem

Pada sub bab ini menjelaskan gambaran web aplikasi dalam infrastruktur sistem berdasarkan perancangan arsitektur pada BAB Perancangan. Tujuan dari sub bab ini adalah menggambarkan arsitektur fisik sistem berbasis *Object Oriented Programming* dan *arsitektur logic* yang sudah menerapkan prinsip MVC. Berikut merupakan gambar *deployment diagram* untuk aplikasi yang akan dibangun:



Gambar VI. 1 Infrastruktur sistem

Deployment diagram digunakan untuk memodelkan perangkat lunak diimplementasikan pada perangkat keras. Pada gambar diatas terdapat beberapa komponen sebagai berikut:

1. *Device*, merupakan perangkat yang digunakan oleh *user* untuk menjalankan sebuah perangkat lunak seperti *website* dengan aplikasi *web browser* yang terhubung dengan koneksi internet.
2. *Web Server*, merupakan perangkat lunak yang memberikan layanan data yang mempunyai fungsi untuk menerima permintaan HTTP (*HyperText Transfer Protocol*) atau HTTPS yang dikirim oleh klien melalui web browser dan mengirimkan kembali hasilnya dalam bentuk halaman web yang umumnya berbentuk dokumen HTML(*HyperText Markup Language*).
3. *Database Server*, merupakan sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/server.

VI.2 Matriks Implementasi

Pada sub bab ini menjelaskan mengenai daftar requirement yang telah diimplementasikan dalam pengembangan aplikasi. Daftar requirement tersebut mengacu pada dokumen SRS.

Tabel VI. 1 Matriks implementasi

Kode FR	Requirement	Use Case	User Interface	Status
REQ-F-01	Aplikasi dapat melakukan autentikasi pengguna.	UC1	UI-01, UI-02	Selesai
REQ-F-02	Aplikasi dapat melakukan proses digital signature	UC2	UI-07	Selesai
REQ-F-03	Aplikasi dapat melakukan verifikasi dokumen.	UC3	UI-08	Selesai
REQ-F-04	Aplikasi dapat mengatur otorisasi pengguna berdasarkan role pengguna, yaitu mahasiswa, dosen dan koordinator TA	UC4	UI-03	Selesai

REQ-F-05	Aplikasi dapat mengunggah dokumen laporan TA	UC5	UI-06	Selesai
REQ-F-06	Aplikasi dapat mengunduh laporan TA	UC6	UI-09	Selesai
REQ-F-07	Aplikasi dapat menambahkan akun pengguna baru	UC7	UI-04, UI-05	Selesai
REQ-F-08	Aplikasi dapat membubuhkan tanda tangan pada dokumen.	UC8	UI-010	Selesai

VI.3 Penggunaan *Library*

Bagian ini memuat kumpulan *library* yang digunakan saat implementasi. Penggunaan *library* ini bertujuan untuk meningkatkan efisiensi sehingga waktu implementasi menjadi lebih banyak. Berikut daftar *library* yang digunakan :

Tabel VI. 2 Penjelasan library

No.	Nama <i>Library</i>	Keterangan
1.	phpseclib	Digunakan untuk keperluan enkripsi, generate key, dan verifikasi digital signature
2.	password_hash	Digunakan untuk melakukan <i>hashing password</i> saat mendaftarkan akun baru
3	Session	Melakukan izin untuk setiap dashboard yang sesuai dengan level akun yang sesuai

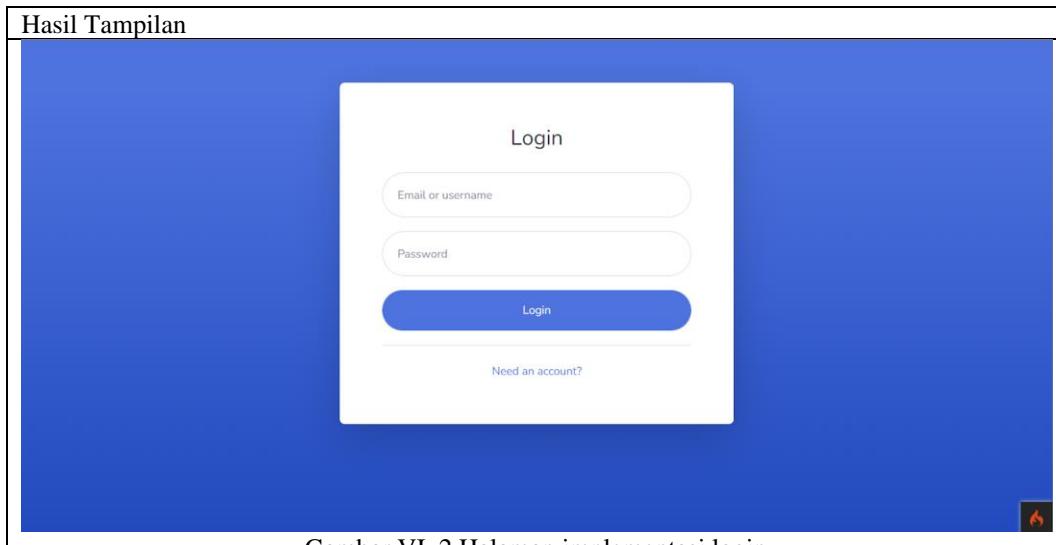
VI.4 Hasil Implementasi

Pada bagian ini berisi penjelasan fitur yang telah diimplementasikan. Fitur digambarkan dengan melampirkan *screenshot* dari aplikasi. Berikut merupakan hasil implementasi aplikasi berbasis *web* yang ditunjukkan pada tabel implementasi dan deskripsinya.

VI.4.1 Halaman Login

Tabel VI. 3 Halaman implementasi login

No. Implementasi	IM-001
Kode UI	UI-001



Gambar VI. 2 Halaman implementasi login

Deskripsi	Gambar diatas merupakan halaman login yang muncul ketika user mengakses website. Pada halaman ini, aplikasi menampilkan tombol login. User mengisi terlebih dahulu email atau username dan kata sandi agar bisa mengakses website.
-----------	--

VI.4.2 Halaman Daftar User

Tabel VI. 4 Halaman implementasi daftar user

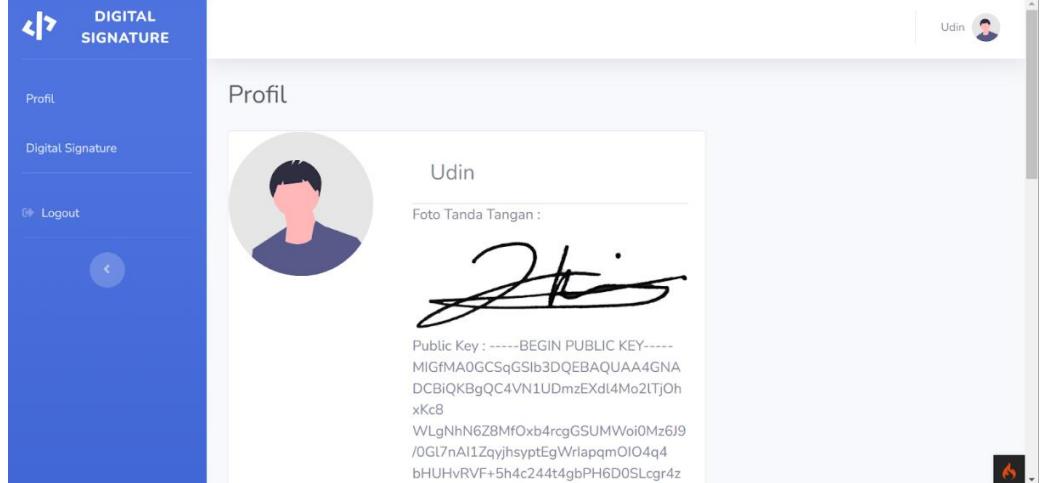
No. Implementasi	IM-002
Kode UI	UI-002
Hasil Tampilan	

Gambar VI. 3 Halaman implementasi daftar user

Deskripsi	Gambar diatas merupakan halaman daftar user yang dapat mengakses website. Halaman ini hanya dapat diakses oleh admin.
-----------	---

VI.4.3 Halaman Profil Dosen

Tabel VI. 5 Halaman implementasi profil dosen

No. Implementasi	IM-003
Kode UI	UI-003
Hasil Tampilan	
	 <p>Udin</p> <p>Foto Tanda Tangan :</p> <p></p> <pre>Public Key : -----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNA DCBiQKBgQC4VN1UDmzExdl4Mo2lTjOh xKcB WLgNhN6Z8MfOxb4rcgGSUMWoi0Mz6J9 /0Gl7nAl1ZqyjhsyptEgWrlapqmOIO4q4 bHUHvRVF+5h4c244t4gbPH6D0SLcgr4z</pre>
Gambar VI. 4 Halaman implementasi profil dosen	
Deskripsi	Gambar diatas merupakan halaman profil dosen. Terdapat nama, citra tanda tangan dan informasi mengenai key.

VI.4.4 Halaman Unduh Dokumen

Tabel VI. 6 Halaman implementasi unduh dokumen

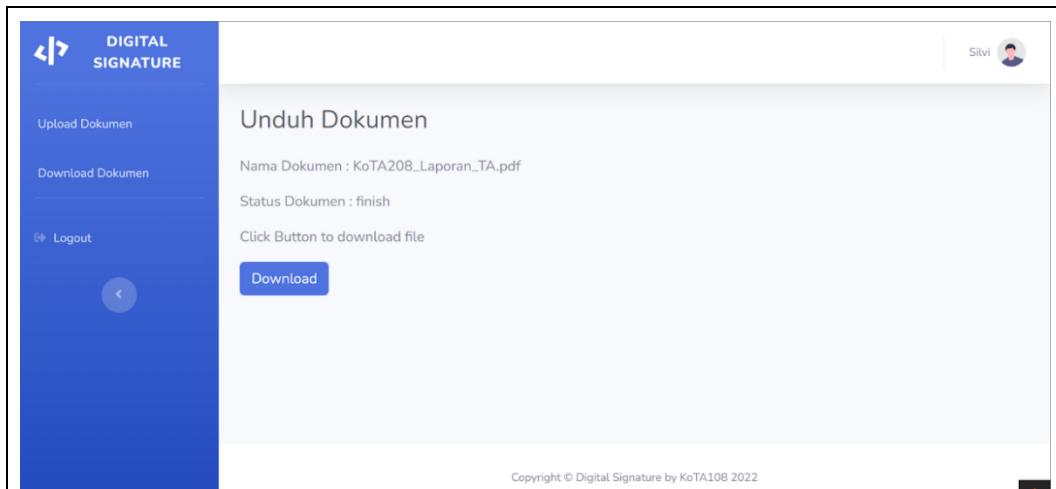
No. Implementasi	IM-004
Kode UI	UI-004
Hasil Tampilan	

	<p>Unduh Dokumen</p> <p>Dokumen Anda masih di proses</p> <p>Copyright © Digital Signature by KoTA108 2022</p>
<p>Gambar VI. 5 Halaman implementasi unduh dokumen</p>	

VI.4.5 Halaman Unduh Dokumen

Tabel VI. 7 Halaman implementasi unduh dokumen

No. Implementasi	IM-005
Kode UI	UI-005
Hasil Tampilan	



The screenshot shows a digital signature application interface. On the left, there's a sidebar with a blue background containing icons for 'Upload Dokumen', 'Download Dokumen', and 'Logout'. The main area has a white background with the title 'Unduh Dokumen'. It displays the file name 'Nama Dokumen : KoTA208_Laporan_TA.pdf', the status 'Status Dokumen : finish', and the instruction 'Click Button to download file'. A blue 'Download' button is present. In the top right corner, there's a user profile with the name 'Silvi' and a small profile picture. At the bottom right, there's a small orange flame icon.

Gambar VI. 6 Halaman implementasi unduh dokumen

Deskripsi	Gambar diatas merupakan halaman unduh dokumen jika dokumen sudah ditandatangani oleh dosen. Dokumen dapat diunduh oleh KoTA jika sudah ditandatangani oleh dosen.
-----------	---

VI.4.6 Halaman Verifikasi Dokumen

Tabel VI. 8 Halaman implementasi verifikasi dokumen

No. Implementasi	IM-006
Kode UI	UI-006
Hasil Tampilan	

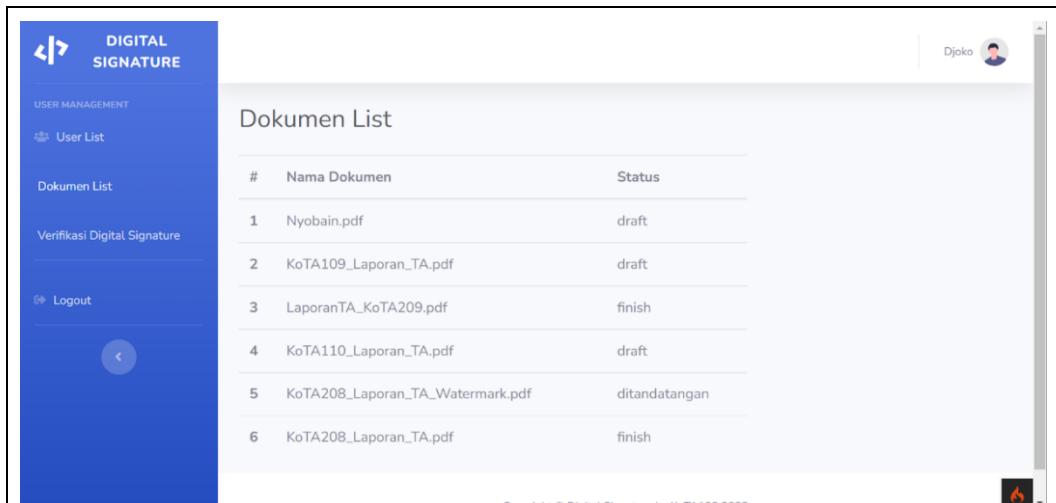
Gambar VI. 7 Halaman implementasi verifikasi dokumen

Deskripsi	Gambar diatas merupakan halaman verifikasi dokumen. Admin akan melakukan verifikasi terhadap dokumen laporan milik KoTA yang sudah selesai ditandatangani oleh dosen.
-----------	---

VI.4.7 Halaman Daftar Dokumen

Tabel VI. 9 Halaman implementasi daftar dokumen

No. Implementasi	IM-007
Kode UI	UI-007
Hasil Tampilan	



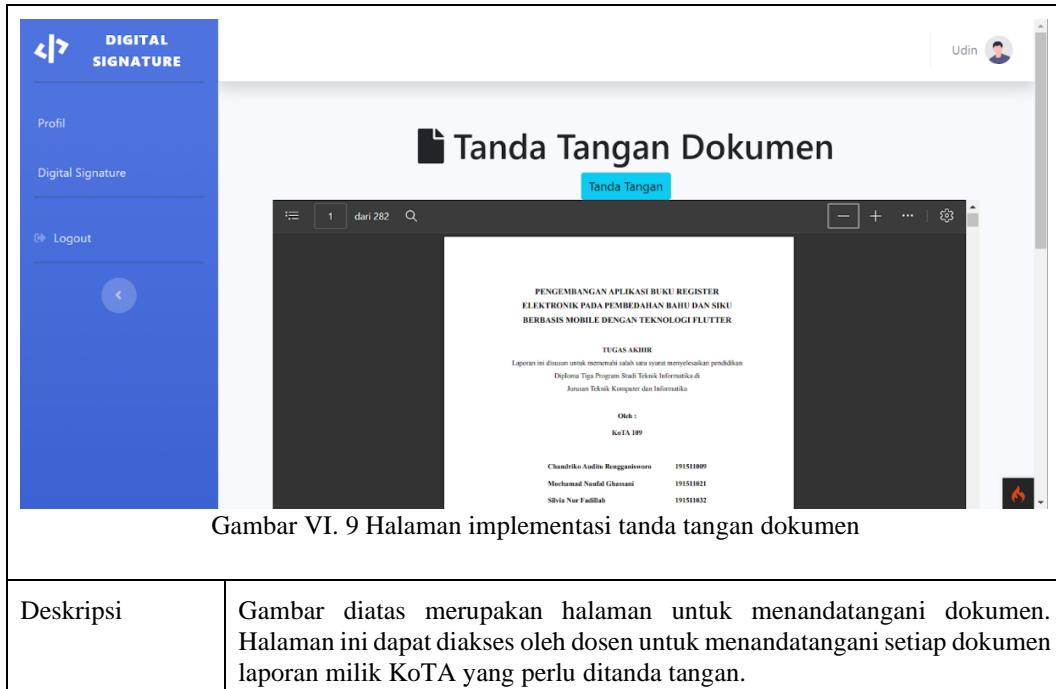
Gambar VI. 8 Halaman implementasi daftar dokumen

Deskripsi	Gambar diatas merupakan halaman daftar dokumen milik semua KoTa serta statusnya. Kolom status ini dapat berisi 3 pilihan yaitu draft, ditandatangan dan finish. Suatu dokumen berstatus <i>draft</i> jika dokumen belum ditandatangani sama sekali oleh dosen. Kemudian, jika suatu dokumen berstatus <i>ditandatangan</i> , maka dokumen tersebut sudah ditandatangani oleh minimal salah satu dosen terkait. Jika suatu dokumen berstatus <i>finish</i> , maka dokumen tersebut sudah selesai ditandatangani oleh semua dosen terkait.
-----------	--

VI.4.8 Halaman Tanda Tangan Dokumen

Tabel VI. 10 Halaman implementasi tanda tangan dokumen

No. Implementasi	IM-008
Kode UI	UI-008
Hasil Tampilan	



VI.4.9 Halaman Unggah Dokumen

Tabel VI. 11 Halaman implementasi unggah dokumen

No. Implementasi	IM-009
Kode UI	UI-009
Hasil Tampilan	

Gambar VI. 10 Halaman implementasi unggah dokumen

Deskripsi	Gambar diatas merupakan halaman unggah dokumen bagi KoTA yang akan mengunggah dokumen laporan tugas akhir. Dokumen yang diunggah harus berekstensi pdf.
-----------	---

VI.4.10 Halaman Detail Dokumen

Tabel VI. 12 Halaman implementasi detail dokumen

No. Implementasi	IM-010
Kode UI	UI-010
Hasil Tampilan	

Gambar VI. 11 Halaman implementasi detail dokumen

Deskripsi	Gambar diatas merupakan halaman detail dari setiap dokumen. Halaman ini berisi form data pembimbing dan penguji KoTA tersebut yang akan menerima dokumen laporan tugas akhir.
-----------	---

VI.4.11 Halaman Daftar Dokumen yang Perlu Ditandatangani Oleh Dosen

Tabel VI. 13 Halaman implementasi daftar dokumen

No. Implementasi	IM-011
Kode UI	UI-011
Hasil Tampilan	

Daftar Dokumen			
Nama Dokumen	Status	Tanggal Dibuat	Aksi
Nyobain.pdf	draft	2022-09-24 10:28:21	Tanda Tangan
KoTA109_Laporan_TA.pdf	draft	2022-09-24 09:52:01	Tanda Tangan

Copyright © Digital Signature by KoTA108 2022

Gambar VI. 12 Halaman implementasi daftar dokumen

VI.4.12 Halaman Registrasi

Tabel VI. 14 Halaman implementasi registrasi

No. Implementasi	IM-012
Kode UI	UI-012
Hasil Tampilan	

Deskripsi	Gambar diatas merupakan halaman registrasi bagi pengguna yang belum memiliki akun.
------------------	--

VI.4.13 Halaman Upload Tanda Tangan

Tabel VI. 15 Halaman implementasi unggah tanda tangan

No. Implementasi	IM-013
Kode UI	UI-013
Hasil Tampilan	

Gambar VI. 14 Halaman implementasi unggah tanda tangan

Deskripsi	Gambar diatas merupakan halaman upload tanda tangan. Halaman ini hanya tersedia untuk role dosen.
-----------	---

VI.4.14 Halaman Upload Tanda Tangan (Generate Key)

Tabel VI. 16 Halaman implementasi unggah tanda tangan (generate key)

No. Implementasi	IM-014
Kode UI	UI-014
Hasil Tampilan	

The screenshot shows a digital signature application interface. On the left, there is a vertical blue sidebar with navigation options: 'Profil', 'Digital Signature', and 'Logout'. The main content area has a header 'Profil' and displays a placeholder circular profile picture of a person with dark hair and a blue shirt. To the right of the picture, the name 'Ade Chandra' is shown. Below the name is a placeholder text 'Foto Tanda Tangan :'. A handwritten signature 'J And' is displayed in this space. Underneath the signature, the text 'Key Belum Ada' is visible. At the bottom of the main content area is a green button labeled '+Generate Key'. In the bottom right corner of the main content area, there is a small red icon. At the very bottom of the screen, the text 'Copyright © Digital Signature by KoTA108 2022' is visible.

Gambar VI. 15 Halaman implementasi unggah tanda tangan (generate key)

Deskripsi	Gambar diatas merupakan halaman generate ke untuk tanda tangan. Halaman ini hanya tersedia untuk role dosen.
-----------	--

BAB VII

PENGUJIAN

Pada bab ini akan dijelaskan mengenai pengujian pada aplikasi *digital signature* pada laporan tugas akhir JTK Polban. Pengujian dilakukan mengacu pada hasil analisis dan perancangan dengan tujuan untuk memastikan aplikasi dapat berjalan sesuai dengan hasil analisis dan perancangan.

VII.1 Lingkup Pengujian

Lingkup pengujian adalah lingkup yang diterapkan dan menjadi acuan dalam pengujian aplikasi. Pada pengujian berfokus pada requirement yang telah didefinisikan pada dokumen SRS. Adapun pengujian yang dilakukan dibatasi terhadap fungsi-fungsi aplikasi sebagai berikut:

1. **[REQ-F-01]** Aplikasi dapat melakukan autentikasi pengguna.
2. **[REQ-F-02]** Aplikasi dapat melakukan proses digital signature
3. **[REQ-F-03]** Aplikasi dapat melakukan verifikasi dokumen.
4. **[REQ-F-04]** Aplikasi dapat mengatur otorisasi pengguna berdasarkan role pengguna, yaitu mahasiswa, dosen dan koordinator TA
5. **[REQ-F-05]** Aplikasi dapat mengunggah dokumen laporan TA
6. **[REQ-F-06]** Aplikasi dapat mengunduh laporan TA
7. **[REQ-F-07]** Aplikasi dapat menambahkan akun pengguna baru
1. **[REQ-F-08]** Aplikasi dapat membubuhkan tanda tangan pada dokumen.

VII.2 Rencana Pengujian

Bagian ini menjelaskan rencana pengujian yang dilakukan terhadap aplikasi. Rencana pengujian meliputi tahapan pengujian yang dilakukan dan jenis pengujian yang dilakukan.

Tabel VII. 1 Profil *tester* aplikasi

Nama	Peran	Pengalaman
------	-------	------------

Alifia Ghea P.P.	Mahasiswa tingkat akhir	Sudah menyelesaikan Tugas Akhir D3 Teknik Informatika JTK Polban
Silvia Nur Fadilah	Mahasiswa tingkat akhir	Sudah menyelesaikan Tugas Akhir D3 Teknik Informatika JTK Polban
Aprianti Nanda Sari	Dosen	Berpengalaman menjadi pembimbing dan penguji Tugas Akhir D3 dan D4 Teknik Informatika JTK Polban
Sri Ratna Wulan	Koordinator TA	Berpengalaman menjadi koordinator Tugas Akhir D3 Teknik Informatika JTK Polban

VII.2.1 Tahapan Pengujian

Tahapan pengujian yang dilakukan mengacu pada dokumentasi testing dari IEEE dengan standar 829-2008. Tahapan pengujian tersebut yaitu:

1. *Test Plan*

Test plan merupakan bagian tahapan perencanaan dan persiapan terhadap pengujian yang dilakukan. *Test plan* berisi penjelasan terkait identifikasi fitur yang diujikan, menetapkan rincian pengujian dan pembagian role saat pengujian, menetapkan perencanaan perangkat yang digunakan saat pengujian berlangsung, dan menetapkan jadwal pengujian.

2. *Test Design*

Test design merupakan tahapan perencanaan pengujian dengan melakukan pengidentifikasi terhadap *test case*.

3. *Test Case*

Test case merupakan tahapan perencanaan yaitu menetapkan *case-case* yang digunakan untuk dapat menguji aplikasi.

4. *Test Procedure*

Test procedure merupakan tahapan perencanaan yaitu menetapkan prosedur yang dilakukan selama pengujian dilakukan berdasarkan *test case* yang ada.

VII.2.2 Jenis Pengujian

Pengujian aplikasi menggunakan dua jenis pengujian yaitu, *unit test* dan *user acceptance test*. Pendekatan yang digunakan adalah *black box testing*.

VII.3 Requirement yang Telah Diujikan

Dalam pengembangan aplikasi, pengujian fitur dilakukan mengacu pada daftar requirement yang telah berhasil diimplementasikan ke dalam aplikasi. Berikut merupakan tabel yang menjelaskan terkait *requirement* yang telah dilakukan pengujian terhadap aplikasi yang dikembangkan pada tugas akhir.

Tabel VII. 2 Tahap *testing* aplikasi

No. <i>Requirements</i>	<i>Requirements</i>	Cara Verifikasi			Metode/Pendekatan Pengujian	Jenis Pengujian
		Inspeksi	Analisis	Demonstrasi		
[REQ-F-01]	Aplikasi dapat melakukan autentikasi pengguna.	✓		✓	<i>Black box Testing</i>	<i>Functional Test</i>
[REQ-F-02]	Aplikasi dapat melakukan proses digital signature	✓		✓	<i>Black box Testing</i>	<i>Functional Test</i>
[REQ-F-03]	Aplikasi dapat melakukan verifikasi dokumen.	✓		✓	<i>Black box Testing</i>	<i>Functional Test</i>
[REQ-F-04]	Aplikasi dapat mengatur otorisasi pengguna berdasarkan role pengguna, yaitu mahasiswa, dosen dan koordinator TA	✓		✓	<i>Black box Testing</i>	<i>Functional Test</i>
[REQ-F-05]	Aplikasi dapat mengunggah dokumen laporan TA	✓		✓	<i>Black box Testing</i>	<i>Functional Test</i>
[REQ-F-06]	Aplikasi dapat mengunduh laporan TA	✓		✓	<i>Black box Testing</i>	<i>Functional Test</i>
[REQ-F-07]	Aplikasi dapat menambahkan pengguna baru	✓		✓	<i>Black box Testing</i>	<i>Functional Test</i>
[REQ-F-08]	Aplikasi dapat membubuhkan tanda tangan pada dokumen.	✓		✓	<i>Black box Testing</i>	<i>Functional Test</i>

BAB VIII

PENUTUP

Bagian ini menjelaskan kesimpulan dan saran terhadap pengembangan aplikasi yang telah dilakukan selama pengerjaan tugas akhir

VIII.1 Kesimpulan

Aplikasi yang dikembangkan untuk tugas akhir adalah aplikasi yang dibuat untuk membantu proses pengurusan tanda tangan dokumen laporan tugas akhir pada lingkup JTK Polban yang dapat dilakukan secara online. Aplikasi ini ditujukan untuk membantu dosen dan mahasiswa mengurus dokumen laporan tugas akhir.

Berdasarkan proses pengerjaan yang telah dilakukan selama tugas akhir, aplikasi yang dibangun telah memenuhi tujuan yang telah didefinisikan yaitu:

1. Aplikasi dapat menyediakan fitur mengenkripsi dokumen laporan tugas akhir.
2. Aplikasi dapat menyediakan fitur memverifikasi dokumen laporan tugas akhir.
3. Aplikasi dapat menyediakan fitur membubuhkan tanda tangan pada lembar pengesahan laporan tugas akhir.

Berdasarkan pengerjaan tugas akhir yang telah dilakukan, diharapkan untuk pengembangan selanjutnya aplikasi dapat memberikan solusi terhadap permasalahan yang sedang dihadapi dalam melakukan pengurusan tanda tangan pada lembar pengesahan dokumen laporan tugas akhir.

VIII.2 Saran

Berdasarkan pengerjaan tugas akhir ini, banyak hal yang belum tercapai sehingga dibawah ini merupakan saran yang diharapkan dapat membantu proses pengembangan selanjutnya.

1. Pada saat membubuhkan tanda tangan pada dokumen PDF, posisi tanda tangan masih bersifat statis sehingga posisi citra tanda tangan belum bisa berpindah tempat. Sebaiknya, bahwa setiap dosen membubuhkan tanda tangan maka letak citra akan menyesuaikan posisi pada bagian tanda tangan dosen yang membubuhkan tanda tangan.

2. Pada saat proses enkripsi, alokasi file PHAR dan ZIP masih belum tertata dengan baik di path yang seharusnya. Untuk kedepannya, Alokasi file PHAR dan ZIP sebaiknya disimpan pada path yang seharusnya.
3. Tanda tangan belum terdapat validasi apakah tanda tangan yang terdapat pada dokumen terenkripsi memang dari dosen yang bersangkutan untuk memberikan tanda tangan. Sebaiknya, ditambahkan informasi seperti waktu penandatanganan dan nama penandatangan pada bagian samping tanda tangan.
4. Sebaiknya UI/UX perlu ditambahkan penjelasan saat pemilihan form, bagian mana saja yang wajib diisi dan tidak wajib diisi.
5. Penambahan detail status dosen pada sebuah dokumen, apakah pada dokumen tersebut dosen menjadi pembimbing atau penguji perlu diperjelas.
6. Sebaiknya ditambahkan fitur kembali atau pembatalan di aplikasi ini karena fitur ini penting untuk mengidentifikasi apabila terdapat kesalahan input yang perlu dibatalkan.
7. Setiap kali proses verifikasi dokumen yang sudah ditandatangani, hanya tanda tangan dosen terakhir yang dapat terverifikasi. Hal ini dikarenakan Konsep dari RSA yang tidak dikhususkan untuk proses enkripsi multiple user dan juga batasan aplikasi yang dibangun. Sebaiknya gunakan metode yang dapat melakukan proses enkripsi *multi user* untuk kasus serupa tetapi apabila kasusnya hanya dua belah pihak maka metode yang cocok adalah RSA.
8. Fitur monitoring perolehan tanda tangan dari setiap dosen diperlukan pada aplikasi ini sehingga mahasiswa akan mengetahui status perolehan tanda tangan dosen.
9. Untuk kedepannya sebaiknya ditambahkan fitur baru seperti download dokumen pada halaman Koordinator.
10. Terkait enkripsi dokumen sebaiknya tidak mengenkripsi keseluruhan dokumen karena akan berdampak pada kecepatan proses enkripsi. Sebaiknya, hanya tanda tangan yang dienkripsi

DAFTAR PUSTAKA

- [1] Taufiqurrahman, Irawan, dan Syamsuddin. 2020. “Perancangan Sistem Tanda Tangan Digital (*Digital Signature*)”. *Prosiding Seminar Nasional Teknik Elektro dan Informatika (SNTEI)*. Makassar, 2020.
- [2] Permana, A dan Destriana, A. 2018. “Pengamanan Teks Menggunakan Metode Algoritma RSA Dengan Verifikasi Realtime Biometrik Menggunakan OpenCV”. *Jurnal Teknik: Universitas Muhammadiyah Tangerang*. 7(2), 3.
- [3] Kontributor Wikipedia. (2020, Februari 26). Aplikasi web. Retrieved from Wikipedia: https://id.wikipedia.org/wiki/Aplikasi_web
- [4] Purwoko, Lyco Adhi. 2012. “Analisis Penerapan *Digital Signature* Sebagai Pengamanan Pada Fitur *Workflow - DMS (Document Management System)*”. *Makalah IF3058 Kriptografi*. Bandung, 2012.
- [5] Panduan Tugas Akhir Program Diploma Tiga Politeknik Negeri Bandung
- [6] Sansprayada, A, Mariskhana, K, dan Aziz, R.A . 2020. “Sistem Informasi Akademik Menggunakan CI (CodeIgniter) pada Yayasan Az zahra Tangerang Selatan”. *Jurnal Teknologi Informatika dan Komputer MH Thamrin*. 6(2), 34.
- [7] NurmalaSari, N, Anna, A, dan Arissusandi, R. 2019. Rancang Bangun Sistem Informasi Akuntansi Laporan Laba Rugi Berbasis Web Pada Pt. United Tractors Pontianak. *Evolusi: Jurnal Sains dan Manajemen*. 7(2), 9.
- [8] Hidayat, H., Hartono and Sukiman (2017) ‘Pengembangan Learning Management System (LMS) untuk Bahasa Pemrograman PHP’, *Jurnal Ilmiah Core IT: Community Research Information Technology*, 5(1), pp. 20–29.
- [9] Putra, A. C., Simanjuntak, M., & Nurhayati. (2021). Penerapan Algoritma Rivest Shamir Adleman (RSA) Untuk Mengamankan Database Program Keluarga Harapan (PHK). *Jurnal Informatika Kaputama (JIK)*, 5(1), 101.

- [10] Brink, J. van den (Pieter J. C. M., Monumentenstichting Baet en Borgh., N. B., Historische Vereniging Tweestromenland., J., & Azanuddin, A. (2014). Mensen van Maas en Waal. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer)*, 18(1), 30–34. <https://ojs.trigunadharma.ac.id/index.php/jis/article/view/100>
- [11] E. Noroozi,. 2013. Secure Digital signature Schemes Based on Hash Functions. *International Journal of Innovative Technology and Exploring Engineering(IJITEE)*.
- [12] Hutasuhut, B. K., Efendi, S., & Situmorang, Z. (2019). Digital Signature untuk Menjaga Keaslian Data dengan Algoritma MD5 dan Algoritma RSA.
- [13] Larman, C. (2004). *Applying UML and Patterns: An Introduction to Object Oriented Analysis and Design and Iterative Development*. Pearson Prentice Hall.
- [14] Sommerville, I. (2011). Software Engineering Ninth Edition.
- [15] Pressman, Roger S. (2010). *Software Engineering seventh edition: A Practitioner's Approach*
- [16] MariaDB foundation. MariaDB.org. (2019, November 13). Retrieved October 9, 2022, from <https://mariadb.org/>
- [17] TCPDF. (n.d.). Retrieved October 3, 2022, from <https://tcpdf.org/>
- [18] PHPSeclib. (n.d.). Retrieved March 20, 2022, from <https://phpseclib.com/>
- [19] Setasign, <https://www.setasign.com>. (n.d.). *TCPDF in combination with FPDI ▷ setasign.com*. Setasign. Retrieved October 12, 2022, from <https://www.setasign.com/products/fpdi/demos/tcpdf-demo/>
- [20] Phar. php. (n.d.). Retrieved October 12, 2022, from <https://www.php.net/manual/en/book.phar.php>
- [21] Silitonga, J., Suswaini, E., & Kurniawan, H. (2013). Pendaftaran Mahasiswa Baru Berbasis Mobile (Studi Kasus : Universitas Maritim Raja Ali Haji). *Jurnal Umrah*, 1.